Fingeravtrykkbasert arbeidstidsregistrering

Ei juridisk analyse av arbeidsgjevars åtgang til å innføre og drifte fingeravtrykkbaserte tidsregistreringssystem ovanfor verksemdas arbeidstakarar.

Kandidatnummer: 199

Antall ord: 13 813

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

11. desember 2024

Innhald

1 Innleiing 2

1.1 Problemstilling 2

1.2 Materielle vegval og metodiske særpreg 2

1.3 Biometri og system for tidsregistrering 3

1.4 Personvernregulering, trinnhøgare personvern og personverninteresser 4

2 Forordningas utgangspunkt om biometriske opplysningar 6

2.1 Personopplysningsvern som arbeidstakarrett 6

2.2 Behandlingsforbodet 7

2.3 Behandling av personopplysningar 9

2.4 Biometriske opplysningar – eit juridisk omgrep 10

2.5 Eintydige identifikasjonar 11

3 Behandlingsprosessens innleiande kartleggingsfase 14

3.1 Vegen inn mot PVF art. 9 nr. 2 14

3.2 Alminneleg lovleg behandling 14

3.3 Kartleggings- og informasjonsplikta 15

3.4 Den norske særregelen om eintydig identifikasjon 17

3.5 Problemstillinga knytt til arbeidstakars samtykke 18

4 PVF art. 9 nr. 2 bokstav b 22

4.1 Ordlyd 22

4.2 Vilkåret om ytterlegare rettslege grunnlag 22

4.3 Vilkåret om naudsynte garantiar 25

4.4 Vilkåret om naudsemd 26

4.5 Proporsjonalitetsvurderinga 30

Litteraturliste 38

Lov, forskrift og konvensjon mv. 38

Rettspraksis og underrettspraksis 38

Førarbeid 39

Rettleiingsskriv 39

Tidsskrifter 39

Artiklar og lovkommentarar 40

1 Innleiing

1.1 Problemstilling

I fleire tusen år har menneskjer brukt kroppslege avtrykk for å identifisere seg sjølv.[1] Moderne biometrisk teknologi har vel å merke gått vekk frå oldtidas leirtavler og over til mekaniske sensorar, men prinsippet er framleis det same: unik fysisk- og åtferdsmessig karakteristikk blir brukt til å fastslå kven eit individ er. Dette er eit felt som gjennom dei siste tiåra har gjennomgått ei enorm utvikling. Sjukehus kan nå drive smittesporing ved å installere sensorar som målar temperaturen på forbi-passerande,[2] våpenprodusentar utviklar avtrekkarar som berre let seg bruke av eigarens hender[3] og skular kan bruke ansiktsattkjennande videokamera til å registrere fråvær.[4] Korleis er så bruken av biometriske løysingar regulert? Gjennom denne masteroppgåva ser eg på EU-rettsleg- og norsk regulering kring behandling av arbeidstakarar sine biometriske opplysningar. Oppgåvas primære problemstilling er om – og eventuelt i kva utstrekning - ein arbeidsgjevar har åtgang til å bruke digitale system som registrer arbeidstid gjennom fingeravtrykkregistrering. Analysen ser fyrst til den heilskaplege reguleringa kring biometrisk tidsregistrering og rettar dinest særleg fokus mot personvernforordningas artikkel 9 nr. 2 bokstav b.

1.2 Materielle vegval og metodiske særpreg

Problemstillinga har nær tilknyting til båe personvernretten- og arbeidsrettens område. Denne oppgåva rettar seg hovudsakleg mot personvernretten og vil i mindre grad behandle arbeidsrettslege problemstillingar. Analysen søker å framheve heilskapen kring reguleringa av arbeidsrelatert fingeravtrykkregistrering og mykje av oppgåvas fokus er difor retta mot moglegheita til å rettmessig drive biometrisk arbeidstidsregistrering på basis av rettslege forpliktingar, samt basert på drøftingar av naudsemd og interessekonfliktar. Ettersom det i praksis har vist seg at arbeidsgjevarar også ofte

[1] Jf. 1) Hopkins R. *An Introduction to Biometrics and Large Scale Civilian Identification* (1999), s. 338 og 348. 2) Taal, A. *The GDPR Challenge: (…)* (2021), side 162, med vidare tilvisingar.
[2] Jf. Burt C., «Facial recognition and temperature scanning (…)», Biometric Update.com, 06. januar 2023, URL: https://www.biometricupdate.com/202301/facial-recognition-and-temperature-scanning-devices-launched-deployed-for-access-control, (lese den: 27.09.23).
[3] Jf. Smith M. og Miller S. *Biometric Identification, Law and Ethics* (2021), side 4 og 5.
[4] Jf. Burt C., «Australian schools testing facial recognition for attendance», Biometric Update.com, 29. august 2018, URL: https://www.biometricupdate.com/201808/australian-schools-testing-facial-recognition-for-attendance (lese den: 27.09.23).

søker å realisere biometriske prosessar gjennom arbeidstakars samtykke, så blir problemstillinga knytt til samtykke som eit alternativt rettsleg grunnlag også diskutert i teksten.

Rettskjeldebilete kring personvernretten kan vere vanskeleg å navigere seg i. Norsk personvern er knytt til EU-retten, heimla i den Europeiske Personvernforordninga - eit forholdsvis nytt regelverk som søker å harmonisere medlemsstatars regulering av personopplysningsvernet. Fylgjeleg kunne ein gjerne sett at det eksisterte mykje rettleiande praksis frå båe EU-domstolen og frå norske domstolar. Ettersom utvalet av praksis - knytt til problemstillinga i denne oppgåva - derimot er avgrensa så har eg valt å gjere eit vidt kjeldesøk. Analysen rettar fylgjeleg ein del søkeljos mot EØS-statars administrative og rettslege praksis. I tillegg vil det bli vist til fleire offentlege rettleiingsskriv frå EU-organ og andre personvernmyndigheiter for å avhjelpe fråværet av aktuelle og nyanserande førarbeid knyt til personvernforordninga. Til sist kjem peronverninteresser til å stå i sentrum av naudsynsdrøftinga i forordningas artikkel 9 nr. 2 bokstav b; dimed kjem desse til å utgjera ein raud tråd gjennom oppgåva.

1.3 Biometri og system for tidsregistrering

Læra om biometri handlar om å slå fast identiteten til eit individ med teknologi som måler og samanliknar kroppslege kjenneteikn, så som ved fingeravtrykkregistrering og ansiktsattkjenning. Desse prosessane har to primære funksjonar, dei er anten meint å slå fast kven eit individ er (identifisering), eller å avklare om ein identifisert person er den han eller ho utgjer seg for å vere (verifisering).[5] For næringsdrivande har biometri, blant anna, potensial til å vere eit verkemiddel som forenklar, styrkar og effektiviserer verksemdas administrative tidsregistreringssystem. Føremålet med sånne system er å lage ei oversikt som synar når verksemdas tilsette arbeider. Systema skal dimed sikre at båe arbeidsgjevar og tilsette mottek ytingane dei har krav på. Arbeidstidsregistra bidreg òg til arbeidet med å avdekke potensielle avvik frå reglar knytt til blant anna arbeidstid, pausar og ferie.[6]

Gjennom effektivisering, teknisk utbetring og reduserte kostnader har tilgangen og interessa for biometriske løysingar - så som biometribaserte system for tidsregistrering – auka dei siste åra. Pågangen har også å gjere med at biometriske målingar jamt over er prega av å vere tidsresistente.[7] Dataa kan med andre ord brukast over lang tid, utan at det er nødvendig å gjere nye målingar. Vidare kan tilsette naturleg nok verken miste eller låne vekk sine biometriske kjenneteikn. Ein kan fylgjeleg forstå at mange innovative næringsdrivande ynskjer å implementere biometrisk teknologi.

[5] Jf. Fairhurst, M., *Biometrics – A very short introduction* (2018), side 29 og 30.
[6] Jf. 1) Arbeidsmiljølova § 10-7, og
2) Ot.prp.nr. 49 (2004-05), side 320. Meir om dette i delkapittel 4.2.
[7] Jf. Holland P. og Tham T. L. «Workplace biometrics: (…)», *Economic and Industrial Democracy*, volum 43, (2020), side 501–515.

Baksida med biometriske system er at prosessane føreset ei innsamling og vidarebehandling av informasjon og persondata som - i kraft av å vere uløyseleg knytt til det registrerte individet sin integritet og kroppslege privatsfære - har eit inherent sensitivt og verneverdig preg.[8] At dataa er verneverdige bygger ikkje berre på at desse er nært knytt til kroppen vår, men òg på ei rekke andre moment som leier til at behandlinga ikkje er i den registrerte si interesse. Eksempelvis let ikkje biometriske data seg resette; så som ein kan gjere med gløymde passord og tapte nøkkelkort. Ein har altså ingen nødknapp i høve det skulle bli naudsynt å endre dataa, noko som gjer det risikabelt å nytte biometriske behandlingsprosessar.

1.4 Personvernregulering, trinnhøgare personvern og personverninteresser

Norsk regulering av biometriske opplysningar fylgjer som nemnd, primært, av EUs forordning 2016/679 the General Data Protection Regulation, frå 27. april 2016 om vern av fysiske personar i samband med behandling av personopplysningar, og om fri utveksling av sånne personopplysningar. På norsk heiter denne EUs personvernforordning, typisk avkorta til personvernforordninga eller PVF. Målsetjinga med forordninga er å etablere ei harmonisert, generell og heilskapleg personvern-regulering for båe EU-borgarar og andre som oppheld seg i EU og EØS-statar.[9] For også å bitte EØS-statane til PVF fatta EØS-komiteen vedtak den 06. juli 2018 om å innlemme forordninga i EØS-avtalen.[10] Inkorporeringa i norsk rett skjedde den 15. juni 2018, ved lov nr. 38 om behandling av personopplysningar (heretter personopplysningslova eller pol.), jf. § 1.

Ei av personopplysningsvernets overordna målsetjingar er å bidra til ivaretakinga av den einskilde sin autonomi og rett til respekt for sitt privatliv.[11] I tillegg til å ha sjølvstendig betyding utgjer person-opplysningsvernet òg eit underordna ledd ved det trinnhøgare personvernet, heimla blant anna i Den Europeiske Menneskerettskonvensjonen (EMK) artikkel 8- og Grunnlovens (Grl.) § 102 om respekt for eins privatliv, familieliv, heim og korrespondanse, samt etter EMK art. 10 og Grl. § 100 om den einskilde sin rett på ytringsfridom. Denne samanhengen mellom personopplysningsvern og menneskerettane er betydeleg nok til at personopplysningsvernet kan skildrast som ein sentral føresetnad for det moderne og digitaliserte demokratiet.[12]

EMD-dommen GLUKHIN v. RUSSLAND frå 04.07.23 synar godt validiteten av utsegna over.[13]

[8] Jf. Schartum D. W. *Personvernforordningen – en lærebok* (2020), side 13-15.
[9] Jf. 1) Personvernforordningas fortalepunkt nr. 2 og 3, og
2) PVF artikkel 3 nr. 2 om sakleg verkeområde.
[10] Jf. EØS-avtalen, Vedlegg XI, nr. 5e om Datasikring.
[11] Jf. PVF fortalepunkt nr. 2 og 4.
[12] Jf. NOU 2022: 11 *Ditt personvern – vårt felles ansvar*, side 9.
[13] Jf. *Glukhin v. Russia* [J] 2023, no. 11519/20.

Saka omhandla Nikolay Sergeyevich Glukhin som i 2020 reiste med ein plakat på russisk T-bane. På plakaten uttrykke Glukhin støtte til ein russisk aktivist og motstandar av det russiske statsapparatet. Ved å bruke ansiktsattkjennande videoovervaking i undergrunnen klarte russisk etterretning etter kort tid å identifisere, oppsøke, arrestere og skulde Glukhin for å ha demonstrert ulovleg. Domstolen kom til at identifiseringsmetoden - sett i kontekst av at den vart brukt for å sanksjonere Glukhin for ei fredeleg protest - var svært invaderande, samt at den ikkje var «nessecary in a democratic society». Retten kom til at inngrepet braut med EMK art. 8 og 10, som Russland framleis var botne av i 2020.

I tillegg til å skildre koplinga mellom personopplysningsvernet og det trinnhøgare personvernet utgjer GLUKHIN v. RUSSLAND eit frykteksempel på korleis nettopp biometrisk teknologi kan misbrukast til skade for befolkninga og på tvers individets interesser. Saka synar nøyaktig kor makteslaus den registrerte kan vere i møte med biometriske prosessar og mot behandlingsansvarlege som har makt til å ivareta og få gjennomslag for eigne interesser. Det er i situasjonar som denne at den svake part står i fare for å erfare skilnaden mellom å ha rett og å få rett. Samanfatta er altså dommen også eit godt døme på kvifor den enkelte innbyggar har store interesser knytt til personopplysningsvernet.

2 Forordningas utgangspunkt om biometriske opplysningar

2.1 Personopplysningsvern som arbeidstakarrett

Personvernet gjeld ikkje berre når me opptrer som privatpersonar, men er også ein arbeidstakarrett.[14] Arbeidsforhold utfoldar seg på mangfaldige vis, men ein fellesnemnar er at arbeidsgjevar sit med styringsretten og dimed også den sterkaste posisjonen i tilsetjingsforholdets interne maktrelasjon.[15] Personopplysningsvernet bidreg til å jamne ut dette misforholdet ved å skjerme arbeidstakarar mot invaderande og urettmessige behandlingsprosessar. Nye teknologiske løysningar og kontrolltiltak nødvendiggjer altså at verksemda fyrst avdekker konsekvensane av å implementere det nye tiltaket. Eit grunnleggjande spørsmål ved denne kartleggjande konsekvensdrøftinga er nettopp om tiltaket er foreinleg med arbeidstakaranes rett på personopplysningsvern.[16]

Ei rekke alminnelege personverninteresser kan aktualiserast ovanfor arbeidstakarar. Fyrst og fremst kan kontrolltiltak og monitorering av verksemdas tilsette leie til at dei råka arbeidstakarane kjenner seg pressa til å avstå frå å utøve grunnleggande rettar. Eksempelvis er overvaking eigna til å medføre ubehag knytt til å samle seg og å tale fritt på jobb.[17] For det andre kan monitorering slå negativt ut i relasjon til den daglege drifta på arbeidsplassen. Til dømes vil arbeidsmiljøets heilskap lide i høve tilsette ikkje rapporterer om interne avvik og konfliktsituasjonar. Eit sånt omstende kan eksempelvis oppstå dersom korrespondansen til arbeidstakarar blir vaka over, og dei tilsette dimed ikkje har tillit til at verksemdas varslingsprosedyrar er anonyme.[18] Resonnementet mitt er fylgjeleg at inngripande behandlingsprosessar er eigna til å skape mistillit og flid mellom arbeidsgjevar og arbeidstakarane.[19] Dersom verksemda ikkje handterer sånne konfliktsituasjonar risikerer ein at arbeidsmiljøet får ein betydeleg smell, eller at det utviklar seg fryktkulturar på arbeidsplassen. Sånne arbeidsforhold kan i tur resultere i til dømes misstrivsel på jobb, samt nedsett mental- og fysisk helse.[20] Fylgjeleg er det ikkje berre i arbeidstakars- men òg arbeidsgjevars interesse å unngå behandlingsprosessar som går utover dei tilsette sine personverninteresser og utover personopplysningsvernet.

