

# Vegprising og personvern

Personvern i møte med dynamisk vegprising og overvaking i trafikken



Bacheloroppgåve i statsvitskap

Universitetet i Stavanger

**Benjamin Varhaug**

Studentnummer: 256121

Vegleiar: Morten Ryen Loe

Lvert dato: 11.05.2022

Tal på ord: 8744

## Samandrag

Oppgåva tek sikte på å diskutera personvernet si rolle i dynamisk vegprising. Nye digitale løysingar krev stadig fleire opplysningar om oss – også i trafikken. Dynamisk vegprising som ei ny løysing for vegprising kan potensielt ha stor innverknad på overvakingsgrada i trafikken. Problemstillinga er: Kan innføring av dynamisk vegprising ha implikasjonar for overvakingsgrada og personvernet i trafikken? Problemstillinga vert forsøkt løyst ved å svara på tre forskingsspørsmål: Kan dynamisk vegprising ha påverknad på omfanget av overvaking i trafikken? Kan løysinga få fleire formål enn berre berekning av avgifter? Og kva implikasjonar kan dette ha på personvernet? Ved hjelp av relevant teori om overvaking og personvern vil personvernet si rolle i dynamisk vegprising analyserast. Oppgåva diskuterer personvernet si tilknytning til retten til privatliv og viktigheita av desse rettane for å oppretthalda fridomen til enkeltindivid og demokratiet. Sentrale prinsipp for personvern i personvernforordningen løftast fram som viktige rettesnorer for å sikra eit godt personvern. Det peikast vidare på korleis statlege aktørar og multinasjonale aktørar ofte motiverte av økonomiske faktorar eller omsyn til tryggleik, vil ha interesse av data generert ved dynamisk vegprising – og kvifor det vert viktig å forhindra deling av data med desse aktørane. Ulike løysingsforslag for dynamisk vegprising drøftast. Til slutt grunngjev og understrekar oppgåva den overordna viktigheita av ei personvernvenleg løysing for dynamisk vegprising.

## **Førord**

Denne oppgåva markerar slutten på statsvitskapstudiet ved universitetet i Stavanger. Det har vore kjekt og ikkje minst svært interessant å fordjupa seg i dynamisk vegprising, overvaking og personvern. Gjennom arbeidet har eg møtt på spanande utfordringar som har gjeve stort læringsutbytte. Djupdykket mitt i tematikken har kveikja opp eit initiativ for eit sterkt personvern og synleggjort personvernet si viktighet for det liberale demokratiet for meg.

Fyrst og fremst vil eg takka rettleiar, Morten Ryen Loe, for gode og raske tilbakemeldingar. Møta med rettleiar har gjeve fornya motivasjon og nye spanande innfallsvinklar. Eg vil også retta takk til vener og kjende som har bidrege med korrekturlesing og ikkje minst familie som har vore til stønad gjennom heile arbeidet.

Eg vonar at lesaren får ei god oppleving ved gjennomlesing og at han finn temaet like interessant og lærerikt som det har vore for meg gjennom arbeidet.

Benjamin Varhaug

Stavanger, Mai 2022

## Innholdsliste

|   |           |
|---|-----------|
| <b>1. Innleiing .....</b>   | <b>1</b>  |
| 1.1.1 Avgrensing .....  | 2         |
| 1.1.2 Struktur .....  | 3         |
| <b>1.2 Dynamisk vegprising .....</b>                                    | <b>3</b>  |
| <b>2 Metode .....</b>   | <b>3</b>  |
| <b>2.1 Kvifor teoretisk oppgåve .....</b>                               | <b>3</b>  |
| <b>2.2 Data og kjelder .....</b>  | <b>4</b>  |
| <b>2.3 Metodekritikk og utfordringar .....</b>                          | <b>4</b>  |
| <b>2.4 Framgangsmåte .....</b>  | <b>5</b>  |
| <b>2.5 Empiri .....</b>   | <b>5</b>  |
| <b>3 Teori .....</b>  | <b>6</b>  |
| <b>3.1 Overvaking .....</b>   | <b>6</b>  |
| 3.1.1 Kva meinast med overvaking .....                                  | 6         |
| 3.1.2 Korleis overvaking kan gå føre seg .....                          | 7         |
| 3.1.3 Moglege årsakar og konsekvensar ved overvaking .....              | 7         |
| <b>3.2 Personvern .....</b>   | <b>9</b>  |
| 3.2.1 Kvifor personvern er viktig .....                                 | 9         |
| 3.2.2 Personvernet sitt normative grunnlag .....                        | 10        |
| 3.2.3 Neglisjering av personvernet .....                                | 11        |
| 3.2.4 Personopplysningsloven og personvernforordningen .....            | 11        |
| <b>4. Analyse .....</b>   | <b>13</b> |
| <b>4.1 Dynamisk vegprising og overvaking .....</b>                      | <b>13</b> |
| <b>4.2 Personvern og dynamisk vegprising .....</b>                      | <b>14</b> |
| 4.2.1 Når krenkast eller svekkast personvernet? .....                   | 14        |
| 4.2.2 Dynamisk vegprising og personvernet sitt normative grunnlag ..... | 15        |
| 4.2.3 Dynamisk vegprising og personvernforordningen .....               | 16        |
| 4.2.4 Har dynamisk vegprising implikasjonar på personvernet? .....      | 17        |
| <b>4.3 Potensielle langsiktige utfordringar .....</b>                   | <b>18</b> |
| 4.3.1 Staten .....  | 18        |
| 4.3.2 Overvakingskapitalismen .....                                     | 19        |
| <b>4.4 Tilnærming til løysingar .....</b>                               | <b>21</b> |
| 4.4.1 Moglege løysingar .....   | 21        |
| 4.4.2 Avsluttande refleksjon .....                                      | 22        |
| <b>5. Konklusjon .....</b>  | <b>23</b> |
| <b>6. Litteraturliste .....</b>   | <b>25</b> |
| <b>6.1 Teoretiske kjelder .....</b>                                     | <b>25</b> |
| <b>6.2 Rettskjelder .....</b>   | <b>25</b> |
| <b>6.3 Andre kjelder .....</b>  | <b>26</b> |

## 1. Innleiing

I takt med aukande utvikling dukkar det stadig opp nye løysingar som skal gjere kvardagen vår enklare. Brukartilpassing og auka effektivitet er nokre av fordelane ved nye løysingar i vår digitale verd, samstundes er føresetnaden at meir informasjon om brukarane samlast inn og nyttast for å oppnå dette. Dynamisk vegprising er ei løysing som kan gjennomføra vegprising meir presist og effektivt, men som mange andre nye løysingar er dette systemet òg avhengig av meir køyredata og informasjon om brukarane. Dynamisk vegprising kan potensielt få konsekvensar for korleis enkeltindivid stillar seg til bilkøyning i trafikken. Det er difor nødvendig å stilla spørsmål ved potensielle konsekvensar ved dynamisk vegprising. Problemstillinga i oppgåva vert difor: *Kan innføring av dynamisk vegprising ha implikasjonar for overvåkingsgrada og personvernet i trafikken?*

Temaet i oppgåva dreier seg altså om dynamisk vegprising og kva følgjene kan verte av å innføra dette i Noreg. Tradisjonell vegprising som hovudsakleg er nytta i dag inneber automatisk betaling ved passering av gjevne passeringpunkt. Det er derimot ikkje denne forma for vegprising eg i denne oppgåva vil fokusera på, men i staden ein annan modell. Denne modellen inneber at det ved bruk av GPS-teknologi vert registrert kor langt og på kva vegar ein bilist køyrer, og reknar avgift ut frå dette. Her kan ein i tillegg basera avgiftsklassar på type drivstoff eller bilen sine klimagassutslepp. Slik kan avgifter «skreddarsyast» til brukarane alt etter deira forbruk av veg og miljøbelastning. Føresetnaden er at alle bilar må sporast til ei kvar tid. Diskusjonen om dynamisk vegprising dreier seg om konsekvensar for personvernet med tanke på overvakinga, som heile løysinga legg til grunn. Problemstillinga vil difor løysast med tre forskingsspørsmål, som skal svarast på i teksten:

*Kan dynamisk vegprising ha påverknad på omfanget av overvaking i trafikken? Kan løysinga få fleire formål enn berre berekning av avgifter? Og kva implikasjonar kan dette ha på personvernet?*

Eg vil med utgangspunkt i desse spørsmåla diskutera kva konsekvensane og ringverknadane kan verte av å ta i bruk dynamisk vegprising. Dette vil eg gjera med grunnlag i relevant teori som dekker områder ved overvaking og personvern. Eg vil fyrst forklara den nye forma for vegprising, korleis den fungerer og kva den gjer. Vidare vil eg forklara kva omgrepa overvaking og personvern inneber, før eg diskuterer kva implikasjonar dynamisk vegprising kan ha på personvernet i trafikken.

### 1.1.1 Avgrensing

Hovudfokuset i oppgåva er avgrensa til å drøfta GPS- og sporingsteknologi som kan nyttast til dynamisk vegprising. Altså verktøy som sporar køyretøy si rørsle og posisjon. Oppgåva vil difor ikkje drøfta vegprising som betalast ved passering av bomstasjon.

Oppgåva vil avgrensast til å fokusera på vegprising på personbilar og ikkje næringstransport. Grunnen til dette er at ei eventuell auke av overvaking i næringstransport vil kunna reknast som eit kontrolltiltak ovanfor tilsette i arbeidssituasjonen. Ei verksemd kan og nytta sporingsteknologi for å overhalda rettslege plikter.

Personvernforordningen (GDPR: General Data Protection Regulation, vedteke som norsk lov 20. juli 2018) er svært omfattande. I denne oppgåva vil berre dei mest relevante prinsippa brukast i analysen. Oppgåva tek difor i hovudsak berre for seg dei sentrale prinsippa i personvernforordningen artikkel 5 i tillegg til kravet om innebygd personvern i personvernforordningen artikkel 25. Oppgåva vil heller ikkje gå inn på personvernføresegner i andre lover enn personopplysningsloven.

Overvaking kan gå føre seg på mange vis. I denne oppgåva er overvaking avgrensa til elektronisk/digital overvaking.

I utgangspunktet finnast det ingen standardisert modell for dynamisk vegprising. Den metoden som presenterast i oppgåva viser berre dei grunnleggjande mekanismane som er nødvendige i eit GPS-basert vegprisingssystem. Sidan det er uklart korleis detaljane i løysingane vert for til dømes registrering og lagring av personopplysningar og korleis betaling skal gå føre seg må modellen diskutera på generelt grunnlag og ut frå dei mekanismane i modellen som alt er kjende.

### 1.1.2 Struktur

I teoridelen presenterast grunnleggande kunnskap om overvaking og personvern og kva som kan reknast som overvaking og kva som kan krenka rettane personvernet skal gje. Dette vert relevant i drøftinga rundt problemstillinga. Metodekapittelet presenterer og argumenterer for framgangsmåten som vart nytta for å utforska problemstillinga. Vidare vert det i analysen drøfta om dynamisk vegprising i større grad enn i dag kan overvaka trafikantane, om kva ringverknadar dynamisk vegprising kan ha og om dette kan koma i konflikt med personvernet. Avslutningsvis vil dei viktigaste aspekta summerast og dei ulike refleksjonane knytast saman til ein konklusjon.

## 1.2 Dynamisk vegprising

Dynamisk vegprising eller ei sporingsbasert vegprising inneber avgiftsberekning ved bruk av GPS- og sporingsteknologi. Mens dagens bompengeløysing belastar bilførarar for forbruk når dei passerar gjevne passeringpunkt, inneber dynamisk vegprising ei løysing som alltid sporar køyretøyet og gjev avgifter ut frå dei vegane ein køyrer på (Thon, 2019). Dette resulterer i at store mengder med data samlast inn om kvar bilen har køyrt, kvar den køyrer og kvar den står parkert. Denne nye modellen har ikkje formelt sett fått eit namn, men har ofte vorte omtalt som GPS- eller satellittbasert vegprising, men også dynamisk vegprising. Eg vil gjennom oppgåva referera til modellen på fleire av desse måtane, men har i hovudsak valt skriva dynamisk vegprising.