[14] Jf. Skullerud, mfl., *Personopplysningsloven og Personvernforordningen (GDPR) – (…)*, (2019), side 38.
[15] Jf. Artikkel 29-gruppa, *Opinion 2/2017 on data processing at work*, (2017), side 9 og 10.
[16] Jf. Arbeidstilsynet, Datatilsynet, mfl., *Veileder om kontroll og overvåking i arbeidslivet*, (2019), side 3.
[17] Jf. Artikkel 29-gruppa, *Opinion 2/2017 (…)*, (2017), side 9 og 10.
[18] Ibid. side 10.
[19] Jf. Holland P. og Tham T. L. «Workplace biometrics: (…)», *Economic and Industrial Democracy*, volum 43, (2020), side 501–515.
[20] Jf. Nielsen, M. B. og Einarsen, S., «Outcomes of exposure to workplace bullying: (…)», (2012), *Work and Stress*, vol. 26, side 327. Merk at kjelda omhandlar konsekvensar av dårlege arbeidsmiljø generelt.

Ettersom arbeidsgjevar er den som definerer føremålet med behandlinga og peikar ut midlane som skal brukast for å gjennomføre behandlingsprosessen, så opptrer denne som behandlingsansvarleg og er dimed også forplikta til aktivt å etterleve personvernreglane, jf. PVF art. 4 nr. 7 og art. 5 nr. 2.

I praksis er arbeidsgjevarar likevel ikkje kjende for alltid å vise forståing for betydninga av persondata og interessene som er knytt til desse.[21] I åra sidan personvernsforordninga tredde i kraft har nasjonale tilsynsmyndigheiter over heile Europa avdekka og sanksjonert mangfaldige næringslivsaktørar for avvikande og urettmessig behandling av personopplysningar og biometriske data. Seinast i november 2022 vart klubben Sportitalia bøtlagt av det italienske datatilsynet for å urettmessig registrere tilsette sine fingeravtrykk, som ledd i eit system for arbeidstidsregistrering.[22] Saka enda med ei bot på 20 000 Euro og klubben vart pålagt å avvikle prosesseringa. Kva seier så PVF om biometriske opplysningar?

2.2 Behandlingsforbodet

Behandling av biometriske opplysningar er regulert i forordningas artikkel 9 nr. 1 som gjeld såkalla særlege personopplysningar. Føresegna bestemmer at: *«Behandling av personopplysninger om (…) biometriske opplysninger med det formål å entydig identifisere en fysisk person (…) er forbudt».* Artikkelen reiser eit alminneleg utgangspunkt om at det ikkje skal førekome behandling av biometriske opplysningar. Forordningas fortalepunkt nr. 51 grunngjev forbodet med å vise til at særleg kategoriserte personopplysningar er sensitive for misbruk og at behandling av denne type data jamt over inneberer ein høgare risiko for brot mot den registrerte sine rettar og fridom. Behandlingsforbodet er likevel berre eit utgangspunkt, og vidare i teksten kjem me til å sjå at det eksisterer unntak som, gjennom strenge vilkår, likevel opnar for behandling av biometriske data.

PVF art. 9 nr. 1 reiser tre rettslege spørsmål. For det fyrste må arbeidsgjevar avklare om fingeravtrykk-registreringa medfører ei *behandling* av personopplysningar. Dinest om det skjer ei behandling av *biometriske opplysningar.* Til sist om behandlinga har som *føremål å identifisere ein fysisk person*.

Før me går vidare med drøftinga av dei tre nemnde vilkåra, kjem me til å sjå nærare på kvifor nettopp biometriske data og fingeravtrykk er inkludert som ein særleg kategori personopplysningar. Artikkelforfattar Daria Bulgakova skriv at «Biometric data are personal data directly, univocally, and in a tendential way stable over time, connected to the individual and denote the profound relationship

[21] Jf. Holland P. og Tham T. L. «Workplace biometrics: (…)», *Economic and Industrial Democracy*, volum 43, (2020), side 501–515.

[22] Sjå i databasen: GDPR.it - *Garante per la protezione dei dati personali*, nasjonalt saksnr.: 9832838, URL: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9832838 (lese 14.11.23).

between the person's body, behavior, and identity».[23] Skildringa til Bulgakova framhevar mange av dei same momenta som vart nemnd i innleiinga. Fyrst og fremst har biometri ein tett samanheng med kroppen vår. Dette aspektet ved biometriske opplysningar gjer at risikoen og skadepotensialet knytt til identitetstjuveri aukar. Dette har i fyrste omgang å gjere med at arbeidstakaren verken kan resette eller kalle attende dei biometriske opplysningane; tidsresistensen medfører at dataa derimot vil vere verdifulle og brukande over lang tid. I tillegg vil identitetstjuveriet potensielt medføre ringeffektar for andre biometriske system som også er basert på registrering av den råka sine fingeravtrykk.[24]

Eit anna uheldig aspekt ved biometri og målingar av fingeravtrykk er at desse opplysingane kan samlast inn utan at den registrerte har kjennskap til det.[25] Me etterlet oss alle fingeravtrykk på kaffikoppar, handtak og andre overflater, og individ med ureielege intensjonar kan, på same vis som krimteknikarar, samle inn desse biometriske spora våre. Med rette er det nok dei færraste som bekymrar seg for fingeravtrykktjuveri. I forlenging av resonnementet i føre avsnitt kan ein likevel ha i mente at verdien av biometriske data aukar etter kvart som me tek i bruk fleire biometriske prosessar. Desto viktigare blir det difor å unngå ein for vid åtgang til å behandle desse.[26]

Eit tredje uheldig aspekt ved registrering av fingeravtrykk er at dataa kan brukast til å oppdage andre sensitive opplysningar om den registrerte. Til dømes synar forsking at fingeravtrykk-målingar er eigna til å avdekke den registrerte sin etniske bakgrunn.[27] Fingeravtrykk kan vidare, indirekte, røpe intime helseopplysningar. Ein kan for eksempel gjere anslag på sjansen for at den registrerte anten har diabetes eller eventuelt om personen ligg ann til å pådra seg sjukdomen.[28]

Presisjonsnivået til biometriske prosessar utgjer eit fjerde aspekt som seier noko om kvifor desse inngår i behandlingsforbodet i PVF art. 9 nr. 1. I innleiinga nemnde eg vel å merke at biometriske prosessar har vorte populære fordi teknologien er nøyaktig, men den er ikkje 100% presis. Det alltid fare for tekniske svikt som leier til at systemet avviser den registrerte, eller verre, at personen blir feilaktig akseptert. Legg ein til grunn at presisjonsnivået til biometriske prosessar ligg på rundt 96% - i motsetning til passord som anten er 100% korrekt eller feil - så kan ein argumentere for

[23] Jf. Bulgakova, D., *Case Study on the Fingerprint Processing in a Workplace under GDPR Article 9 (2, b)*, (2022), Vilnius University, Faculty of Law, side 32.
[24] Jf. Det Europeiske Datatilsynet (EDPS), *Opinion of [EDPS] on the Proposal (…) concerning the Visa Information System (VIS) (…)*, (2005), C 181/19 – seksjon 3.4.2.
[25] Jf. Datatilsynet, *Biometri – Biometriske data kan samles uten at du vet det*, (sist endra 17.07.19), URL: https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/biometri/ (lese: 02.11.23).
[26] Ibid.
[27] Jf. Fournier, N. A. og Ross A. H., «Sex, Ancestral, and pattern type variation of fingerprint minutiae: (…)», (2016), *American Journal of Physical Anthropology*, Vol. 160, side 625–632 (630).
[28] Jf. Kahn H., mfl., «A fingerprint marker from early gestation associated with diabetes in middle age: (…)», (2009), *International Journal of Epidemiology*, Vol. 38, Issue 1, side 101–109 (105-107).

at passordmetoden er sikrare.[29] Denne siste ulempa let seg vel å merke avhjelpe ved å bruke biometriske system i kombinasjon med andre identifikasjons- og verifikasjons metodar.

Kumulert synar momenta over kvifor behandling av biometriske data, som alminneleg utgangspunkt, er forbode. Det fyrste ein kvar aktør som ynskjer å gjennomføre biometriske prosessar må gjere er fylgjeleg å avklare om behandlinga aktualiserer behandlingsforbodet i forordningas artikkel 9 nr. 1. Gjennom dei neste punkta går me difor gjennom dei tre nemnde rettslege vilkåra.

2.3 Behandling av personopplysningar

Det fyrste vilkåret arbeidsgjevar må ta stilling til, etter PVF art. 9 nr. 1, er som nemnd om den fingeravtrykkbaserte tidsregistreringa medfører ei *behandling* av personopplysningar. Ordet «behandling» kan skildrast som ei open eller vid formulering, noko som dimed tilseier at føresegna har eit vidt bruksområde. Nemninga er legaldefinert i PVF artikkel 4 nr. 2, som legger til grunn at: «*enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring».* Ei naturleg ordlydsfortolking av frasen «enhver operasjon» tilseier også at nemninga *behandling* har eit vidfarande bruksområde. Utgangspunktet er altså at den behandlingsansvarlege sjeldan handsamar personopplysningar, utan at prosessen utgjer ei *behandling*.[30] Fingeravtrykkbasert tidsregistrering vil med dette utgjere ein behandlingsprosess som innfrir det fyrste vilkåret i PVF art. 9 nr. 1.

I ei sak frå 2021, tinga for klagedomstolen Audiencia Provincial de Barcelona i Spania, jf. AP Barcelona - Auto 72/2021, ser ein nøyaktig kor langt behandlingsnemninga rekker. Den spanske domstolen tok stilling til om ei matvarekjede kunne montere ansiktsattkjennande videokamera i butikkane sine. Føremålet med overvakinga var å sikre kjeda sine butikkar frå to individ, som begge vart pålagde besøksforbod mot butikkane for å ha gjort eit valdeleg ran. Selskapet noterte at biometrisk informasjon om andre registrerte personar automatiske ville bli sletta etter 0,3 sekund. Domstolen konstaterte at sjølv ekstremt kortvarig behandling av passerande sine ansiktsformer, med føremål om å identifisere personar, medfører ei behandling av særleg kategoriar personopplysningar. Forbodet i PVF art. 9 nr. 1 kom dimed til bruk. Ettersom retten ikkje fant at det kunne gjerast rettslege unntak for den aktuelle prosesseringa så vart videoovervakinga forbode. Dommen eksemplifiserer at

[29] Jf. EDPS i samarbeid med den spanske datatilsynsmyndigheita (AEPD), *14 Misunderstandings with regard to biometric identification and authentication*, (2020), side 2. URL: https://edps.europa.eu
[30] Jf. Jarbekk, E. og Sommerfeldt, S. *Personvern og GDPR i praksis* (2019), side 41.

sjølv særs kortvarig handsaming utgjer ei *behandling* som aktualiserer personvernregelverket. Det same utgangspunktet vil vere relevant også for fingeravtrykkbasert tidsregistrering. Eksempelvis vil arbeidsgjevar ikkje få medhald i at det ikkje skjer ei behandling til tross for at dei innhenta og registrerte biometriske dataa blir sletta med ein gong innstemplingsprosessen er gjennomført.

2.4 Biometriske opplysningar – eit juridisk omgrep

Det andre rettspørsmålet etter art. 9 nr. 1 er om prosesseringa av fingeravtrykk utgjer ei behandling av *personopplysningar*. Omgrepet personopplysning er definert i art. 4 nr. 1 som seier at: «*enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. (…) ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, (…) identitet».* Bestemminga skildrar kven som er subjekt og mottakar av vern etter personvernforordninga; nemleg individ som kan identifiserast. Frasen «enhver opplysning om» tilseier at terskelen, som utgangspunkt, ligg lågt for å rekne informasjon om ein fysisk person for å vere personopplysningar.[31] Det gjeld likevel eit par aktuelle unntak. Eksempelvis er det ikkje korrekt, etter PVF, å snakke om behandling av personopplysningar dersom arbeidstakaren omkjem.[32]

Eit underspørsmål knytt til personopplysnings-omgrepet er om den registrerte er *identifiserbar* dersom fingeravtrykkmålingane blir gjort om til uleseleg digitale data. For å innfri vilkåret om å integrere tekniske personverntiltak, jf. PVF art. 25, er det blitt vanleg å la systemet automatisk gjere målingane om til digitale stringar. Arbeidsgjevar påstår gjerne at desse dataa ikkje lenger kan koplast til den tilsette og at dataa er gjort om til anonyme opplysningar som ikkje skal omfattast av PVF. Ettersom stringane framleis må koplast til eit register med detaljar om dei tilsette - for å registrere arbeidstida på desse - så er ikkje dataa anonyme, men pseudonymiserte. Dette vil seie at dei framleis kan brukast til å skildre den registrerte gjennom rett tilhøyrande informasjon. Pseudonymiserte data bidreg til å sikre personopplysningsvernet under behandlinga, men opplysningane fell, jf. fortalepunkt nr. 26, ikkje utanfor personvernforordninga sitt verkeområde.[33]

Personopplysningane skal tilleggsvis, jf. art. 9 nr. 1, omhandle «biometriske opplysninger». Omgrepet blir legaldefinert i PVF artikkel 4 nr. 14 som «*personopplysninger som stammer fra en særskilt teknisk*

[31] Jf. *Nowac* [C5], C-434/16, avsnitt 33 og 34.
Sjå også t.d. Jarbekk E. og Sommerfeldt S. *Personvern og GDPR i praksis*, (2019), side 42.
[32] Jf. PVF sitt fortalepunkt nr. 27 og Prop.56 LS (2017-18) side 26. NB. Unntaket gjeld likevel ikkje dersom opplysningane kan brukast til å identifisere andre, eksempelvis eit familiemedlem.
[33] Jf. PVF art. 4 nr. 5 for legaldefinisjonen på pseudonymisering.

behandling knyttet til en fysisk persons fysiske, fysiologiske eller atferdsmessige egenskaper, og som muliggjør eller bekrefter en entydig identifikasjon av nevnte fysiske person, f.eks. ansiktsbilder eller fingeravtrykksopplysninger». Legaldefinisjonen fremjar her tre underordna rettsspørsmål. Fyrst må arbeidsgjevar altså avklare om fingeravtrykkmålingar utgjer ein type *biometriske personopplysningar*. Dernest om dei biometriske opplysningane gjennomgår ei *særskilt teknisk handsaming*. Til sist må det takast stilling til om prosesseringa *mogleggjer eller bekreftar ein eintydig identifikasjon*.