## 2 Metode

### 2.1 Kvifor teoretisk oppgåve

For å kunna drøfta spørsmåla i problemstillinga og svara på det oppgåva spør om, var det naudsynt å ha ei teoretisk tilnærming. Spørsmåla i problemstillinga søker å gje ei vurdering på om overvaksingsgrada i samfunnet vil auka med dynamisk vegprising, om denne teknologien kan ha uheldige ringverknadar, og om dette kan ha implikasjonar for personvernet. Statistikkar og informantar kan ikkje gje konkrete og målbare opplysningar på eit tenkt tilfelle og teoretisk moglege effektar. Altså må moglege følger og effektar av ein teknologi som ennå ikkje er teke i bruk diskuterast på teoretiske premisser. Det vart difor

viktig å finna ut kva som meinast med overvaking i tillegg til kunnskap om kva personvern er og når dette eventuelt krenkast. Vidare måtte eg forstå dynamisk vegprising, kva konseptet innebar og korleis det fungerte – før eg, med grunnlag i teorien, diskuterte spørsmåla og svara på problemstillinga.

## 2.2 Data og kjelder

Sidan oppgåva er ei teoretisk oppgåve vart det viktig å ha eit solid teoretisk grunnlag. Oppgåva bygger difor på sekundærkjelder i form av data frå faglitteratur og lærebøker. I tillegg har eg også fleire kjelder frå både nasjonalt og internasjonalt lovverk, samt noko prosessdata frå blant anna stortingshøyringar. Faglitteraturen har vorte nytta til å framlegga relevante perspektiv på personvern og overvaking. Norsk og internasjonal lov og rett er innhenta for å få rett og presis kunnskap om rettane knytt til behandling av personopplysningar og personvern som igjen gjev grunnlag for å drøfta problemstillinga.

## 2.3 Metodekritikk og utfordringar

Under arbeidet med oppgåva har det dukka opp fleire utfordringar som bør påpeikast. Nokre av desse er knytt til kjeldene, mens andre har med eigne og fornuftige avgrensingar og metodeval. Sidan oppgåva er ei teoretisk oppgåve vart det lagt stor vekt på kvalitetssikring av kjelder. Teoretisk litteratur og rettsreglar pregar kjeldelista. Samstundes vart det også naturleg å henta empiri frå nettstader og nyheiter. Ei utfordring med dette er at regjeringen.no til dømes ikkje har oppgjeve forfattar av innhald på sidene. Vidare var eg i tvil om det var riktig å sitera personvernbloggen (datatilsynet sin blogg), ein blogg, i ei akademisk oppgåve. På den andre sida representerer begge sidene viktige aktørar i Noreg, regjeringa og datatilsynet som begge har svært nyttig og presis informasjon om overvaking, personvern og GPS-basert vegprising.

Vidare er det ingen tvil om at oppgåva beveger seg inn på eit område med mykje rettsreglar. Ut frå problemstillinga sin karakter i tillegg til dei omfattande og klare lovane som finnast på personvernområdet var det nødvendig å ta føre seg sentrale element frå lovverket. Faren for å meina noko om lov og rett som fell utanfor kompetanseområdet er til stades, men ikkje overhengande stor. Slik oppgåva framstiller lovane som er brukte lukkast det etter alt sannsyn å diskutera viktige prinsipp i lovverket på eit teoretisk nivå utan at det når eit komplekst



juridisk nivå. Det må også understrekes at det aktuelle lovverket er nært knytt til personvernets normative grunnlag og at kjennskap om dette gjev ei klarare forståing av oppgåva.

Etter grundig vurdering vart omgrepsdefinisjonar lagt inn under teoridelen i staden for eige kapittel. Dette fungerte bra og var det mest naturlege valet ut frå oppgåva sin struktur.

## 2.4 Framgangsmåte

Framgangsmåten for å forsøka å løysa spørsmåla i oppgåva, dreier seg om å finna ut kva som kjenneteiknar auka overvaking i tillegg til framgangsmåten for å finna ut korleis ein identifiserer og finner kjenneteikn på kva som kan krenka, eller svekka personvernet. Dette skjer på følgjande måte: forklara overvaking, kva det er, korleis det går føre seg og vidare kva som drivar og mogleggjer overvaking. Vidare vert det sentralt å forklara kvifor personvern er viktig, personvernet sitt normative grunnlag og sentrale prinsipp i norsk personvernlovgjeving. Etter det vil det som har vorte presentert diskutert i analysedelen, der overvakinggrad og personvernets rammer vart satt opp mot dynamisk vegprising. Moglege langsiktige konsekvensar og ulike former for bruk og misbruk av data generert gjennom dynamisk vegprising vert diskutert så vel som moglege tilnæringsmåtar til ulike løysingar på dynamisk vegprising, for å gje tydelege svar på dei tre sentrale spørsmåla i oppgåva.

## 2.5 Empiri

Rettsdata er formelt sett ein del av empirien, men vert gjort greie for i teoridelen av praktiske og strukturelle årsaker. Aktuelle lovar i teksten er blant anna personopplysningsloven og personvernforordningen. Den nye personopplysningsloven sitt vedlegg 1, er personvernforordningen som er ei direkte omsetjing av EU si General Data Protection Regulation. Sidan GDPR er ei forordning og ikkje eit direktiv er omsetjinga heilt bokstavtru (Jarbekk & Sommerfeldt, 2019. s. 35). Det er personvernforordningen artikkel 5 (om grunnleggande prinsipp) og artikkel 25 (om innebygd personvern) som er artikkane som vert anvende i teksten. Vidare tek teksten også for seg den europeiske menneskerettskonvensjonen artikkel 8 om retten til privatliv. Det vert også vist til ei stortingshøyring frå 8. Januar 2019 der direktør i Datatilsynet, Bjørn Erik Thon kjem med sine synspunkt i forhold til dynamisk

vegprising og personvern. Andre sider der informasjon har vorte henta er frå regjeringa og datatilsynet si nettside i tillegg til nokre nyheitssider. Nyheiter vert viste til for å illustrera moment i den pågåande debatten. Desse kjeldene har relevant informasjon som eg har vurdert å vera presise og truverdige.

## 3 Teori

I dette kapitlet skal eg fyrst introdusera omgrepet overvaking og kva som meinast med det, før eg forklarar korleis overvaking kan gå føre seg og til slutt peika på årsaker og konsekvensar ved overvaking.

### 3.1 Overvaking

#### 3.1.1 Kva meinast med overvaking

Overvaking inneber registrering og lagring av opplysningar, ofte om personar; deira åtferd og aktivitetar. Samstundes må det understrekast at, for at innsamling av informasjon skal kunne kvalifisera som overvaking, er føresetnaden at det er av stort omfang, lang varigheit og til ei viss grad ein systematisk framgangsmåte (Schartum, 2010. s. 22). Overvaking kan også forklarast som aktivitet som inneber registrering og lagring av opplysningar, anten ved hjelp av menneskeleg eller teknisk observasjon, skriftlege eller munnlege overleveringar eller elektroniske spor, om hendingar, åtferd og aktivitetar utført av andre menneske (Bye & Sjøe, 2008. S. 53-54).

Myndighetene si overvaking har fyrst og fremst som formål å tryggja innbyggjarane frå truslar som kriminalitet, terror, ulykker, indre og ytre farer osv. som kan oppstå på mange forskjellige område i samfunnet. Dette kan argumenterast for ut frå politisk teori. Liberale filosofar og tenkarar som Hobbes, Locke og Rousseau har vist til ein teoretisk sosial kontrakt, der staten legitimerar seg sjølv ved å tryggja sine innbyggjarar (Kymlicka, 2002). Altså er staten sin legitimitet grunna på at den tilstrekkeleg kan ivareta ei tilfredsstillande grad av tryggleik innanfor statens grenser. Det er difor klart at overvaking frå myndighetene si side er legitim. Likevel vil det alltid vera eit spørsmål om kva som er tilstrekkeleg overvaking og kva som er for mykje (Schartum, 2010. s. 21). Det må også undrstrekast at myndighetene berre er éin aktør, det er også private aktørar, som bedrifter, konsern og institusjonar i tillegg

til kriminelle nettverk og framande makter som også har interesse av informasjonen overvaking gjev (Bye & Sjøe, 2008. s. 53).

### 3.1.2 Korleis overvaking kan gå føre seg

Overvaking går føre seg på mange måtar og på alle område i kvardagen og i samfunnet. Fyrst kan ein peike på det meir opplagde; at myndigheiter og tryggingsorgan overvakar kriminelle nettverk og potensielle terroristar osv. Dette kan skje ved spaning, men også elektronisk; overvaking av internettsøk, telefonavlytting, rørslemønster og meir (Schartum, 2010. s. 198-199). Det interessante er at mesteparten av desse opplysningane ikkje vert innhenta fyrst når ein er mistenkt, men vert kontinuerlig samla og lagra hjå ulike aktørar til ei kvar tid. Mobilen sporar rørsla vår geografisk, det finnast programvare som kan gje tilgang til mikrofonen og avlytte sjølv når ein ikkje er i ein telefonsamtale (Bye & Sjøe, 2008. s. 228) Vidare vert også alle e-postar og internettsøk registrert og lagra hjå tredjepartar. E-post ender opp i logg- og backupfiler og dei som drifrar servaren som e-posten ender opp i kan lesa e-posten. IP-adressa er endå ein ledetråd som kan brukast til å spora aktiviteten vår på internettet (Bye & Sjøe, 2008. s. 229-230). Vidare vert me også overvaka der me går, reiser og oppheld oss. Overvakingskamera finnast over alt og i tillegg til at mobilen avslørar oss geografisk vil også netthandel gjere det (Bye & Sjøe, 2008. s. 68-80). Sist men ikkje minst vert også kvar passering av bomstasjonar og gjevne passeringpunkt i trafikken lagra om oss (Thon, 2019). Her ser ein mange av dei tinga ein gjer i kvardagen som samlar opplysningar om oss og som til slutt ender opp hjå ein ofte ukjent tredjepart. Sjølv om mesteparten av desse opplysningane skal vera utilgjengeleg er det likevel mange aktørar som ønsker desse opplysningane og som kan omsetja dei.

### 3.1.3 Moglege årsakar og konsekvensar ved overvaking

Eit anna aktuelt spørsmål som reiser seg er kva for nokre krefter det er som driv denne utviklinga og førar oss mot noko som liknar eit overvakingssamfunn? Det er ikkje, som enkelte er freista til å hevda, ein konspirasjon mellom statar om å få meir kontroll over sine innbyggjarar, som driver utviklinga. Det er ikkje nødvendigvis slik at myndigheitene utviklar ny teknologi for å overvaka innbyggjarane, men ofte snarare teknologien som stadig gjer det lettare for myndigheitene å følgja med på innbyggjarane (Bye & Sjøe, 2008. s. 52).

Myndigheitene har naturlegvis også, som me har sett, ein legitim grunn til å villa overvaka

innbyggjarane sine, nemleg tryggingsomsyn. Overvaking for å førebygga og stoppa eventuelle kriminelle handlingar, terror, truslar frå framande makter, økonomisk kriminalitet osv. Frå andre hald avskrivast tryggingsomsyn som hovuddrivkrafta bak overvaking, men visar til økonomisk vinning som den viktigaste faktoren. Bye og Sjue skriv at: «...den digitale revolusjonen er primært et resultat av en økonomisk-teknologisk utvikling. Den har gjort mulig en langt mer effektiv administrasjon og flere måter å oppnå maksimal økonomisk vinning på. ... At statene og internasjonale organisasjoner tar elektronisk overvåking i bruk for å sikre sine interesser, er en av flere viktige sider ved utviklingen.» (Bye & Sjue, 2008. s. 52).