Det fyrste underspørsmålet knytt til art. 4 nr. 14 er nettopp om fingeravtrykkregistrering utgjer biometriske opplysningar. Artikkelens ordlyd tilseier at biometriske opplysningar skal forståast som informasjon frå målingar om fysiske og personlege karakteristikkar ved individ - gjerne skildra som personlege kjenneteikn - som gjennom teknologiske prosessar kan brukast til å fastslå identitet. Biometrisk informasjon om personar er altså objektet ved behandlinga, og det fylgjer ordrett av føresegna at blant anna opplysningar om *fingeravtrykk* utgjer biometriske personopplysningar.

Det andre rettspørsmålet etter PVF art. 4 nr. 14 er kva som er meint med at det må skje ei *særskilt teknisk behandling* av fingeravtrykkopplysningane. Ei naturleg ordlydsfortolking av termen «særskilt teknisk» tilseier at regelen er avgrensa til databehandling som skjer ved tekniske prosessar, men ordlyden gjev ikkje haldepunkt for å fastslå nøyaktig kva tekniske prosessar som skal omfattast. Den abstrakte ordlyden kan forklarast gjennom forordningas målsetting om teknologinøytralitet.[34] Fungerande biometriske system består av eit sett med operasjonar som, samanfatta, gjer målingane av kroppslege kjenneteikn om til digitale modellar som kan brukast til å identifisere den registrerte. Vilkåret om ei særskild teknisk behandling vil dimed vere innfria så lenge dei aktuelle person-opplysningane blir prosesserte på eit vis som formar desse om til sånne identifiserande data.[35]

Det tredje vilkåret etter art. 4 nr. 14 omhandlar den eintydige identifikasjonen av arbeidstakaren. Tematisk kan dette tredje vilkåret koplast opp mot drøftingsemnet ved det tredje og siste vilkåret i artikkel 9 nr. 1. Behandlinga av desse to vilkåra er difor slått saman i neste punkt.

2.5 Eintydige identifikasjonar

Det siste rettspørsmålet PVF art. 4 nr. 14 reiser, er om fingeravtrykkregistreringa *mogleggjer* eller *bekreftar en eintydig identifikasjon*. Spørsmålet kan slåast saman med det siste kravet i PVF art. 9 nr. 1 om at behandlinga må ha som *siktemål å oppnå ein eintydig identifikasjon* av den registrerte.

[34] Jf. PVF fortalepunkt nr. 15.
[35] Jf. Jasserand, C. «Legal nature of biometric data: (…)», *European Data Protection Law Review*, (2016), s. 302-304.

Spørsmåla arbeidsgjevar må ta stilling til er altså for det fyrste, om føremålet og intensjonen med fingeravtrykkregistreringa er å eintydig identifisere den registrerte arbeidstakaren, jf. art. 9 nr. 1. Dernest må arbeidsgjevar avklare om det biometriske tidsregistreringssystemet, reint teknisk, anten er eigna til å mogleggjere- eller å bekrefte identifiseringa av den innstempla personen, jf. art. 4 nr. 14.

Det fyrste vilkåret - om at behandlinga har som siktemål å oppnå ei identifisering - reiser ikkje nemneverdige problem. Arbeidsgjevars intensjon med eit fingeravtrykkbasert tidsregistreringssystem vil alltid vere å identifisere individet som forsøker å stemple seg inn eller ut. Vilkåret i PVF art. 9 nr. 1 om at registreringa skal ha som føremål å oppnå ein eintydig identifikasjon vil dimed vere innfria.

Ved det andre rettspørsmålet - knytt til den tekniske mogleggjeringa eller bekreftinga av den eintydige identifikasjonen – kan ein fyrst slå fast at eit fingeravtrykkbasert tidsregistreringssystem som er meint å *identifisere* den registrerte arbeidstakaren vil innfri dette vilkåret i PVF art. 4 nr. 14.

Eit underspørsmål arbeidsgjevar dernest kan reise byggjer på ordlyden «eintydig identifikasjon». Den som gjer ei streng ordlydsfortolking vil kunne spørja seg om nemninga eintydig identifikasjon betyr at regelen kunn omhandlar identifikasjonsprosessar, samt om artikkelen dimed gjer ei avgrensing mot biometriske verifikasjonsprosessar. Distinksjonen er viktig ettersom biometriske tidsregistrerings-system kan bestå av ein innleiande identifikasjonsmetode som ikkje er basert på biometri - til dømes ved magnetiske id-kort, etterfylgt av ein biometrisk verifiseringsmetode. Meir nyansert er altså underspørsmålet om biometriske verifikasjonssystem fell utanfor ordlyden i art. 4 nr. 14?

Eit moment som talar for å forstå ordlyden som ei avgrensing mot verifisering kan byggje på at desse prosessane, i motsetning til identifikasjonsprosessar, ikkje krev eit vidtgåande registersøk. Verifiseringsprosessar inneberer derimot kunn å avvise eller akseptere det identifiserte individet. Resonnementet for denne fortolkinga er altså at verifikasjonsprosessar utgjer eit mindre personvern-inngrep enn identifikasjonsprosessar og fylgjeleg ikkje aktualiserer det same behovet for personopplysningsvern. Motsetningsvis kan ein samtidig poengtere at behandlinga vil opplevast like inngripande for den eller dei aktuelle registrerte arbeidstakarane, uavhengig av om systemet er identifiserande eller verifiserande. Dette poenget avgrensar betydninga av resonnementet over.

Vidare kan ein fortolke nemninga eintydig identifikasjon i kontekst av orda «mogleggjer» og «fastslå». Fyrstnemnde kan fortolkast som eit uttrykk for prosessar som mogleggjer eller avdekker individets identitet. Dette vil i så høve vere ein referanse til identifikasjonsprosessar. Dernest kan ordet *fastslå* fortolkast som eit uttrykk for prosessar som bekreftar at den registrerte matchar med ein gitt biometrisk profil. Denne fortolkinga vil innebere at verifikasjonsprosessar er inkludert i ordlyden til art. 4 nr. 14.[36] I forordningas fortalepunkt nr. 51 kan ein lese at biometriske prosessar

[36] Ibid., s. 304-306.

omhandlar både identifisering og «autentifisering» - eit synonym for verifisering. Med fortalen som bakteppe kan ein fylgjeleg legge til grunn denne fortolkinga av ordet *fastslå*.

Konklusjonen er fylgjeleg at både fingeravtrykkregistreringssystem som identifiserer og verifiserer verksemdas arbeidstakarar feller inn under ordlyden i PVF art. 4 nr. 14. Innfriinga av dette siste kravet knytt til PVF. art. 4 nr. 14 inneberer at system basert på verifiserande eller identifiserande fingeravtrykkregistrering medfører ei behandling av *biometriske opplysningar,* jf. PVF art 9 nr. 1.

Fingeravtrykkregistrering som ledd i eit system for arbeidstidsregistrering aktualiserer fylgjeleg *behandling* av *biometriske opplysningar* med *føremål om gjere ein eintydig identifikasjon.* Behandlingsforbodet i artikkel 9 nr. 1 gjer seg dimed, som alminneleg utgangspunkt, gjeldande for denne type behandlingsprosessar. Gjennom dei neste to kapitla kjem eg til å sjå nærare på kva som eventuelt skal til for at arbeidsgjevarar likevel unntaksvis kan ta i bruk fingeravtrykkregistrering.

3 Behandlingsprosessens innleiande kartleggingsfase

3.1 Vegen inn mot PVF art. 9 nr. 2

I føre kapittel avklarte me at tidsregistreringssystem basert på fingeravtrykkregistrering, som alminneleg utgangspunkt, er forbode. Dette behandlingsforbodet gjeld likevel ikkje utan unntak. Forordningas artikkel 9 nr. 2 bestemmer at nr. 1 «*ikke får anvendelse dersom et av følgende vilkår er oppfylt».* Føresegna presenterer dinest ei liste på ti punkt som alle gjer unntak frå det alminnelege behandlingsforbodet. Før me går i gang med drøftinga av vilkåra knytt til ein av desse unntaksreglane så må arbeidsgjevar gjere seg kjend med og avklare eit par overordna rettslege problemstillingar.

Kapitel 3 handlar altså primært om det essensielle grunnarbeidet som arbeidsgjevar må sikre før det i det heile er aktuelt å byrje på ei drøfting av unntaksvilkåra i artikkel 9 nr. 2 bokstav b. Neste punkt vil fylgjeleg ta opp dei mest grunnleggjande krava knytt til behandlingsprosessen. I punkt 3.3. kjem eg til å sjå nærare på arbeidsgjevars handlings- og informasjonsplikt og konsekvensar av å ikkje opptre i tråd denne plikta. Punkt 3.4. omhandlar avgjerande nasjonale tilleggsvilkår knytt til biometriske behandlingsprosessar. Det siste punktet i kapittel 3 byggjer så vidare på punkt 3.3. I dette siste punktet ser me nærare på unntaksregelen i PVF art. 9 nr. 2 bokstav a, samt på kvifor arbeidstakars samtykke ikkje burde brukast som særskild unntaksgrunnlag frå forbodet i PVF art. 9 nr. 1.

3.2 Alminneleg lovleg behandling

Behandlinga av særlege kategoriar personopplysningar skal, jf. forordningas fortalepunkt nr. 51, skje i tråd med forordningas alminnelege prinsipp og reglar. Fortalepunktet framhevar at dette er særs relevant angåande vilkåra om alminneleg lovleg behandling. Dette inneberer at det ekstra vernet om særleg kategoriserte personopplysningar, jf. art. 9 nr. 1, kjem i tillegg til forordningas generelle reglar.

Fylgjeleg må behandlinga, jf. art. 6 nr. 1, bygge på eit alminneleg behandlingsgrunnlag. Det fylgjer av PVF art. 6 nr. 1 bokstav b og c at behandlinga er lovleg i høve den er naudsynt for å innfri ein «*avtale»* som den registrerte er part i, eller dersom behandlinga er «nødvendig» *for å innfri ei rettsleg forplikting* knytt til arbeidsgjevar. Registrering av arbeidstid utgjer eit kontrolltiltak som verksemda definitivt har ei legitim interesse i å utføre.[37] I tillegg vil arbeidsavtalen typisk forplikte den tilsette til å arbeide innan eit gitt tidsrom eller over eit gitt tal timar. Arbeidsgjevar kan fylgjeleg anten grunngjeve

[37] Meir om dette i punkt 4.2.

behandlinga i *arbeidsavtalen* eller i ei eventuell *rettsleg forplikting* som gjer det *naudsynt* å drive den gitte timeregistreringa.[38] Påvisinga av eit alminneleg behandlingsgrunnlag byr altså ikkje på problem.

Prinsippet om føremålsavgrensing, jf. PVF art. 5 nr. 1 bokstav b, utgjer endå ein essensiell del av forordningas grunnleggjande prinsipp og kring behandlingas rettmessigheit. Den tilviste føresegna krev at arbeidsgjevar utformar «*spesifikke, uttrykkelig angitte og berettigede formål*» for behandlingsprosessen. Føremålsavgrensingsomsynets to overordna aspekt går ut på at den registrerte har krav på informasjon om kva føremål behandlinga skal realisere, samt dernest at arbeidsgjevar ikkje kan nytte prosessen for andre alternative føremål som ikkje er kome til uttrykk.[39] Prinsippet har stor betyding ettersom fingeravtrykkopplysningar kan brukast til ei rekke forskjellege føremål, eksempelvis å indirekte avdekke anna sensitiv informasjon om den registrerte.

3.3 Kartleggings- og informasjonsplikta

For å innfri handleplikta- og kravet om gjennomføre eigna «*organisatoriske tiltak»,* som sikrar effektiv gjennomføring av personvernprinsippa, jf. PVF art. 25, så burde arbeidsgjevar så tideleg som mogleg, avklare kva særskild unntaksgrunnlag han kjem til å aktualisere for potensielt å gjere den biometriske prosessen lovleg.[40] Biometrisk arbeidstidsregistrering vil typisk innebere omfattande og dagleg behandling av tilsette sine biometriske data, noko som medfører at arbeidsgjevar, jf. PVF art. 35 nr. 3, b, jf. nr. 4, er forplikta til å utforme ei personvernkonsekvensvurdering.[41] Vurderinga føreset at arbeidsgjevar, blant fleire viktige emne, tar stilling til båe behandlingsgrunnlaget og særlege unntaksgrunnlag.

Personvernomsynet om openheit, heimla i PVF art. 5 nr. 1 bokstav a, utgjer endå ein faktor som spelar inn på dette innleiande kartleggingsarbeidet. For den registrerte har openheitsomsynet krystallisert seg som ein innsynsrett, jf. PVF art. 12 nr. 1, jf. art. 13 nr. 1 bokstav c. Innsynsretten skal sikre at han eller ho får sjansen til å ivareta sine rettar og interesser under behandlingsprosessen, eksempelvis ved å avklare om behandlinga er rettmessig. Informasjon om behandlinga skal vere enkel å oppdrive og utforma på eit vis som gjer det lett for arbeidstakaren å få innsikt i kva

[38] Jf. Blekstad og Hirst, *Personvern og kontroll i arbeidslivet* (2021), side 357.
[39] Jf. PVF fortalepunkt nr. 39.
[40] Merk at kartlegginsplikta kunn utgjer ein avgrensa del av handleplikta etter art. 25 om innebygd personvern.
[41] Jf. Datatilsynet, *Vurdering av personvernkonsekvensar (DPIA) – (…),* (sist endra 27.07.23), kulepunkt 2 og 5 om biometriske data og om monitorering av tilsette, URL: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdering-av-personvernkonsekvenser/nar-ma-man-gjennomfore-en-vurdering-av-personvernkonsekvenser/, (lese 24.10.23).

behandlinga går ut på, korleis denne blir gjennomført og omfanget av dei behandla opplysningane.[42] For arbeidsgjevar utgjer arbeidstakars innsynsrett dimed ei forplikting om å kartlegge- og informere dei tilsette om behandlingsprosessen, samt der i blant om behandlingas rettslege grunnlag.[43]

I høve arbeidsgjevar ikkje innfrir forpliktinga om å informere dei registrerte om behandlings-prosessen så kan verksemda sanksjonerast av datatilsynsmyndigheitene. Dette var tilfelle i ei spansk tilsynssak om eit byråd som dreiv fingeravtrykkregistrering på administrasjonens tilsette.[44] Det spanske datatilsynet kommenterte at biometriske tidsregistreringssystem etter omstenda kan brukast, sjølv om dei sjeldan burde vere det einaste aktive identifikasjonssystemet. Tilsynet fant at Byrådet ikkje hadde informert dei tilsette om behandlingsprosessen; sjølv ikkje etter at ein av dei tilsette fremja ein skriftleg førespurnad om informasjon knytt til fingeravtrykkregistreringa. Datatilsynet skreiv det fylgjande om informasjonsplikta: «*it must be noted that the implementation and integration of a fingerprint-based time control system by the employer must be informed to the employees in a complete, clear manner., concise and, in addition, the aforementioned information must be completed with reference to both the legal bases that cover said type of access control, as well as the basic information referred to in article 13 of the [PVF]».* Ettersom byrådet ikkje opptredde i tråd med den omtala forpliktinga vart det sanksjonert med ei åtvaring knytt til peronvernbrotet. Tilsynssaka framhevar at eit totalt fråvær av informasjon- og manglande oppfylging av innsyns-førespurnader ganske opplagt strir med openheitskravet.