Vidare vert det nemnt fire sentrale samfunnskrefter som nyttar seg av og har motiv for elektronisk overvaking: staten og spesielle statlege organ og tenester; private selskap, konsern, bedrifter og institusjonar; private nettverk som driv organisert kriminalitet; og framande makter (Bye & Sjue, 2008. s. 53). Det er ikkje særleg overraskande at desse aktørane nyttar seg av digital overvaking for økonomisk vinning. Ikkje berre det, men også at dei stadig utviklar nye innovasjonar og teknologiar for å få endå meir informasjon om menneske. Kunnskap om enkeltindivid si atferd, rutinar og preferansar er informasjon som er lett omsetteleg på den digitale marknaden.

David Lyon sin oversikt over overvakingstudiar (Lyon, 2007) gjev moglege forklaringar på årsak og konsekvensar av den moderne overvakinga. Dei seier i stor grad det same som Bye og Sjue; at den moderne overvakinga kan sporast til framveksten av den moderne kapitalismen og byråkratisk praksis. Lyon hevdar at noko av det som er med på å driva fram overvaking er konsolidering av administrative fullmakter i nasjonalstatar og incentivet for kapitalistisk kontroll over arbeidskraft, råvarer og marknader og at dette er ein konstant katalysator for overvaking. I tillegg bidreg ønske om rasjonalitet, effektivitet, overskot, variasjon, kontroll og omsorg for innbyggjarane til auka overvaking (Lyon, 2007. s. 68). Konsekvensane av dette vert at det skapast eit konstant behov for innsamling av data og informasjon. Dette driver, ifølgje Lyon, samfunnet mot eit overvakingssamfunn og motivasjonen er fundamentalt økonomisk vinning. Ifølgje Lyon ser ein resultat av dette i kvardagslivet. Enkle daglegdagse gjeremål som betalningar, fotograferingar, bruk av nøklar og nøkkelkort osv. vert meir og meir digitaliserte, meir kostnadseffektive og meir høvelege (Lyon, 2007. s. 69). Samstundes overvaker desse digitale løysingane oss og samlar inn større mengder opplysningar om oss.

## 3.2 Personvern

### 3.2.1 Kvifor personvern er viktig

Eit ikkje uvanleg argument for kvifor personvernet er viktig, er argumentet at det er ein moglegheit for at informasjon om oss kan misbrukast. Ifølgje Lars Fr. H. Svendsen er det likevel noko med personvernet som er nærare knytt til menneske sine eksistensielle kår enn argumentet om misbruk av informasjon (Clemet & Egeland, 2010. s. 15). Ei viss grad av privatliv er ifølgje Svendsen avgjerande for utvikling av relasjonar til andre menneske, i tillegg til eiga personlegdomsdanning. Sjølve årsaka til at me har omgrepet personvern kan på mange måtar knytast til den europeiske menneskerettskonvensjonen artikkel 8, som er gjeldane norsk lov gjennom menneskerettsloven, om retten til respekt for privatliv og familieliv. «*Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse*» (EMK Art. 8). Svendsen skriv vidare at ei privatsfære ikkje er ein luksus, men ei nødvendighet. Han viser til Friedrich Hayek som seier at «*Fridom forutsetter således at individet er sikret en privatsfære, og at det finnes en rekke omstendigheter rundt det som andre ikke kan blande seg inn i*» (Hayek, 1960. s. 240).

Ved ei svekking av personvernet ser ein ikkje openberre fysiske avgrensingar på handlingsromet sitt, ein står ofte tilsynelatande fritt. Dette er likevel berre tilsynelatande, ifølgje Svendsen, for ein vil med dette begynna å leggja band på kva ein seier og gjer (Clemet & Egeland, 2010. s. 23). I denne samanhengen kan ein også nemna formålsutgliding som noko som delvis skjult og over tid, påfører skade. Spesielt tiltak der store mengder opplysningar akkumulerast, systematiserast og brukast. Formålsutgliding vil seie at opplysningane som vert innsamla vert brukt til noko anna enn til det som var det opprinnelege formålet (Ballangrud, 2022). Vidare skriv Svendsen at ein prikk på eit ark seier lite, mens mange prikkar teikna tett saman kan utgjere eit portrett (Clemet & Egeland, 2010. s. 16) Altså vil det alltid vera ein fare for at massiv innsamling av data på ulike område av liva våre vil kunne danne eit svært nøyaktig bilete av oss og kven me er. Dette er spesielt viktig å påpeike med tanke på aktørar utanom staten som ønsker å samla og «sentralisera» enorme mengder av data om befolkninga. Store aktørar som Facebook i tillegg til Amazon har ikkje lagt skjul på sine ambisjonar om å få kjennskap til enkeltindivid. Amazon vil selja deg ting før du veit at du vil kjøpa dei (Simpson, 2014). I tillegg ønskjer Facebook løyse

verdsproblem ved å føre folk saman gjennom deira kanalar og bruk av kunstig intelligens (Zuboff, 2019. s. 403).

### 3.2.2 Personvernet sitt normative grunnlag

Reint normativt ser ein at eit sterkt personvern forsvarast i kraft av rolla og verdien det har i det liberale samfunnet. Fridom frå overvaking og kontroll er ifølgje Svendsen avgjerande for to sentrale element i den moderne liberale staten. Overvaking har direkte påverknad på fridom og ytringsfridom. Ut frå dette påverkast også individet sine handlingar og moglegheit til personlegdomsutvikling (Clemet & Egeland, 2010. s. 18-21).

Svendsen gjev ei grundig forklaring på korleis personvern, ytringsfridom og personlegdomsutvikling heng saman. Han viser til James Rachels sine tankar om at verdien i privatlivsombrekket ligg i vår evne til å kontrollere kven som har tilgang til oss og kven me vel å skapa og utvikla sosiale relasjonar til (Clemet & Egeland, 2010. s. 19). Vår identitet skapast og definerast i stor grad ved vår relasjonsbygging og sosial omgang med medmenneske. Me presenterer ulike sider av oss til ulike menneske, nokon, kanskje nære, deler me mykje med, mens andre deler me mindre med. Det er ikkje det same som at alle er falske, men alle innrettar seg etter dei normene som er gjeldane i den sosiale samanhengen. Dersom me til ei kvar tid overvakast vil me alltid måtte spela på dei sidene av oss sjølv som oppfyller normene til dei som ser oss. Vidare står me i fare for å mista denne evna til å sjølv kontrollere relasjonsbygging og identitetsbygging, dersom, alle veit alt om oss (Clemet & Egeland, 2010. s. 19-21). Dette kan knytast opp mot overvaking og Jeremy Bentham si kjende fengselsteikning han kalla Panopticon, der fangane vert observert til ei kvar tid og uønskt atferd får reaksjonar (Clemet & Egeland, 2010. s. 21). Dersom ein ikkje har ein stad ein kan trekke seg unna, der ein ikkje treng å tilpassa seg dei gjeldane normene, så vil det kunne gå ut over individet si moglegheit til å reflektera, slappe av og utvikla sin eigen personlegdom (Clemet & Egeland, 2010. s. 20). I ein kvardag der ein alltid er overvaka, eller veit at alt ein gjer kan verte sett, vil både individet sin fridom og ytringsfridom verte svekka på grunn av at menneske endrar atferda si når det veit det vert observert. Svendsen skriv: *«Den som ustanselig må tenke over sine handlinger, selv i den enkleste hverdagslighet, har fått en innskrenkning av sitt frie handlingsrom. Når vi overvåker oss selv fordi vi tror vi kan være overvåket av andre, mister vi denne spontaniteten – vår hverdagslige utvungenhet»* (Clemet & Egeland, 2010. s. 21).

### 3.2.3 Neglisjering av personvernet

Daniel J. Solove er også ein som er kritisk til ingenting-å-gøyma argumentet. Solove peikar på nokre potensielle farar ved innsamling av opplysningar: at innsamling av mindre personopplysingar til slutt avdekkjer det som ein kanskje ønsker å skjule. At ein ikkje får vita korleis data vert samla inn, eller kva opplysningar som vert samla inn og bruk av data som opprinneleg var innsamla til eit anna formål. (Solove, 2011. s. 20-24) (Solove, 2011. Truthout). Solove meiner at personvern ikkje får den merksemda som den burde, i takt med den teknologiske utviklinga som mogleggjer masseovervaking på eit heilt nytt nivå. Mangelen kan vera tydelege konsekvensar for folk flest. Solove hevdar at personvernutfordringar manglar fatale utfall (Solove, 2008). Med dette meinast at personvernet si gjennomslagskraft svekkast i mangel på store openbare konsekvensar for folk. Til dømes vart det eit stort fokus og endringar i den internasjonale tryggingpolitikken etter terroråtaket i New York i 2001 (Schartum, 2010. s. 199-200). Ofte er det vanskeleg å retta fokus på potensielle farar og truslar før dei inntreff. Samstundes finnast det også døme på norsk historie som visar oss at ein ikkje bør ta personvern for gitt. Lund-kommisjonen som vart oppnemnt av stortinget for å granska påstandar om ulovleg overvaking av norske borgarar etter 1945 konkluderte i sin rapport som vart framlagt i 1996 at ulovleg politisk overvaking hadde gått føre seg i Noreg etter andre verdskrig (Lund-kommisjonen, 1996).

### 3.2.4 Personopplysningsloven og personvernforordningen

Vårt forhold til personvern har ikkje berre eit normativt grunnlag som gjev idear om korleis ting bør vere, men har også persopplysningsloven og personvernforordningen som gjev eit solid rettsleg grunnlag. Som tidligare nemnt gjennomfører den nye personopplysningsloven frå 2018, EU si personvernforordning (GDPR). Personopplysningsloven er unik for Noreg og supplerer personvernforordningen på område som er opp til dei enkelte landa å fastsetja. Det er personopplysningsloven som gjeld for behandling av personopplysningar.

Personopplysningar definerast i personvernforordningen artikkel 4 (1) som: *«envher 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. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle*

*eller sosiale identitet.*». Personopplysningsloven har blant anna egne føresegner for forholdet til yrings- og informasjonsfridom, tilgangen til behandling av særlege kategoriar (tidligere sensitive personopplysningar) for forskning, arkivformål og statistiske formål i tillegg til føresegner om norsk aldersgrense for barns samtykke til behandling av personopplysningar osv. samt nokre unntak frå føresegner i personvernforordningen artikkel 4 knytt til informasjonsplikt og innsynsrett (Kommunal- og distriktsdepartementet, 2019).

Det er altså EU si personvernforordning som gjev dei sentrale prinsippa i gjeldane lovgjeving rundt personvern og personopplysningar. Personvernforordningen presenterte fleire nye prinsipp som ikkje har vore del av norsk lov tidlegare. Til dømes artikkel 5 i personvernforordningen som etablerer dei grunnleggjande prinsippa som gjeld for all databehandling som fell inn under forordninga. Det er den behandlingsansvarlige som har ansvaret for at desse prinsippa vert følgd (Voigt & von dem Bussche, 2017. Side 87). Prinsippa i artikkel 5 tek utgangspunkt i lovlegheit, rettferd, openheit, formål, nøyaktigheit og lagringstid. Dette inneber at personopplysningar skal: *«a) behandles på en lovlige, rettferdig og åpen måte med hensyn til de registrerte; b) samles inn for spesifikke, utrykkelige angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene...; c) være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for (dataminimering); d) være korrekte og om nødvendig oppdaterte...; e) lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for...; f) behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene...»* (Personvernforordningen art. 5, a-f). Eit anna sentralt prinsipp i personvernforordningen som er relevant i oppgåva er prinsippet i artikkel 25 om kravet til innebygd personvern (Personvernforordningen art. 25).



## 4. Analyse

I analysedelen vil er sjå nærare på når personvernet vert krenka eller svekka ut frå personvernet sitt normative og rettslege grunnlag. Vidare vil eg diskutera langsiktige utfordringar og moglege løysingar i tillegg til drøfting av avsluttande refleksjonar rundt problemstillinga.