Tilsvarande vil arbeidsgjevar kunne sanksjonerast for å tilby arbeidstakarane mangelfull- eller feil informasjon. I den tidlegare tilviste Sportitalia-saka frå 2022 vart arbeidsgjevar bøtlagd for å ikkje ha eit legitimt behandlingsgrunnlag for fingeravtrykkregistreringa. SportItalia pretenderte å ha tilbode dei 132 tilsette tilstrekkeleg informasjon om prosjektet og å ha henta inn uttrykkelege samtykker som grunnlag for behandlinga. Tilsynsmyndigheita avklarte at dette ikkje var tilfelle. Derimot fant det italienske datatilsynet at Sportitalia kunn hadde utforma eit kort avsnitt om behandlingsprosessen i eit dokument knytt til tilsetjingsforholdet. Det vart også avdekka at selskapet hadde unnlate å nemne dei biometriske prosessane i verksemdas gjeldande dokument om aktive behandlingsaktivitetar.

Ein legitim biometriske behandlingsprosess vil fylgjeleg ikkje berre bygge på behandlingsgrunnlaget og på eit potensielt særskilt unntaksgrunnlag. Arbeidsgjevar skal derimot også opptre i tråd med

[42] Jf. PVF fortalepunkt nr. 39
[43] Spiecker gen. Dohman, med fleire, *Genereal Data Protection Regulation (…)*, 2023, side 269.
[44] Jf. Det Spanske Datatilsynet (AEPD), *RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR*, nasjonalt saksnr.: PS/00128/2020, URL: https://www.aepd.es/documento/ps-00128-2020.pdf, (lese: 07.11.23). Merk at dokumentet kunn er publisert på originalspråket.

handleplikta, samt ei kvar annan personvernrettsleg forplikting. Dette vil vere særs viktig ettersom fingeravtrykkregistreringa medfører ein betydeleg personvernrisiko for dei tilsette.

3.4 Den norske særregelen om eintydig identifikasjon

Personvernforordningas art. 9 nr. 4 opnar for at nasjonale myndigheiter kan «*opprettholde eller innføre ytterligere vilkår, herunder begrensninger»,* relatert til behandlinga av blant anna «*biometriske opplysninger».* Utover dette bestemmer PVF art. 87 at myndigheitene òg kan opprette «*nærmere særlige vilkår»* for behandlinga av «*generelle identifikatorerer»* m.m., dersom desse identifikatorane blir brukt saman med «*nødvendige garantier for den registrertes rettigheter og friheter».* Nemninga *generelle identifikatorar* visar eksempelvis til biometriske modalitetar som fingeravtrykk, gongelag, irisregistrering, m.m.[45] Dei to føresegnene gjev altså medlemsland handlingsrom til å presisere og skjerpe vilkåra knytt til behandlinga av biometriske opplysningar. Ordlyden av nemningane *oppretthalde, ytterlegare vilkår, avgrensingar* og *nærare særlege vilkår* tilseier at reglane kunn opnar for å skjerpe vilkåra som gjeld for behandling av biometriske data.

Noreg har nytta dette nasjonale handlingsrommet til å bringe dagens pol. § 12 - om bruk av fødselsnummer og andre eintydige identifikasjonsmidlar - vidare frå personopplysningslova av 2000. Føresegna bestemmer at «*Fødselsnummer og andre entydige identifikasjonsmidler»* berre kan behandlast i høve det er eit «*saklig behov for sikker identifisering»* og om prosessen er «*nødvendig for å oppnå slik identifisering».* Som nemnd i føre avsnitt omhandlar termen *generelle identifikatorar* blant anna fingeravtrykkregistrering.[46] Den norske føresegna gjeld altså òg behandling av biometriske opplysningar og fungerer som eit supplement til regelverket som fylgjer av personvernforordninga.[47] Dei to rettsspørsmåla me står att med er altså om behandlingsporsessen er sakleg og naudsynt.

Det fyrste vilkåret arbeidsgjevarar må ta stilling til etter pol. § 12 er om behovet for å bruke det biometriske tidsregistreringssystemet er *sakleg*. Den som kan aktualisere ei rettsleg forplikting som føreset at verksemda skal drive arbeidsrettsleg timeregistring, vil kunne argumentere for at behandlingsprosessen er sakleg i kraft av å etterfylgje den rettslege forpliktinga.[48] Arbeidsrettsleg timeregistrering skal tross alt, blant anna, medverke til offentleg tilsynsarbeid i arbeidslivet, og den

[45] Jf. Skullerud, mfl., *Personopplysningsloven og Personvernforordningen (GDPR) – (...)*, (2019), side 475.
[46] Jf. Ibid., side 79-80.
[47] Sjå eksempelvis Prop.56 LS (2017-18), side 216.
[48] Meir om rettslege forpliktingar i kapitel 4.

som legger til grunn at prosesseringa er til fordel for offentleg verksemd vil typisk ha eit godt utgangspunkt ved saklegheitsdrøftinga.[49]

Det andre vilkåret omhandlar *naudsynet* av å bruke nettopp fingeravtrykkregistring for å innfri det saklege behovet om føre timeregistrering. Vilkåret er ikkje nyansert i dagens førarbeid, men desse visar derimot til førarbeida for den originale føresegna av personopplysningslova av 2000, jf. Prop.56 LS (2017-18), side 215, jf. Ot.prp.nr.92 (1998-99), side 114. Desse eldre førarbeida legg til grunn at «*Kravet til nødvendighet i første ledd vil bare være oppfylt dersom andre og mindre sikre identifikasjonsmidler, som f.eks navn, adresse og kundenummer ikke er tilstrekkelig».* I tillegg vil det vere av betydning «*hvor viktig sikker identifisering er for den registrerte, dvs hvilke konsekvenser en forveksling kan føre til. Også samfunnets behov kan tillegges vekt*». Vilkåret legg fylgjeleg opp til ei drøfting av om det eksistere mindre inngripande metodar og dernest ei interessedrøfting sett mellom verksemdas og samfunnets behov, sett opp mot den registrerte sine personverninteresser.

Naudsynsdrøftinga feller i stor grad saman med naudsynsvilkåret i PVF art. 9 nr. 2 bokstav b. Ettersom denne oppgåva tar utgangspunkt i personvernforordninga så er den vidare utgreiinga av naudsynskravet i pol. § 12 ikkje utbrodert vidare. I staden blir naudsynsvilkåret, basert på PVF art. 9 nr. 2 bokstav b, behandla i detalj i kapittel 4. Avslutningsvis burde arbeidsgjevar vel å merke vere seg obs på at vilkåra i pol. § 12 gjelder i tillegg til forordningas reglar og supplerer det europeiske personopplysningsvernet etter personvernforordninga.

3.5 Problemstillinga knytt til arbeidstakars samtykke

Som nemnd fastsett PVF art. 9 nr. 2 ti unntaksføresegner og mi hovudproblemstilling rettar seg primært mot artikkelens bokstav b. Men ein kan vel å merke anta at dei to mest aktuelle unntaks-grunnlaga for arbeidsgjevarar som søkjer å drive biometrisk tidsregistrering båe er bokstav a og b. Ettersom det i praksis har vist seg at arbeidsgjevar i ei rekke saker har søkt å bruke arbeidstakars samtykke som unntaksgrunnlag så kjem eg òg til å gjere ei utgreiing kring art. 9 nr. 2 bokstav a.

Artikkel 9 nr. 2 bokstav a går ut på å vere i overeinskomst med den registrerte om behandlinga. Føresegna lyd: «*Den registrerte har gitt uttrykkelig samtykke til behandling av slike person-opplysninger for ett eller flere spesifikke formål, unntatt dersom det i unionsretten eller medlems-statenes nasjonale rett er fastsatt at den registrerte ikke kan oppheve forbudet nevnt i nr. 1*». Føresegnas avgjerande vilkår og rettsspørsmål er om det er gjeve eit kvalifisert *uttrykkeleg samtykke.*

[49] Jf. Skullerud, mfl., *Personopplysningsloven og Personvernforordningen (GDPR) – (…)*, (2019), side 80-81

Nemninga er ikkje legaldefinert, men eit alminneleg samtykke skal, jf. PVF art. 4 nr. 1 punkt 11, vere ei «*frivillig, spesifikk, informert og utvetydig viljesytring*» som bekreftar at den registrerte samtykker til den gitte behandlinga. Fortalen nyanserer at eit samtykke ikkje er valid i høve den registrerte mangla reell valfridom, eller dersom han ville risikere represaliar i høve han avslo samtykke-førespurnaden.[50] I relasjon til arbeidstakars samtykke er det nettopp vilkåret om frivilligheit som typisk byr på problem. Spørsmålet vidare er dimed om og når arbeidstakars samtykke er *frivillig*.

Dei tilviste fortalepunkta i PVF, nr. 42 og 43, utbroderer at vilkåret om frivilligheit ikkje er innfria i høve den registrerte mangla «*reell valgfrihet, eller ikke er i stand til å nekte å gi eller trekke tilbake et samtykke uten at det er til skade for vedkommende*». Her skisserer fortalen at i høve den behandlingsansvarlege er overordna den registrerte, så talar dette omstende mot å rekne samtykke til behandlinga for å vere frivillig gitt. Tilsetjingsforhold utgjer vel å merke, som me diskuterte i kapittel 2, ein maktrelasjon der den registrerte er underordna den behandlingsansvarlege. Fortalepunkta peikar med dette i retning av at arbeidsrettslege behandlingssamtykke ikkje er greitt.

Problemstillinga kring frivilligheit er dinest tatt opp av Det Europeiske Databeskyttelsesråd (EDPS) som har presisert at det kunn i unntakstilfelle er aktuelt å rekne eit samtykke til databehandling som frivillig i tilsetjingsforhold.[51] I det tilviste dokumentet skriv EDPS at det avgjerande kriteriet kring frivilligheitsvurderinga i tilsetjingsforhold er om arbeidstakaren hadde grunn til å frykte ein eller annan form for negative konsekvensar av å avslå førespurnaden, og om han dermed kjende seg pressa til å samtykke. I eit sånt tilhøve vil ikkje frivilligheitsvilkåret vere innfria, uavhengig av om risikoen var reell eller ikkje. Rådet konkluderer fylgjeleg med at det, i alminnelegheit, sjeldan er aktuelt å akseptere arbeidstakars samtykke som eit legitimt alminneleg behandlingsgrunnlag.[52]

Vidare utforma også Europarådet eit sett med anbefalingar i 2015 som, blant anna, rettar seg særskilt mot behandling av biometriske persondata i tilsetjingsforhold.[53] Det fylgjer av dokumentet at «*The collection and further processing of biometric data should only be undertaken when it is necessary to protect the legitimate interests of employers, employees or third parties, only if there are no other less intrusive means available and only if accompanied by appropriate safeguards, including the additional safeguards provided for in principle 21*». Utsegna synar at behandlinga av biometriske opplysningar aktualiserte eit krav om naudsemd og proporsjonalitet også før biometriske person-

[50] Jf. 1) fortalepunkt nr. 42 siste setning, og
2) fortalepunkt 32 og 43 om krava til samtykke.
[51] Det Europeiske Datatilsynet, *Guidelines 05/2020 on Consent (…),* (2020*)*, side 9.
[52] Jf. 1) Ibid. og
2) Artikkel-29 gruppa (Personvernrådets forgjenger), *Opinion 2/2017 (…)*, side 6-7.
[53] Jf. Europarådet, *Recommendation CM/Rec (2015) 5 (…)*, del 2, punkt 18.
Merk at også dette dokumentet vart utforma i ljos av Personverndirektivet.

opplysningar fekk formelt vern gjennom dagens personvernforordning. Ettersom Europarådet seinast i 2015 formulerte dette utgangspunktet om at biometrisk databehandling skal bygje på ei naudsyns-vurdering så kan ein anta at den same tilnærminga framleis er den mest aktuelle, også etter at personvernforordninga tredde i kraft.

I saka PVN-2006-10, med tilvising til PVN-2006-7 og PVN-2005-6, tok den norske Personvernnemnda stilling til spørsmålet om arbeidstakars samtykke, knytt til fingeravtrykkregistrering. Saka omhandla ESSO Norge som implementerte eit internt tilråda, men valfritt, biometrisk tilgangssystem som auka sikringa inn til arbeidsplassens tankanlegg. I forkant av behandlinga vart arbeidstakarane godt informerte om prosessen, dei vart lært opp i korleis systemet verka, dei fekk ein spesielt utforma samtykkeerklæring og ikkje minst kunne dei, utan fare for negative konsekvensar, velja eit alternativt system, basert på PIN-kodar og nøkkelkort. Personvernnemnda la til grunn same utgangspunkt som dagens regelverk: dei føresette at arbeidstakarars samtykke som hovudregel ikkje er eit passande behandlingsgrunnlag. Likevel kom nemnda til at saksomstenda spegla ein behandlingsprosess som bar preg av tilstrekkeleg reell frivilligheit, og konkluderte fylgjeleg med at samtykket var akseptabelt.

Ein kan stille spørsmålsteikn ved om vedtaket hadde fått gjennomslag i dag.[54] Nemnda kommenterer i vedtaket at dei registrerte arbeidstakarane ikkje risikerte negative konsekvensar, men samtidig kan ein lese at ESSO primært ynskja at arbeidstakarane skulle velja vekk PIN-kodesystemet. Me veit ikkje korleis dette ynsket vart presentert ovanfor dei tilsette, men det utgjer i alle høve ein implikasjon om at ESSO hadde ein preferanse mellom dei to alternative systema. Ein sånn preferanse er etter omstenda eigna til å reise tvil kring frivilligheitsvilkåret, ettersom tilsette som kjenner til at ei løysing fell saman med selskapets interesser - samt at den andre løysinga ikkje samsvarer med desse interessene - vil kunne frykte at han setter seg sjølv opp mot arbeidsgjevar dersom han ikkje vel det føretrekte alternativet. Ettersom samtykke, som utgangspunkt, uansett ikkje utgjer eit akseptabelt behandlingsgrunnlag, så burde arbeisgjevar helst søke å rettferdiggjere behandlingsprosessen gjennom eit anna rettsgrunnlag.

Resonnementet er etter dette at ein framleis helst burde aktualisere ei unntaksføresegn som speglar prinsippa om naudsemd og proporsjonalitet. Noreg har vel å merke ein særregel som stadfestar eit alminneleg krav om saklegheit og proporsjonalitet, jf. pol. § 12. Til tross for at desse tilleggsvilkåra garanterer arbeidstakarane eit ekstra vern så burde arbeidsgjevar, av omsyn til dei tilsette, unngå behandlingsgrunnlag som er eigna til å plassere desse i ein pressa situasjon. I alle høve medfører

[54] Her kan ein særs sjå tilbake til fortalen til PVF og EDPS sine retningslinjer frå 05/2020.

overordnaforholdet at vilkåret om frivilligheit sjeldan er innfria; dimed talar også behovet for klarheit rundt prosessen for at behandlinga burde baserast på eit anna unntaksgrunnlag enn samtykke.