### 4.1 Dynamisk vegprising og overvaking

Det vert nødvendig å svara på om dynamisk vegprising kan reknast som overvaking, og dersom det kan, vil det påvirke grada av overvaking i samfunnet? Sjølv om det fyrste spørsmålet kan oppfattast som openbart, er det viktig å sjå på dynamisk vegprising i forhold til kva ein definerer som overvaking. Som tidlegare vist forklarast overvaking som registrering og lagring av personopplysningar. I tillegg må dette gå føre seg over tid, ha eit stort omfang og vera systematisk. Sjølv om ein kan koma opp med ulike løysingar på korleis registrering og lagring går føre seg, som kanskje i tillegg i større grad tek omsyn til personvernet, vil det mest sannsynleg fortsatt dreie seg om registrering og lagring av personopplysningar og difor kunne reknast som overvaking.

Det andre spørsmålet vil i utgangspunktet vere vanskeleg å gje eit nøyaktig svar på i og med at overvakingsgraden i samfunnet er vanskeleg å måle, eller å setja tal på. Samstundes er det mogleg å sjå på den noverande løysinga, og vidare vurderer om den nye løysinga er meir omfattande med tanke på innsamling av opplysningar enn den gamle løysinga. I tilfellet med dynamisk vegprising i forhold til dagens løysing er det inga tvil om at dynamisk vegprising samlar inn større mengder og meir nøyaktige opplysningar. Dette går føre seg til ei kvar tid, mens bilen køyrar eller står parkert – i motsetnad til dagens løysing som berre kan hente inn opplysningar i det bilen passerer ved gjevne passeringpunkt. Ut frå denne argumentasjonen vil ein kunne seie at overvakingsgraden i samfunnet vil auke med dynamisk vegprising. Samstundes har denne argumentasjonen ein del føresetnadar som må oppfyllest: viktigast at den gamle løysinga er mindre personvernorientert enn den nye, noko som ikkje nødvendigvis er tilfellet, men avhenger av korleis ein ny modell løysast ut frå dei sentrale prinsippa i personvernlovgjevinga.

## 4.2 Personvern og dynamisk vegprising

### 4.2.1 Når krenkast eller svekkast personvernet?

Når krenkast eller svekkast personvernet? Ein kan gje svar på dette ut frå to perspektiv, som begge vart presentert i teoridelen: eit normativt perspektiv og eit rettsleg perspektiv. Det normative gjev ei rettleiing for korleis noko bør vere, snarare enn ei skildring av korleis noko er. Personvernet sitt normative grunnlag inneber tanken om at eit privatliv fritt frå overvaking og kontroll er noko av det som skapar moglegheit for utvikling av eigen personlegdom i tillegg til vern av ytringsfridomen. Personvernet er det som vernar om privatlivet og i utvida forståing er personvernet også eit vern for, utvikling og fasthalding av den frie tanke- og ytringsfridomen. Ut frå dette perspektivet vil det som trengjer seg inn på privatlivet, anten det er ved overvaking eller anna innsamling av personopplysningar, slik at ein endrar åtferd og veremåte i kvardagslege gjere mål, vere noko som svekker privatlivet. Her finnast det også rom for diskusjon, som til dømes om bilen og rørslemønster reknast som ein offentleg stad, eller innanfor privatlivets rammer. Likevel, ut frå denne forståinga vil tilfelle der kvardagsleg åtferd endrast på grunn av at ein vert observert og registrert ha negative følgjer for personvern, individets tankefridom og dermed også demokratiet.

Ut frå eit perspektiv som tek utgangspunkt i rettsreglar er det tydeleg enklare å avgjere kva som er ei krenking og ikkje i og med at rettsreglar oftast er klare på kva som er lovleg og kva som er ulovleg. Personopplysningsloven og personvernforordningen kan seiast å byggja på retten til privatliv og rettsreglar har ofte tilknytning til det normative grunnlaget. Samstundes skil det seg klart ved at rettsreglane har tydelege prinsipp som angjev reglane. Som tidlegare nemnt er det prinsippa frå personvernforordningen som etablerer dei grunnleggjande reglane for behandling av personopplysningar: lovlegheit, rettferd, openheit, formål, nøyaktigheit og lagringstid. Ei krenking eller svekking av personvernet vil ut frå norsk lov vera behandling av personopplysningar som ikkje er i tråd med desse, i tillegg til andre deler av forordninga og personopplysningsloven.

#### 4.2.2 Dynamisk vegprising og personvernet sitt normative grunnlag

Teknologien som kjem til å nyttast i dynamisk vegprising mogleggjer ei potensiell stor generering av data om innbyggjarane og brukarane. Dette vil kunna gje myndigheitene stor oversikt og innsikt i folk sine reisevanar og åtferd. Dette systemet kan avsløra mykje om oss, til dømes kvar me arbeider, kvar me går og handlar, hobbyar me praktiserer eller når me er på eit legebesøk. Altså kan ei samling av slik data danna eit tydeleg bilete av kvardagen vår og ikkje minst kva me held på med. Informasjon som dette er nyttig for både myndigheiter og aktørar som ønsker å tena pengar på slik data eller framande makter med verre intensjonar. Korleis ei innsamling av slike mengder data om oss kan vera uheldig skal me også koma inn på seinare.