4 PVF art. 9 nr. 2 bokstav b

4.1 Ordlyd

Personvernforordningas artikkel 9 nr. 2 bokstav b gjer unntak frå behandlingsforbodet når: «*Behandlingen er nødvendig for at den behandlingsansvarlige eller den registrerte skal kunne oppfylle sine forpliktelser og utøve sine særlige rettigheter på området arbeidsrett, trygderett og sosialrett i den grad dette er tillatt i henhold til unionsretten eller medlemsstatenes nasjonale rett, eller en tariffavtale i henhold til medlemsstatenes nasjonale rett som gir nødvendige garantier for den registrertes grunnleggende rettigheter og interesser.»* Artikkelens ordlyd - utforma som éi lang og litt innvikla setning - er tung å lese. Broten opp krev regelen for det fyrste at arbeidsgjevar opptrer i tråd med ei arbeidsrettsleg *forplikting.* For det andre skal denne plikta vere supplert med *naudsynte garantiar* som sikrar den registrerte arbeidstakaren sine grunnleggjande rettar og interesser. Til sist er det kravd at den gitte behandlingsprosessen må vere *nødvendig* for å innfri den rettslege forpliktinga.

Krava er kumulative og unntaksføresegna kjem dimed ikkje til bruk med mindre kvart vilkår er innfria. Gjennom kapittel 4 kjem eg fylgjeleg til å vurdere i kva grad arbeidsgjevarar kan ta i bruk denne unntaksbestemminga for å gjennomføre den arbeidsrettslege tidsregisregistreringa med eit system basert på fingeravtrykkregistrering. Vilkåra er behandla i tur, så som dei vart presentert i føre avsnitt.

4.2 Vilkåret om ytterlegare rettslege grunnlag

Artikkel 9 nr. 2 bokstav b utgjer ikkje ei isolert unntaksbestemming, ordlyden føreset derimot at regelen er supplert gjennom anten unionsretten, nasjonal lovgjeving eller ved tariffavtale. Ein kan seie at unntaksføresegna må aktiverast gjennom andre reglar og at dette supplementet skal fastsette ein rett eller ei forplikting ovanfor arbeidsgjevar eller arbeidstakar.[55] Spørsmålet arbeidsgjevar må ta stilling til er fylgjeleg om det eksisterer eit passande rettsgrunnlag som etablerer ei forplikting om å føre tidsregistrering, samt om plikta opnar for behandling av biometriske personopplysningar.

Ei eventuell forplikting om å registrere arbeidstid vil høyre til arbeidsrettens område. I Noreg har lovgjevar utforma ei generell føresegn, jf. pol. § 6, om behandlinga av særlege kategoriar av personopplysningar i arbeidsforhold. Det fylgjer av denne at *«Personopplysninger som nevnt i personvernforordningen artikkel 9 nr. 1 kan behandles når det er nødvendig for å gjennomføre arbeidsrettslige*

[55] Jf. Prop.56 LS (2017-18), side 40.

plikter eller rettigheter». Føresegna har sitt rettslege utgangspunkt i båe PVF art. 9 nr. 4 og art. 88. Desse to tilviste artikkalen opnar for nasjonal regulering og vern om *«rettigheter og friheter ved behandling av arbeidstakeres personopplysninger*». Personopplysningslova § 6 utgjer ikkje ein sjølvstendig regel, og den fastset heller ikkje konkrete rettar eller plikter. Det er dimed noko usikkert eksakt kva praktisk verdi denne føresegna har.[56] I alle høve bidreg regelen til å framheve naudsynskravet, som også fylgjer av forordningas art. 9 nr. 2 bokstav b.

I Noreg er det utforma reglar om arbeidstidsregistrering i arbeidsmiljølova av 2005 (heretter aml.). Lovens kapittel 10, jf. § 10-7, bestemmer at arbeidsgjevar er forplikta til å syte for at det blir ført ei «*oversikt som viser hvor mye den enkelte arbeidstaker har arbeidet. Oversikten skal være tilgjengelig for Arbeidstilsynet og arbeidstakerenes tillitsvalgte».* Regelen forpliktar altså ein kvar arbeidsgjevar til å implementere eit system som held oversikt over når og kor lenge den enkelte arbeidstakar jobbar. Vidare kan ein lese i lovens førarbeid, jf. Ot.prp.nr.49 (2004-05) side 320, at føremålet med denne forpliktinga er å sikre arbeidsgjevar ei intern oversikt over kva arbeidstakarane har krav på. I tillegg nyanserer førarbeida at oversikta skal bidra til arbeidet tilsynsmyndigheitene gjer for å kontrollere om næringsdrivande fylgjer regelverket knytt til arbeidstid, derunder om dei tilsette blir tildelt rett ferie, fri, permisjon osv. Vilkåret om ei arbeidsrettsleg forplikting om å drive tidsregistrering er fylgjeleg, som utgangspunkt, innfria for ein kvar arbeidsgjevar som er underlagt norsk lovverk.

I forlenging av den rettslege analysen av aml. § 10-7 kan ein presisere at regelen er teknologinøytral. Med dette meiner eg at regelen ikkje spesifiserer korleis den tekniske gjennomføringa skal føregå. Eit interessant underspørsmål er dimed om regelen likevel ikkje er presis nok til å innfri vilkåret i om at det biometriske systemet skal imøtekome ei arbeidsrettsleg plikt. Med andre ord må arbeidsgjevar avklare om plikta skal bygge på ein heimel som presiserer at biometriske data kan behandlast.

Det fylgjer av PVF art. 9 nr. 2 bokstav b at arbeidsgjevar berre kan gjennomføre behandlinga i høve dette er naudsynt for å innfri arbeidsrettslege *forpliktingar* m.m. Ordlyden er generell og seier ikkje noko om korleis forpliktinga skal innfriast. Forordningas fortalepunkt nr. 45 nyanserer at det ikkje er kravd ei særskild lovbestemming for kvar enkelt behandling som skal innfri ei forplikting. Vidare fylgjer det av fortalepunktets femte punktum at det rettslege grunnlaget «*kan»* presisere allmenne vilkår; så som kva typar personopplysningar som skal behandlast. Ordet *kan* synar at dette er valfritt, noko som talar for at den rettslege forpliktinga også kan vere teknologinøytral.

Problemstillinga kom opp for Tysklands regionale arbeidsrettsdomstol Berlin-Brandenburg.[57]

---

[56] Jf. Skullerud, mfl., *Personopplysningsloven og Personvernforordningen (GDPR) – (...)*, (2019), side 61.
[57] Jf. databasen: Berlin.de – Vorschriften- und Rechtsprechungsdatenbank, nasjonalt saksnummer er: 10 Sat 2130/19, URL: https://gesetze.berlin.de/bsbe/document/JURE200011045/part/K (lese 27.10.23).

Ankesaka, datert den 04.06.20, omhandla rettmessigheita kring tre arbeidsrettslege åtvaringar. Åtvaringane gjekk ut på at den tilsette, ein radiologiske teknikar, var forplikta til å bruke verksemdas nye biometriske system for registrering av arbeidstid. Retten tok stilling til om sjølve behandlinga var lovleg sett i kontekst av PVF art. 9 nr. 2 bokstav b. I relasjon til vilkåret om å etterkome ytterlegare rettsleg regulering, samt derav ei forplikting om å føre arbeidsrettsleg tidsregistrering, kommenterte domstolen at den radiologiske avdelinga opptredde i tråd med eit sånt kvalifiserande rettsgrunnlag. Forpliktinga fylgde av EU sitt Arbeidstidsdirektiv frå 2003 og frå EU-pakta om grunnleggjande rettar art. 31. Til tross for at forpliktingane ikkje nyanserte presis korleis tidsregistreringa reint teknisk skulle føregå fant retten at desse innfridde vilkåret i PVF art. 9 nr. 2 bokstav b.[58] Standpunktet i den tyske saka er dimed at den arbeidsrettslege forpliktinga kan vere teknologinøytral.

I den spanske byråd-saka frå 2021 kom dei nasjonale datatilsynsmyndigheitene til det som tilsynelatande var same konklusjon. I vedtaket utforma tilsynsmyndigheita ei åtvaring mot byrådet for ikkje å ha innfria handlings- og informasjonsplikta si i tråd med PVF art. 13. Kring vilkåret i PVF art. 9 nr. 2 bokstav b - om ytterlegare regulering - skriv myndigheita, med tilvising til spansk arbeidsrett, at: «*The possibility of using systems based on biometric data to carry out access and time control is undeniable (…)».* Tilsynet kommenterte vidare at alternative system også kunne brukast og ville vere minst like effektive med tanke på å innfri tidsregistreringsplikta.[59] Med andre ord kom også denne myndigheita til at plikta kan bygge på ei teknologinøytral føresegn.

Med utgangspunkt i forordningas fortale og med tilvising til dei to europeiske sakene kan ein fylgjeleg legge til grunn utgangspunktet over om at vilkåret om ytterlegare regulering – i form av ei forplikting om å føre eit arbeidstidsregister - er innfria gjennom arbeidsmiljølova § 10-7, til tross for at denne ikkje presiserer om det er åtgang til bruke eit fingeravtrykkbasert tidsregistreringssystem.

Ein kan nemne at det i tillegg til den generelle regelen i aml. § 10-7 også eksisterer spesifikk bransjeavhengig regulering. Eksempelvis er byggherrar, jf. byggherreforskrifta av 2009 § 15, forplikta til å føre digitale oversiktlister over kven som til ei kvar tid oppheld seg på bygg- og anleggsplassar. Forskriftas § 15 bestemmer at føremålet med forpliktinga er å bidra til «arbeidet med sikkerhet, helse og arbeidsmiljø». Sikkerheitsomsyn er altså eit ekstra viktig omsyn på bygg- og anleggsområdet og kan potensielt spele inn på korleis behandlingsprosessen best let seg gjennomføre. Omsynet til sikkerheit kan eksempelvis utgjere eit argument for at byggherren har eit særskild behov for eit tidsregistreringssystem som er ekstra presis. Fylgjeleg vil spesialreglar, så som i byggherreforskrifta, kunne bygge på ekstraordinære siktemål og samfunnsmessige behov som modifisere forventningane

[58] Jf. dommens avsnitt 57-61.
[59] For kvoteringa og utsegna om spansk arbeidstett, jamfør side 8.

til den tekniske gjennomføringa av behandlingsprosessen. Ein sånn modifikasjon vil vere av interesse ved vurderinga av om fingeravtrykkregistrering er naudsynt for å innfri den aktuelle forpliktinga.

4.3 Vilkåret om naudsynte garantiar

Det andre drøftingsemnet i PVF art. 9 nr. 2 bokstav b er om den ytterlegare reguleringa i tilstrekkeleg grad «*gir nødvendige garantier for den registrertes grunnleggende rettigheter og interesser».* Spørsmålet ein her må ta stilling til er om det finns rettslege sikkerheitsventilar knytt til behandlinga.

I norsk rett må arbeidsgjevar ta stilling til arbeidsmiljølova § 9-1, som avgrensar åtgangen til å sette i verk kontrolltiltak. Føresegnas fyrste ledd bestemmer at «*kontrolltiltak»* berre kan implementerast ovanfor arbeidstakarane i høve tiltaket byggjer på ein «*saklig grunn i virksomhetens forhold»,* samt dersom tiltaket ikkje leier til ein «*uforholdsmessig belastning for arbeidstakeren*». Regelen fremjar med dette tre rettsspørsmål, og det fyrste er om fingeravtrykkregistreringa utgjer eit kontrolltiltak. Ordlyden av «kontrolltiltak» er vid, dette tilseier at det skal lite til for å rekne eit overvakande system som eit kontrolltiltak. Vidare avklarar førarbeida at tidsregistrering utgjer ein type kontrolltiltak.[60] Dernest opnar vilkåra om saklegheit og forholdsmessigheit for meir inngåande rettslege drøftingar.

Det andre rettspørsmålet er altså om fingeravtrykkregistreringa byggjer på ei *sakleg grunngjeving*. Føresegnas ordlyd tilseier at fingeravtrykkregistreringa skal byggje på eit legitimt føremål, samt at den tekniske gjennomføringa at tiltaket skjer på eit måte som er forsvarleg i relasjon til dette føremålet.[61] Ein kan her trekke parallellar til vilkåra i PVF art. 9 nr. 2 bokstav b om at behandlinga skal bygge på ei arbeidsrettsleg forplikting, samt til det norske vilkåret i pol. § 12, fyrste ledd, om at biometriske prosessar berre skal implementerast når desse byggjer på eit sakleg behov. Det er vidare ikkje sagt at kontrolltiltaket, som byggjer på ei rettsleg forplikting om å registrere arbeidstid, automatisk er sakleg. Dersom arbeidsgjevar implementerer eit meir inngripande system enn det som strengt tatt er behov for så kan ein så tvil av om kontrolltiltakets gjennomføring er sakleg. Med andre ord har vilkåret også ein dimensjon mot naudsyns- og proporsjonalitetsvurderinga som er behandla i tekstens neste punkt.

Det tredje rettspørsmålet etter aml. § 9-1 omhandlar innverknaden fingeravtrykkregistreringa har ovanfor dei registrerte arbeidstakarane. At tiltaket ikkje skal vere *uforholdsmessig* tilseier at det må gjerast ei proporsjonalitetsvurdering av tiltakets innverknad, sett opp mot arbeidsgjevar sitt behov for å gjere fingeravtrykkregistreringa.[62] Lovførearbeida utbroderer, jf. Ot.prp.nr. 49 (2004-05), side 145, at

[60] Jf. Ot.prp. nr. 49 (2004-05), side 135.
[61] Ordlydsfortolkinga kan støttas opp gjennom førarbeida, sjå ibid. Side 144.
[62] Jf. Ibid. Side 145.

i høve kontrolltiltaket leier til eit: «*ikke ubetydelig inngrep i rettsgoder som personlig integritet, verdighet, privatlivets fred, legemets ukrenkelighet eller lignende*», så vil ein berre unntaksvis få medhald i at inngrepet er proporsjonalt. Vidare kan ein lese at det derimot skal mykje til før «*mer tradisjonelle kontrolltiltak i arbeidslivet som for eksempel tidsregistrering, (…) osv., vil bli ansett som uforholdsmessig*». Dersom ein les denne siste utsegna i kontekst av utgreiinga over, så kan ein legge til grunn at presumpsjonsstandpunktet kunn omhandlar tradisjonelle og anerkjente tidsregistrerings-metodar. Ettersom fingeravtrykkregistrering derimot, i betydeleg grad, går utover den registrerte sin personlege integritet og privatsfære så tilseier førearbeida at denne typen tidsregistreringssystem berre unntaksvis er akseptable. Forholdsmessigheitsvilkåret leiar arbeidsgjevar inn i ei heilt sentral interessevurdering som, igjen, blir behandla i nærare detalj under.

Dei siste to avsnitta, kring saklegheitsvilkåret og forholdsmessigheitsvilkåret, er kort behandla til tross for at vilkåra presenterer interessante problemstillingar. Nedprioriteringa har samanheng med at denne oppgåva primært er retta mot personvernreglane i PVF. Som ein kan lese av aml. § 9-1, andre ledd, er åtgangen til å iverksette kontrolltiltak også avgrensa direkte gjennom personopplysningslova. Arbeidstakarane som kjem til at personverregelverket ikkje tilbyr tilstrekkeleg vern kan likevel aktualisere fyrste ledd i aml. § 9-1, for potensielt å oppnå eit betre resultat etter denne føresegna.

Vilkåret om naudsynte garantiar for den registrerte sine grunnleggjande rettar og friheiter er med dette innfria gjennom aml. § 9-1.

4.4 Vilkåret om naudsemd

Det tredje drøftingsemnet i artikkel 9 nr. 2 bokstav b, er om - og i så høve når - det er naudsynt å behandle biometriske opplysningar for å innfri den arbeidsrettslege forpliktinga om å registrere arbeidstid. At behandlinga må vere *naudsynt* tilseier, etter ei alminneleg ordlydstolking at behandlinga berre er akseptabel i høve behandlingsføremålet ikkje kan innfriast på ein betre måte.[63] Med andre ord er naudsynskravet ein ventil som sikrar at berre inngrepa som leier til den minste personvernkrenkinga ein kan forvente er rettmessige.[64] For å ta stilling til naudsynsvilkåret må den behandlingsansvarlege dimed gjere eit godt stykke førarbeid med å utforske kva alternative system

[63] Sjå også fortalepunkt nr. 39, 4. punktum frå botn av fortalepunktet.
[64] Jf. Spiecker gen. Dohmann, m.fl., (2023), side 272, avsnitt 49.

denne har tilgang til.[65] I høve det finns alternative og fullgode tidsregistreringssystem, som i mindre grad råkar arbeidstakars personverninteresser, så er ikkje fingeravtrykkregistreringa naudsynt.

Det fyrste spørsmålet eg tek stilling til er fylgjeleg kor eigna eit biometriske system må vere for å innfri artikkelens vilkår. Jussprofessor Dag Wiese Schartum argumenterer for at naudsynsomgrepet, i alminnelegheit, skal fortolkast som eit kraftfullt uttrykk som synar at det er knytt strenge krav til drøftinga. Dersom det eksisterer alternative og mindre inngripande prosessar så skal desse omtrent alltid veljast. Han føresett likevel ikkje at den aktuelle prosessen må vere absolutt naudsynt, men at ordlyden derimot tilseier at eit kvalifisert naudsyn, i prosent, vil ligge på mellom 80-100%.[66]

Ein kan sjå den høge terskelen som ei klar spegling av omsynet om å verne om det registrerte individets personverninteresser. Å bruke biometri mot verksemdas tilsette utan at behandlinga er naudsynt vil ikkje berre utgjere eit uforsvarleg inngrep mot dei registrerte sitt personvern, men er også ein sosialt forkasteleg bruk av makt og arbeidsrettsleg styringsrett.

I ei tilsynssak la Det Europeiske Datatilsynet til grunn eit standpunkt om biometrisk tidsregistrering. Tilsynsmyndigheitas utsegn frå 2014 vart utforma i saka kalla «Processing of leave and flextime».[67] Vedtaket retta seg mot Den Europeiske Banktilsynsmyndigheita som dreiv tidsregistrering av organisasjonens tilsette gjennom eit system basert på fingeravtrykkregistrering. Vedtaket bygde på Regulation (EC) No 45/2001, art. 5(a), som sette opp eit naudsynsvilkår for offentlege institusjonar, knytt til administrative oppgåver som føresette behandling av personopplysningar. Datatilsynet konkluderte at «*the use of fingerprints-based systems for the monitoring of working time of staff memebers is not concidered as necessary, and therefore, not legitimate*». Standpunktet bygde på at tidsregistrering kan gjennomførast med mindre inngripande midlar, noko som tilsa at metoden verken var naudsynt eller proporsjonal i relasjon til behandlingsføremålet om å føre eit arbeidstidsregister.[68] Ettersom vedtakets problemstilling og drøftingsemne fell saman med problemstillinga i denne oppgåva så tildeler eg utsegna argumentasjonsverdi. Vedtaket tilseier altså at biometriske tidsregistreringsystem, på generell basis, ikkje vil innfri naudsynskravet.

Forordningas art. 9 nr. 2 bokstav b inviterer vel å merke til ei konkret drøfting; underspørsmålet vidare er dimed om distinkte saksomstende likevel vil kunne innfri vilkåret om naudsemd. Denne drøftinga kan delast i to. Fyrste del av naudsynsdrøftinga føreset at arbeidsgjevar har inngåande kjennskap til

[65] Sjå Schartum D. W., (2020), side 221, men merk at utsegna rettar seg mot naudsynsvurderinga frå Pol. § 12, ikkje PVF art. 9 nr. 2 bokstav b.
[66] Jf. Schartum D. W., (2020), side 126.
[67] Jf. EDPS-vedtak: 2014-0496, datert 13.10.14, side 3, URL: https://edps.europa.eu/sites/default/files/publication/14-10-13_letter_mr_mifsud_eba_en_0.pdf
[68] Ibid. Sjå vedtakets punkt 4.

det biometriske systemet, samt kva personverninteresser dette systemet kan kome i konflikt med.[69] Arbeidsgjevar skal godtgjere at systemet effektivt innfrir forpliktinga om føre tidsregistrering, samt at prosesseringa skjer i tråd med føremåla bak denne plikta. Spørsmålet ved fyrste trinn av drøftinga er fylgjeleg om systemets teknisk aspekt talar for eller mot at fingeravtrykkregistrering er naudsynt.

Frå eit praktisk perspektiv er fingeravtrykkbaserte tidsregistreringssystem teknisk kapable til effektivt å innfri registreringsplikta i aml. § 10-7. Dette momentet talar til fordel for systema. Baksida med fingeravtrykkregistrering er at prosesseringa medfører behandling av særs intime biometriske data.[70] Med andre ord vil behandlinga ha store konsekvensar for dei registrerte arbeidstakarane sitt person-opplysningsvern og deira personvernrettslege interesser. Fingeravtrykkbaserte system kan vel å merke inneha forskjellige sikringstiltak som modifiserer alvorsgraden av inngrepet, men likevel vil eit kvart biometriske tidsregistreringssystem, jamt over, medføre eit betydeleg personverninngrep. Konklusjonen ved fyrste del av naudsynsdrøftinga er med dette at fingeravtrykkregistrering, generelt, utgjer ein stor personverntrugsel. Dette talar mot å rekne fingeravtrykkregistrering som naudsynt.

Den andre delen av naudsynsdrøftinga går ut på å avklare om arbeidsgjevar kan implementere andre tidsregistreringssystem som er like eigna til effektivt å innfri forpliktinga om å registrere arbeidstid, og som samtidig poserer ein mindre trussel mot personopplysningsvernet.

I den tidlegare tilviste tyske ankesaka frå Berlin-Brandenburg, om den radiologiske teknikaren, kjem det forholdsvis tydeleg fram at tidsregistrering er ein prosess som enkelt let seg gjennomføre med mindre inngripande metodar enn fingeravtrykkregistrering. I saka la domstolen stor vekt på at arbeidsgjevaren - den radiologiske avdelinga - hadde tilgang til ein terminal som kunne driftast gjennom magnetiske nøkkelkort. Domstolen kommenterte at sjølv om det eksisterer ei rekke fullt funksjonelle metodar for å registrere arbeidstid, så som på papir, med id-kort, pinkodar, biometrisk fingeravtrykkavlesing m.m. så avgrensa naudsynsvilkåret arbeidsgjevars valmoglegheit mellom desse. Den tyske og EU-rettslege forpliktinga om å registrere arbeidstid, som skulle sikre betre helse og velvære for arbeidstakarane, kunne ikkje innfriast gjennom kvar av dei nemnde metodane.

Domstolen kommenterte at terminalen «IT 8200» utgjorde eit alternativt tidsregistrerings-system som var eigna til å innfri forpliktinga, og som ikkje føresette avlesing av biometri.[71] Denne terminalen ville dimed ikkje påverke dei tilsette sine personverninteresser i same grad som «ZEUS» - det biometriske systemet – kom til å gjere. Den radiologiske avdelinga argumenterte for at «ZEUS»-systemet likevel var naudsynt ettersom eit ID-kort basert system ville medføre meirkostnader. Eksempelvis i form av utgifter knytt til nye ID-kort, samt kostnader rundt det administrative arbeidet

[69] Jf. Det Europeiske Datatilsynet, *Neccesity Toolkit (…)*, (2017), side 9 og 10.
[70] Her viser eg tilbake til utgreinga frå kapittel 1 og 2.
[71] Jf. Radiolog-saka, 2020, avsnitt 65 og 66.

med å føre oversikt over desse. Verksemda presenterte vel å merke verken ei kostnadskalkyle eller andre bevis som støtta opp om utsegna. Domstolen avviste dimed noteringa på basis av manglande bevisgrunnlag, og det vart ikkje tatt stilling til kva meirutgifter som potensielt kunne godtgjere at eit biometrisk system ville vere naudsynt. Hadde problemstillinga vorte sett meir på spissen ville det vere naturleg å vurdere kostnadsmomentet i ljos av den høge unntaksterskelen som vart lagt til grunn over. Det strenge naudsynsvilkåret tilseier at det truleg må vere tale om ei betydeleg innsparing- eller utgifter før kostnadsargumentet kan reknast som eit nokon lunde legitim utspel.[72]

Vidare argumenterte den radiologiske avdelinga for at fingeravtrykkregistreringa likevel var naudsynt av omsyn til ei rekke andre behov verksemda hadde. Den nye terminalen «ZEUS» skulle førebygge urettmessige innstemplingar frå kollegaer, auke systemets presisjonsnivå og dimed også den digitale sikkerheita kring verksemdas databasar. I tillegg skulle det auka presisjonsnivået òg medverke til betre smittesporing på arbeidsplassen. Til sist kunne verksemda bruke plattforma til å honorere framståande tilsette. Ettersom dei nemnde behova og interessene gjekk utover den rettslege forpliktinga gjekk domstolen over i ei proporsjonalitetsvurdering, knytt til naudsynsvilkåret.

Radiolog-saka stør altså opp om standpunktet i Det Europeiske Datatilsynets vedtak - om at det sjeldan vil vere naudsynt å innfri ei forplikting om å registrere arbeidstid gjennom eit system som er basert på fingeravtrykkregistrering. Standpunktet blir i også denne saka grunngjeve med at arbeidsgjevaren hadde tilgang til eit alternativt system som ikkje føresette fingeravtrykkregistrering.

Argumentasjonen frå føre avsnitt vil truleg kunne gjerast gjeldande ovanfor dei fleste arbeidsgjevarar. Konklusjonen for andre del av naudsynsdrøftinga er fylgjeleg at tilgangen til andre og meir eigna tidsregistreringssystem tilseier at fingeravtrykkregistrering sjeldan er naudsynt.

Som avklart i utgreiinga over er naudsynsvilkåret strengt. Spørsmålet vidare er om fingeravtrykk-registreringa likevel, unntaksvis, kan vere naudsynt dersom behovet for behandlinga er proporsjonal innverknaden systemet utgjer ovanfor dei tilsette. Dette neste drøftingsemnet har fylgjeleg eit meir subjektivt preg over seg enn den objektivet vurderinga som er gjort av naudsynsvurderinga så langt.

[72] Artikkel 29-gruppa, *Opinion 3/2012 on developments in biometric technologies*, side 8.

4.5 Proporsjonalitetsvurderinga

Eit av dei sentrale aspekta knytt til naudsynsdrøftinga er altså behandlingas proporsjonalitet.[73] Proporsjonalitetsprinsippet utgjer den underliggjande rettleiaren som rettferdiggjer at ei rettsleg forplikting kan gjere det naudsynt å gripe inn i den registrerte sitt personvern. Dette kjem av at proporsjonale behandlingsprosessar byggjer på dei minst mogleg inngripande systema og metodane arbeidsgjevar kan ta i bruk, men som samtidig er eigna til å innfri forpliktinga på ein fullverdig måte.[74] Arbeidsgjevar må med andre ord godtgjere at andre system ikkje er like eigna som det biometriske systemet, ved å aktualisere legitime behov og målsetjingar knytt til gjennomføringa av prosessen. Samtidig må verksemda også godtgjere at fingeravtrykkregistreringa vil innfri desse legitime behova. Ved andre del av proporsjonalitetsvurderinga skal arbeidsgjevar igjen gjere ei konsekvensvurdering av systemet og avklare i kva grad dette grip inn i den registrerte sine personverninteresser.[75] Ved denne delen kan arbeidsgjevar framheve iverksette teknisk og organisatoriske tiltak som skal avgrense det konkrete personverninngrepet. Avslutningsvis må ein gjere ei balansert overordna vekting av dei motstridande interessene mellom arbeidstakars personvern og arbeidsgjevars legitime behov.[76]

Proporsjonalitetsprinsippet tuftar på ulovfesta praksis frå EU-domstolen og blir til dømes kort skildra i Tele 2 Sverige-saka som omhandla rettmessigheita av ein regel som greip inn i konfidensialitets-omsynet.[77] Den aktuelle regelen opna for atterhald av personopplysningar; blant anna på basis av nasjonale sikkerheitsinteresser. Med tilvising til EU-praksis og Den europeiske unions pakt om grunnleggjande rettar, artikkel 52 nr. 1, skriv storkammeret i avsnitt 94 at proporsjonalitetsprinsippet inneberer at personverninngrep «*may be imposed on the exercise of those rights and freedoms only if they are necessary and if they genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others*». Utsegna framhevar at eit gitt peronverninngrep båe må vere naudsynt og vere foreinleg med legitime interesser og føremål. Dette leier oss inn i den fyrste delen av proporsjonalitetsdrøftinga - knytt til arbeidsgjevars behov.

To pretendert behov går att i sakene eg har kome over om fingeravtrykkbasert arbeidstidsregistrering. Overordna sett byggjer desse behova på verksemdas målsetjingar knytt til sikkerheit og presisjon.

---

[73] Jf. 1) Det Europeiske Datatilsynet, *Guidelines on assessing the proportionality of (...),* (2019), side 3, og 2) Artikkel 29-gruppa, *Opinion 2/2017 (...)*, side 23.
[74] Jf. Spiecker gen. Dohmann, mfl., (2023), side 294 og 317-318.
[75] Jf. Radiolog-saka, 2020, avsnitt 63.
[76] Jf. 1) Det Europeiske Datatilsynet, *Guidelines on (...) proportionality (...),* 2019, side 12, og 2) Artikkel 29-gruppa, *Opinion 3/2012 (...)*, side 8.
[77] Jf. Kombinerte storkammer-avgjerd av sakene, *Tele2 Sverige*, C-203/15 og *Tom Watson m.fl.*, C-698/15, ECLI:EU:C:2016:970, avsnitt 93 til 96.

Argumentasjonen går gjerne ut på at det biometriske systemet er naudsynt for å førebygge lovbrot eller andre sikringsrelaterte problem, anten knytt til eksterne aktørar eller internt i verksemda.

Sikringsbehovet var tema i Manfield-saka, behandla og avgjort den 12.08.19, av fyrsteinstans-domstolen i Amsterdam.[78] Saka stod mellom den Nederlandske skobutikkjeda Manfield Schoenen B. V. og ein av deira medarbeidarar som nekta å ta i bruk selskapets nye biometribaserte kassaregister. I tillegg til å fungere som eit system for tilgangskontroll til verksemdas kassasystem utgjorde fingeravtrykkregistreringa også verksemdas einaste system for arbeidstidsregistrering.

I relasjon til kravet om naudsemd og proporsjonalitet noterte Manfield at det føre påloggings-systemet deira - som bygde på personlege pinkodar - hadde sikkerheitsmessige svakheiter og måtte skiftast ut. Selskapet var særskild bekymra for at det etablerte systemet ikkje var motstandsdyktig mot forsøk på hacking og underslag. Manfield hadde nemleg avdekka ein ukultur mellom tilsette som stal pinkodar og innloggingsdetaljar, for så å logge seg inn på kollegaane sine kontoar og dinest stele frå kassaapparata. Denne bedragerske åtferda komprimerte systemets sikringseffekt, og det biometriske systemet skulle avhjelpe dette. Fingeravtrykkregistreringa var meint å motverke underslagstrenden ved å gjere innloggingsprosessen til kassaapparata meir presis og etterprøvbar. Dinest argumenterte Manfield for at fingeravtrykkregistreringa også var lovleg ettersom dei, som behandlingsansvarleg, var forplikta til å syte for adekvat datasikkerheit, jf. PVF art. 24. I forlenging av dette standpunktet utdjupa Manfield at den biometribaserte innlogginga var naudsynt for å verne om sensitiv informasjon om: 1) finansielle forhold, 2) om arbeidstakarars kontraktsdetaljar, samt 3) om kundars personalia. Siktemålet med fingeravtrykkregistreringa var dimed tilleggsvis å verne om desse digitale verdiane ved å gjere det vanskelegare å oppnå urettmessig fjerntilgang inn til datasystemet.

Domstolen kommenterte at behandlingas proporsjonalitet riktig nok vil kunne bygge på verksemdas sikringsrelaterte behov for å implementere det biometriske systemet. Dinest sette retten dette utgangspunktet i kontekst ved å vise til nasjonale førarbeid som argumenterte for at sikrings-behovet, til eksempelvis eit atomkraftverk, er langt større enn sikringsbehovet til ein garasjeverkstad. Fylgjeleg kommenterte domstolen at Manfield, som skoforhandlar, ikkje hadde sikringsinteresser som stod proporsjonalt med omfanget av det personvernrettslege inngrepet ovanfor den saksøkande arbeidstakaren.[79] Her synar dommen at skalaen og betydninga av verksemda som blir drive er eit moment av sentral betydning ved proporsjonalitetsvurderinga. Standpunktet kan også sjåast i samanheng med poenget som vart nemnd i punkt 3.5. og 4.2. om at enkelte samfunnsbehov er eigna til å modifisere utgangspunktet om kva behandlingsmetodar som er proporsjonale. I høve

[78] Saka er tilgjengeleg i databasen: de Rechtspraak, nasjonalt saksnummer er: 7728204 CV VERZ 19-9686, URL: https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBAMS:2019:6005 (lese 27.10.23).
[79] Jf. Manfield-saka, 2019, avsnitt 21.

arbeidsgjevar driv ei forholdsvis alminneleg verksemd som ikkje aktualiserer eit særskilt eller stort behov for ekstra presis sikring, så talar dette mot å rekne behovet som legitimt og proporsjonalt.

Vidare kommenterte domstolen at personvernforordninga, derunder behandlingsforbodet i artikkel 9 nr. 1, ikkje kan setjast til side til tross for at verksemda er utsett for ulovlege handlingar i form av underslag, eller på grunn av andre potensielle sikkerheitsrisikoar.[80] Manfield kunne naturlegvis implementere andre sikringstiltak som ikkje strida med personverregelverket; så som alarmar, videoovervaking eller kontantskrin. Ettersom skobutikken ikkje hadde søkt å implementere nokon sånne alternative tekniske tiltak så talte dette mot at Manfield hadde eit legitimt sikringsbehov. Domstolens resonnement er med andre ord at ein vanskeleg kan godtgjere å ha eit reelt og legitimt behov for å drive fingeravtrykkregistrering, dersom verksemda ikkje i tillegg prioriterer å oppnå den ynskja sikringsgrada gjennom andre eigna tiltak.

Eit sentralt skilje mellom faktum i Manfield-dommen og vår problemstilling er at me vurderer proporsjonaliteten av biometriske tidsregistreringssystem, mens den tilviste saka primært omhandlar eit biometrisk tilgangssystem. Ei verksemd kan - som ein eksempelvis kan lese i ESSO-saka - i kraft av den konkrete verksemda aktualisere eit særskilt behov for sikkerheit og dimed også eit behov for ekstra presis regulering av kven som oppnår tilgang inn til arbeidsplassen.[81] Det same omsynet let seg ikkje like enkelt applisera i relasjon til verksemdas system for tidsregistrering. Desse systema skal derimot typisk innfri ei arbeidsrettsleg forplikting om å føre arbeidsrelatert tidsregistrering; dette føremålet føreset ordinært ikkje same sikringsgrad som eit system for åtgangskontroll.

Sikringsomsynet blir også trekt fram i relasjon til ei rekke pretendert behov i den tyske ankesaka for den radiologiske klinikken.[82] Det fyrste av desse behova bygde på at klinikken ynskja å oppnå eit ekstra vern om sensitiv pasientdata som var lagra inne på avdelingas datasystem. Domstolen avviste denne pretensjonen ettersom digital datasikring skal skje gjennom eigna tekniske tiltak som vernar systemet mot ikkje-autorisert tilgang.[83] Eit biometrisk tidsregistreringssystem ville ikkje vere eit effektivt verkemiddel for å oppnå dette sikringsføremålet. Behovet var fylgjeleg ikkje legitimt.

Vidare pretenderte klinikken - av omsyn til tilsette og pasientar si helse og velvære - at den hadde eit behov for ein særs presis tidregistreringsmetode for å avdekke smittekjelder og potensielle sjukdomsutbrot. Om dette kommenterte retten fyrst at arbeidsgjevar ikkje hadde ført bevis for denne type smittetrugslar. I løpet av den aktuelle arbeidstakarens arbeidskvardag kom denne heller ikkje i kontakt med pasientar, men arbeida derimot primært på datamaskin. Klinikken hadde med andre ord ikkje godtgjort at behovet for å utbetra verksemdas smittesporing var reelt. For det andre hadde

[80] Jf. Ibid. avsnitt 24.
[81] Jf. PVN-2006-10, vedtakets punkt 6.4.
[82] Jf. Den tyske Radiolog-saka av 2020.
[83] Jf. Ibid. avsnitt 72 og 73.

arbeidsgjevar heller ikkje utforma ei risikoanalyse som tilsa at det var naudsynt å innføre tiltak - så som eit biometribasert system - for å imøtekome smittetrugslar.[84] Verksemda hadde med dette heller ikkje eit legitimt behov for å bruke biometrisk tidsregistrering for å førebygge sjukdom.

Behandlinga av desse to fyrste pretenderte sikringsbehova framhevar to sentrale poeng ved naudsyns- og proporsjonalitetsvurderinga. For det fyrste må det biometriske systemet, reint teknisk, vere eigna til å innfri det pretenderte føremålet. For det andre synar saka, i relasjon til noteringa om smittesporing, at sjølv om behovet moglegvis har grunnlag i eit verneverdig samfunnsbehov så må arbeidsgjevar føre bevis for og godtgjere at behovet er reelt og adekvat sett opp mot prosessen.

I båe Manfield-saka og i saka om den radiologiske teknikaren argumenterer arbeidsgjevane for at fingeravtrykkregistreringa også var naudsynt for å førebygge manipulasjon av innstemplingsdataa. Verksemdene argumenterte for at dette kunne skje ved at arbeidstakarane stempla kvarandre inn.

Ifylgje den radiologiske klinikken ville andre system ikkje kunne innfri forpliktinga om å føre timeregistrering ettersom berre eit biometrisk system ville vere tilstrekkeleg presis og etterprøvbart til å avverje juks. Med andre ord pretenderte verksemda å ha eit legitimt sikringsbehov knytt til den skildra svindelrisikoen. Ankedomstolen sa seg einig i at biometriske system er eigna til å førebygge urettmessig innstempling. Likevel ville behovet for å bruke fingeravtrykkregistrering for å førebygge svindel berre vere legitimt i høve arbeidsgjevar fyrst har godtgjort at denne type åtferd utgjer eit reelt og betydeleg problem.[85] Ei generell førebygging kom sjeldan til å vere proporsjonal sett opp mot arbeidstakarane sine personverninteresser. Retten kommenterte vidare at behovet for fingeravtrykk-registrering uansett ikkje var spesielt pressande ettersom juks let seg oppdage på andre vis. Til dømes kan klinikken vanlegvis feste lit til at anten dagleg leiar, eller kollegaer og kundar, legger merke til det dersom den tilsette er fråverande.

Utgreiinga i radiolog-saka framhevar poenget om at berre legitime behov er relevante i relasjon til proporsjonalitetsvurderinga, samt at arbeidsgjevar må bevise at sikringsbehovet båe er reelt og vektig. Behandlingsbehovet må derunder i tillegg vere reelt ovanfor kvar enkelt arbeidstakar. Arbeidsgjevar kan eksempelvis godtgjere relevansen ovanfor den enkelte tilsette dersom verksemda grunngjev korleis den aktuelle arbeidstakaren er knytt til problemet som skal utbetrast. Alternativt må fingeravtrykkregistreringa vere eigna til å avhjelpe ein ekstensiv problemtilstand i verksemda, og behandlinga av den aktuelle tilsette sine biometriske persondata vil bidra til ei alminneleg utbetring. Ved dette sistnemnde tilhøve vil skalaen og alvorsgrada av problemet, eksempelvis den sviksame åtferda, vere av ekstra stor betyding for proporsjonalitetsvurderinga.

[84] Jf. Ibid. avsnitt 74.
[85] Jf. Ibid. avsnitt 78.

Dei nemnde behova – knytt til sikkerheit og etterprøvbarheit – verkar å vere dei vanlegaste behova arbeidsgjevar pretenderer til forsvar for behandlingsprosessen. Andre og mindre opplagte behov kan likevel førekome. Eksempelvis vart det nemnd i punkt 4.4. at den radiologiske avdelinga også argumenterte for at «Zeus» systemet var nødvendig fordi verksemda skulle bruke denne plattforma til å honorere tilsette. Domstolen såg ikkje ein opplagt samanheng mellom tidsregistreringssystemet og den nemnde funksjonen; fylgjeleg vart behovet ikkje rekna som legitimt.[86] Her er det eit poeng at det er behandlingsføremålet som er avgjerande for kva siktemål behandlingsprosessen kan brukast til.[87]

Kva aspekt kring behandlingsprosessen kan ein så ta opp i andre del av proporsjonalitetsdrøftinga? Denne delen omhandlar som nemnd arbeidstakars personverninteresser og ein skal ta stilling til omfanget av det konkrete personvernrettslege inngrepet som fingeravtrykkregistreringa medfører. Skalaen og frekvensen av behandlingsprosessen er eksempelvis moment som seier noko om kor inngripande prosesseringa er. Denne delen av drøftinga vil igjen bygge på utgreiinga som vart gjort i kapitel 1 og 2 om biometriske personverninngrep og arbeidstakaranes personvernrettslege interesser i å unngå fingeravtrykkregistrering. I tråd med dette er behandling av biometriske personopplysningar rekna som eit betydeleg personverninngrep og behandlingsprosessen vil sjeldan vere proporsjonal.[88]

Underspørsmålet altså er om behandlingsprosessar som tek omsyn til den registrerte medfører at fingeravtrykkregistreringa likevel, unntaksvis, kan vere proporsjonal - sett i kontekst av arbeidsgjevars eventuelle legitime behov for å gjennomføre den biometriske tidsregistreringa.

Som nemnd i punkt 4.3. er ikkje biometriske prosessar og system for fingeravtrykkbasert registrering av arbeidstid like. Derimot innehar systema gjerne forskjellige digitale verktøy som i varierande grad er eigna til å ivareta personopplysningsvernet. Sånne verktøy kan eksempelvis ta sikte på å minimere den handsama datamengda, å avkorte lagringsperioden eller å sikre tilstrekkeleg konfidensialitet rundt dei biometriske dataa. Ein kan fylgjeleg sjå denne andre delen av proporsjonalitetsvurderinga i samanheng med forordningas artikkel 5, om grunnleggjande personvernprinsipp, artikkel 25 om innebygd personvern og om å gjennomføre eigna tekniske og organisatoriske tiltak, samt artikkel 32 om vilkår for sikkerheita ved behandlinga. Eit system som innehar gode løysingar for å sikre personvernet og som elles operer i tråd med dei alminnelege personvernprinsippa vil altså medføre eit tilsvarande redusert personverninngrep. Med andre ord vil konkrete tekniske sikringstiltak kunne tale for at fingeravtrykkregistringa likevel utgjer ein proporsjonal behandlingsmetode.[89]

[86] Jf. Ibid. avsnitt 67.
[87] Sjå utgreiinga om dette i tekstens punkt 3.2.
[88] Sjå også denne tekstens punkt 4.3 og 4.4.
[89] Jf. Bulgakova, «Casestudy (…)», 2022, side 29.

Personvernforordninga artikkel 32 nr. 1 krev at verksemda må gjennomføre «*tekniske og organisatoriske tiltak*» som er eigna til å oppnå eit sikkerheitsnivå som er passande i relasjon til personvernrisikoen. Artikkelens punkt a konkretiserer at tiltak som kryptering vil kunne bidra til å auke sikkerheita. Punkt b nemner målsetjinga om å sikre dataas konfidensialitet, integritet, åtgang og generelt robuste digitale system. At tiltaka både skal vere *tekniske* og *organisatoriske* framhevar at det ikkje er tilstrekkeleg å gjennomføre digitale software-tiltak, men også gjennom til dømes rutinar og kursing knytt opp mot ansvaret som kvar av verksemdas aktørar har i relasjon til intern datasikring.[90] Kva tiltak er så eigna til å yte tilstrekkeleg sikkerheit om fingeravtrykkbaserte behandlingsprosessar?

Eg har ikkje kome over publiserte saker som enda med at arbeidsgjevarens fingeravtrykkbaserte tidsregistrering vart kategorisert som naudsynt og proporsjonal etter PVF art. 9 nr. 2, bokstav b. Derimot kan me sjå til ei italiensk sak der tilsynsmyndigheita avviste artikkel 9 nr. 2, bokstav b, på basis av manglande ytterlegare regulering og naudsynte garantiar. I denne saka, datert 14.01.21, hadde arbeidsgjevaren, ein helseinstitusjon kjend som Enna, gjennomført ei rekke tiltak for å avgrense det personvernrettslege inngrepet av fingeravtrykkregistrering på institusjonens tilsette.[91] Føremålet med systemet var å auke det tekniske presisjonsnivået ved innstemplingsprosessen, samt å førebygge urettmessig fråvær frå jobb. Arbeidsgjevaren la til grunn at behovet for fingeravtrykk-registrering både bygde på institusjonens skala og den sentrale samfunnsfunksjonen denne hadde som tilbydar av helsetenester. I forlenging av dette noterte Enna at oppgåva deira med å føre oversikt over oppmøte til meir enn 2000 tilsette (mange med vidt forskjellege turnusar og arbeidstider), blant 4 sjukehus og over 22 kommunar var særs krevjande og at HR-avdelinga dimed hadde eit stort behov for å implementere eit ekstra presis og etterprøvbart tidsregistreringssystem.

Registreringsprossedyra var samansett av ein innleiande identifikasjonsprosess der den registrerte måtte presentere eit personleg id-kort som inneheldt ein kryptert modell av kvar enkelt arbeidstakars fingeravtrykk. Dernest skulle dei tilsette gjennomføre sjølve verifiseringa gjennom ein etterfylgjande fingeravtrykkregistrering. Denne metoden gjorde til at Enna unngjekk at systemet måtte gjere eit vidt registersøk som hadde råka langt fleir enn den eine verifiserte arbeidstakaren.

Vidare sletta systemet automatisk alle dataa som vart registrert ved innstemplinga; sett vekk frå sjølve tidsstempelet. Med andre ord lagra systemet berre den krypterte biometriske stingen i id-kortet, mens kvart etterfylgjande biometriske avtrykk vart sletta etter at innstemplingsprosedyren var gjennomført. Dette sikringstiltaket bidrog til å minimere den lagra datamengda.

Eit tredje aspekt ved prosessen var at dei krypterte biometriske modellane kunn blei lagra

[90] Jf. Spiecker gen. Dohmann, m.fl., (2023), side 667, avsnitt 27.
[91] Sjå i databasen: GDPR - Garante per la protezione dei dati personali, nasjonalt saksnummer er: 9542071, URL: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9542071 (lese 27.10.23).

lokalt på det personlege id-kortet som arbeidstakar hadde full rådigheit over. Dette tiltaket styrka datasikringa ettersom ein ikkje kunne tileigne seg tilgang til dei biometriske opplysningane over verksemdas sentrale databasar. Den lokale lagringa bidrog også til å unngå tap av data i form av teknisk eller organisatorisk svik, eksempelvis ved feilslått overføring eller liknande. Tiltaket bidrog med andre ord til å verne om båe konfidensialiteten og integriteten til opplysningane.

Dei mange sikringstiltaka som var gjennomført av Enna synar at arbeidsgjevar kan gjere mykje for å styrke personvernet kring dei biometriske opplysningane. I teorien er denne saka trekt fram som eksempel på kva personverntiltak som potensielt vil vere tilstrekkeleg for å innfri proporsjonalitets-kravet, dersom arbeidsgjevar også har eit behov som båe er legitimt og betydeleg.[92] I den tilviste artikkelen la forfattaren Daria Bulgakova stor vekt på at lagringa var lokal og at arbeidstakarane dermed hadde full rådigheit over denne.

I den tidlegare tilviste spanske Byråd-saka frå 2021 trekte det spanske datatilsynet fram mange av dei same sentrale momenta som er presentert i Enna-saka. Denne saka omhandla vel å merke primært byrådets mangelfulle innfriing av handlings- og informasjonsplikta, men datatilsynet kommenterte i tillegg at enkelte personverntiltak vil tale til fordel for proporsjonaliteten av behandlingsprosessen.

Av momenta som allereie er presentert gjennom Enna-saka ramsa datatilsynet opp betydninga av lagringsavgrensing, dataminimering, samt krypteringsteknikar for båe å avgrense risikoen for konfidensialitetsbrot og risikoen for at dataa blir tukla med.[93] I tillegg nemnde tilsynet at den behandlingsansvarlege også skal sikre at dei biometriske opplysningane verken kan- eller blir brukt til andre føremål enn den aktuelle tidsregistreringa. Dette poenget har samanheng med omsynet til føremålsavgrensing som me har sett på over. Til sist vart det kommentert at systemets utforming burde sikre ein funksjon for å kalle attende identitetskoplinga mellom individet og biometriske data. Dette siste tiltaket er avgjerande for å sikre at ukorrekte opplysningar, og data som arbeidsgjevar elles ikkje lenger skal handsame, kan gjerast anonyme. Tiltaket bidreg med andre ord også til å styrke sikkerheita av systemets slettingsprosessar.

Eit siste moment som seier noko om proporsjonaliteten av fingeravtrykkregistreringa er om systemet også er til fordel for den registrerte eller om implementeringa på anna vis er i denne si interesse. Ettersom fingeravtrykkregistrering ikkje tilbyr noko meir enn eit tradisjonelt tidsregistreringssystem så vil dette truleg sjeldan vere tilfelle. Skulle det eksempelvis oppstå tvil om den tilsette har møtt opp til arbeid til rett tid så vil denne typisk kunne vende seg til dagleg leiar eller andre som kan konfirmere at

[92] Jf. Bulgakova, «Casestudy (…)», 2022, side 29-32.
[93] Jf. Byråd-saka, 2021, side 10.

han eller ho faktisk var til stades. Momentet vil fylgjeleg sjeldan tale for proporsjonalitet.

I den avsluttande fasen av proporsjonalitetsvurderinga må ein altså vege aktuelle legitime behov opp mot det konkrete personverninngrepet. Fråværet av saker om proporsjonale fingeravtrykkbaserte tidsregistreringsystem framhevar den høge unntaksterskelen som vart lagt til grunn i punkt 4.4.

Summert opp vil kunn veldig særeigne saksomstende vere eigna til å innfri naudsynskravet i personvernforordningas artikkel 9 nr. 2 bokstav b. Arbeidsgjevar må aktualisere legitime og vektige behov som grunngjev kvifor andre metodar ikkje kan takast i bruk. I tillegg må det grunngjevast kvifor arbeidstakar burde tole den konkrete behandlingsprosessen. Utgreiinga i punkta over synar at dei færraste arbeidsgjevarar vil kunne innfri det strenge naudsynskravet, fylgjeleg vil unntaksføresegna PVF art. 9 nr. 2 bokstav b ikkje kome til bruk. For arbeidsgjevaren inneberer dette at fingeravtrykk-registreringa framleis er underlagt behandlingsforbodet etter personvernforordningas art. 9 nr. 1.

Litteraturliste

- Blekstad, Signhild og Marion Hirst, *Personvern og kontroll i arbeidslivet*, Gyldendal 2021
- Taal, Amie (red.), *The GDPR Challenge: Privacy, Technology, and Compliance in an Age of Accelerating Change*, CRC press 2021.
- Schartum, Dag Wiese, *Personvernforordningen – en lærebok*, Fagbokforlaget 2020.
- Smith, Marcus og Seumas Miller, *Biometric Identification, Law and Ethics*, Springer Cham 2021. DOI: https://doi.org/10.1007/978-3-030-90256-8.
- Fairhurst, Michael, *Biometrics – A very short introduction*, Oxford University Press 2018.
- Jarbekk, Eva og Simen Sommerfeldt, *Personvern og GDPR i praksis*, Cappelen Damm akademisk 2019.
- Skullerud, Åste Marie Bergseng, Cecilie Rønnevik, Jørgen Skorstad og Marius Engh Pellerud, *Personopplysningsloven og Personvernforordningen (GDPR) – kommentarutgave*, Universitetsforlaget 2019.
- Dòhmann, Indra Spiecker gen., Vagelis Papakonstantinou, Gerrit Hornung og Paul De Hert (red.) Andras Jori, *Genereal Data Protection Regulation – Article by article Commentary*, Nomos Verlagsgesellschaft mbH & Co 2023.

Lov, forskrift og konvensjon mv.

- Lov 17. mai 1814 Kongeriket Noregs Grunnlov (grunnlova).
- Lov 27. november 1992 nr. 109. Lov om gjennomføring i norsk rett av hovuddelen i avtale om Det Europeiske Økonomiske samarbeidsområde (EØS) m.v. (EØS-lova).
- Lov 13. april 2000 nr. 31. Behandling av personopplysningar (personopplysningsloven). *Oppheva*
- Lov 17. juni 2005 nr. 62. Lov om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljølova).
- Lov 15. juni 2018 nr. 38. Lov om behandling av personopplysningar (personopplysningsloven).

- Forskrift 03. august 2009 nr. 1028. Forskrift om sikkerheit, helse og arbeidsmiljø på bygge- eller anleggsplassar (byggherreforskrifta).

EU-rett

- Convention for the Protection Human Rights and Fundamental Freedoms, vedtatt 4. november 195, tredde i kraft 3. september 1950. (Den europeiske menneskerettskonvensjonen).
- EUs Personverndirektiv frå 1995, Direktiv 95/46/EF om beskyttelse av fysiske personar i forbindelse med behandling av personopplysningar og om fri utveksling av sånne opplysningar. *Oppheva*
- EUs Arbeidstidsdirektiv frå 2003, Directive 03/88/EC of the European Parliament and of the Council of 4 November 2003 concerning certain aspects of the organisation of working time.
- Den europeiske unions pakt om grunnleggende rettigheter, (2000).
- Europaparlamentets- og Rådets forordning (EU) 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 (Personvernforordninga).

Rettspraksis og underrettspraksis

EMD og EU-domstolen

- EMD, *Glukhin mot Russland* [J], no. 11519/20, ECHR 2023.
- EU-domstolens dom av 21. desember 2016, *Tele2 Sverige* [GC], C-203/15, ECLI:EU:C:2016:970.
- EU-domstolens dom av 20. desember 2017, *Nowac* [C5], C-434/16, ECLI:EU:C:2017:994

Personvernnemnda

- PVN 2006-10 (*ESSO Norge AS*)

Utanlandsk rettspraksis

- Fyrsteinstansdomstolen i Amsterdam 2019,
  EU-saks nr.: ECLI:NL:RBAMS:2019:6005 (*Manfield-saka*)
- Regional Arbeidsrettsdomstol i Berlin-Brandenburg 2020,
  EU-saks nr.: ECLI:DE:LAGBEBB:2020:0604.10SA2130.19.00 (*Radiolog-saka*)
- Andreinstansdomstolen i Barcelona 2021,
  EU saks-nr.: ECLI:ES:APB:2021:1448A

Utanlandsk underrettspraksis

- Spansk Datatilsynsmyndigheit 2021, nasjonalt saks-nr. PS/00128/2020 (*Byråd-saka*)
- Italiensk Datatilsynsmyndigheit 2022, nasjonalt saks-nr. 9832838 (*Sportitalia-saka*)
- Italiensk Datatilsynsmyndigheit 2021, nasjonalt saks-nr. 9542071 (*Enna-saka*)

Førarbeid

- Ot.prp.nr.92 (1998–1999) Om lov om behandling av personopplysninger (personopplysningsloven).
- Ot.prp.nr.49 (2004–2005) Om lov om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljøloven).
- 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.
- NOU 2022:11 Ditt personvern - vårt felles ansvar. Tid for en personvernpolitikk.

Rettleiingsskriv

- Det Europeiske Datatilsynet, *Opinion of [EDPS] on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas (COM(2004)835 final)*, C 181/19, 2005.
- Europarådets Ministerkomite, *Recommendation CM/Rec (2015) 5 on the processing of personal data in the context of employment.*
- Artikkel 29-gruppa, *Opinion 3/2012 on developments in biometric technologies*, 2012.
- Artikkel 29-gruppa, *Opinion 2/2017 on data processing at work*, 2017.
- Det Europeiske Datatilsynet, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, 2017.
- Arbeidstilsynet, Datatilsynet, Petroleumstilsynet og Partene i Arbeidslivet, *Veileder om kontroll og overvåking i arbeidslivet*, 2019.
- Det Europeiske Datatilsynet, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 2019.*
- Det Europeiske Datatilsynet og Den Spanske Datatilsynsmyndigheita, *14 Misunderstandings with regard to biometric identification and authentication,* 2020.
- Det Europeiske Personvernrådet, *Guidelines 05/2020 on consent under Regulation 2016/679*, 2020.
- Datatilsynet, *Vurdering av personvernkonsekvensar (DPIA) – liste over behandlingsaktiviteter som alltid krever at det gjennomføres en DPIA,* sist endra 27.07.2023.

Tidsskrifter

- Fournier, Nicole A. og Ann H. Ross, *Sex, Ancestral, and pattern type variation of fingerprint minutiae: A forensic perspective on anthropological dermatoglyphics*, American Journal of Physical Anthropology 2016, Vol. 160, side 625–632.
  DOI: https://onlinelibrary.wiley.com/doi/10.1002/ajpa.22869
- Holland, Peter og Tse Leng Tham, *Workplace biometrics: Protecting employee privacy one fingerprint at a time*, Economic and Industrial Democracy 2020, volum 43 side 501-515.
  DOI: https://doi.org/10.1177/0143831X209174
- Hopkins, Richard, *An Introduction to Biometrics and Large Scale Civilian Identification*, International review of law computers & technology 1999. DOI: https://doi.org/10.1080/13600869955017

- Kahn, Henry S., Mariaelisa Graff, Aryeh Stein og Lumey LH, *A fingerprint marker from early gestation associated with diabetes in middle age: The Dutch Hunger Winter Families Study*, International Journal of Epidemiology 2009, Vol. 38, Issue 1, side 101–109. DOI: https://doi.org/10.1093/ije/dyn158
- Nielsen, Morten Birkeland og Ståle Valvatne Einarsen, *Outcomes of exposure to workplace bullying: A meta-analytic review*, Work & Stress: An International Journal of Work,Health & Organisations 2012, 26:4, 309-332. DOI: https://www.tandfonline.com/doi/full/10.1080/02678373.2012.734709
- Jasserand, Catherine, *Legal nature of biometric data: From 'Generic' Personal Data to Sensitive Data'*, European Data Protection Law Review 2016, Vol. 2, Issue 3, pp. 297-311. DOI: https://doi.org/10.21552/EDPL/2016/3/6

Artiklar og lovkommentarar

- Burt, Chris, *Facial recognition and temperature scanning devices launched, deployed for access control*, Biometric Update.com 2023, URL: https://www.biometricupdate.com/202301/facial-recognition-and-temperature-scanning-devices-launched-deployed-for-access-control
- Burt, Chris, *Australian schools testing facial recognition for attendance*, Biometric Update.com 2018, URL: https://www.biometricupdate.com/201808/australian-schools-testing-facial-recognition-for-attendance
- Bulgakova, Daria, *Case Study on the Fingerprint Processing ina Workplace under GDPR Article 9 (2, b),* Vilnius University, Faculty of Law 2022. DOI: 10.15388/Teise.2022.124.2
- Datatilsynet, *Biometri – Biometriske data kan samles uten at du vet det*, 2019. URL: https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/biometri/ (lese: 02.11.23).