Som me har sett, hevdar nokon at ei overvaking som dette kan påverka fridomen vår og personlegdomsutviklinga vår (Clemet & Egeland, 2010. s. 20). Altså kan det seiast at ein mister deler av fridomen sin når ein veit at nokon stadig observerer kvardagen eins og meir eller mindre bevisst tilpassar seg etter det. Spørsmålet som reiser seg når ein vurderer denne argumentasjonen er korleis dynamisk vegprising kan påverka køyreåtferda til trafikantar. Ein kan til dømes tenkja seg at nokon vil la vera å bruka bilen når ein skal stader som ein ikkje ønsker at andre skal vita. Eller vel å parkera eit stykke borte frå der ein oppheld seg. Som tidligare vist er det ikkje berre kriminelle som kan ha noko å skjule, men alle kan ha saker dei ikkje ønsker registrert og lagra. Ein veit heller ikkje om registrerte og systematiserte reisevaner kan få følgjer for brukaren i framtida dersom innsamla data vert nyttig for aktørar med andre intensjonar. Uansett vil ein ut frå dette perspektivet kunna argumentera med at køyreåtferd vil endra seg dersom innbyggjarar forstår at dei vert observert. Dette vert også eit spørsmål om tillit. Dersom befolkninga trur at myndigheitene eller andre aktørar til ei kvar til ser kvar bilen er, vil dette kunna endra åtferda uavhengig om det i det heile er mogleg å overvaka enkeltpersonar på denne måten. På den andre sida er det ikkje nødvendigvis så vanskeleg å eliminera dei faktorane som effektivt vil kunna hindra uønskte følge. Aggregering og sletting av data i tillegg til openheit og innsyn er nokre av faktorane som kan bidra til ei meir personvernorientert løysing og at formålet berre vert berekning av avgifter. Dette skal me sjå nærare på.

### 4.2.3 Dynamisk vegprising og personvernforordningen

Tidlegare i teksten er det vist at registrering, lagring og behandling av personopplysningar som ikkje er i samsvar med reglar og prinsipp i personopplysningsloven og personvernforordningen kan reknast som krenking av personvernet og norsk lov.

I dette avsnittet vil dynamisk vegprising som konsept heilt konkret vurderast i forhold til prinsippa i personvernforordningen artikkel 5, der utfordringar ved konseptet vil illustrerast.

A: Det fyrste prinsippet legg vekt på lovlegheit, rettferd og openheit. Etter alt å døme kan dynamisk vegprising gå føre seg på ein måte som har heimel i lov og at behandling går føre seg på ein måte som er rimeleg for å oppnå formålet. Dette inkluderer også openheit om formål og behandling ovanfor den som får sine personopplysningar behandla.

B: Neste prinsipp omhandlar spesifikke, uttrykkeleg angitte og berettigede formål, og at personopplysningane ikkje vidarebehandlast på ein måte som er i strid med formåla. Dette handlar i stor grad om å formulera klare formål, men også å utføre behandling av personopplysningar i samsvar med formåla. Det som alltid vil vera ein fare er formålsutgliding. Spesielt der det akkumulerast store mengder med data knytt til individ si rørsle og posisjon over tid. Som tidlegare nemnt og som skal poengterast seinare i teksten er det mange både statlege og ikkje-statlege aktørar som har stor interesse av denne type data, spesielt dersom den er systematisert og sentralisert. Dynamisk vegprising kjem ikkje nødvendigvis til å koma i konflikt med dette prinsippet, men eventuelle ukklarheiter i formålsformulering vil potensielt ha store konsekvensar.

C: Dataminimering er også eit sentralt prinsipp, altså at så lite personopplysningar som mogleg skal samlast inn. Dette inngår i same argumentasjon som i føregåande prinsipp i tillegg til at di meir opplysningar som samlast di klårare bilete og meir kjennskap får ein av personen som opplysningane samlast inn om.

D, E og F: Dei neste prinsippa omhandlar at behandling av personopplysningar må vera korrekte og oppdaterte og lagrast slik at det ikkje er mogleg å identifisera dei registrerte i lengre periodar, i tillegg til tilstrekkeleg sikkerheit for personopplysningane. Av desse er det særleg lagringstid interessant. Datatilsynet har tidlegare uttalt at dagens vegprisingssystem

lagrar informasjon om passeringar i fem år ut frå bokføringsomsyn, noko som ikkje er særleg personvernvenleg (Thon, 2019. Åpen høring).

Ein ny modell for dynamisk vegprising bør dermed lagra personopplysningar som kan knytast opp mot personar betrakteleg kortare enn dette. Altså er prinsippa som omhandlar formålsutgliding, dataminimering og lagring spesielt interessante i diskusjonen rundt dynamisk vegprising. Dette fordi dynamisk vegprising ut frå denne vurderinga kan få utfordringar med å oppfylle desse prinsippa tilstrekkeleg – usikkerheita ligg i at me ikkje veit korleis ei endeleg løysing ser ut, om den er tilfredsstillende desse prinsippa, eller ikkje.

Når dynamisk vegprising her vert diskutert i forhold til dei sentrale prinsippa i personvernforordningen skjer dette utan at det eigentleg finnast ein opparbeidd ferdig modell for korleis behandling av personopplysningar skal gå føre seg i vegprisingsløysinga. Difor vert det på eit vis berre kasta ljøs på dei største generelle utfordringane som kan oppstå i utforming av ein modell for dynamisk vegprising.

Dette kan til ei viss grad opplevast framstilt som eit verst-tenkeleg-tilfelle og oppfattast som teknologipessimisme. Det er derimot stor grunn til å vera optimistisk med tanke på korleis ein modell for dynamisk vegprising kan verte utforma med omsyn til eit sterkt personvern. Dette er på grunn av prinsippa om innebygd personvern. Innebygd personvern er stadfesta i personvernforordningen artikkel 25 og er difor gjeldane norsk lov. Dei sentrale elementa i innebygd personvern skal sikra at det ved utvikling av løysingar som dynamisk vegprising skal vere i forkant med å byggja personvern inn i sjølve designet til systemet. Ifølgje artikkel 25 skal personvern vera ei standardinnstilling, sikra informasjonstryggleiken frå start til slutt og visa openheit til brukarane. Difor kan ein argumentera med at det er stort sannsyn for at dynamisk vegprising kan utviklast i tråd med dei sentrale prinsippa i personvernforordningen. Samstundes vert det difor viktig å påpeika kva utfordringane rundt å bygga godt personvern er, i utviklinga av ein modell for dynamisk vegprising.

#### 4.2.4 Har dynamisk vegprising implikasjonar på personvernet?

Ut frå momenta som er framlagde ser ein at auka overvaking av trafikantar ved dynamisk vegprising i teorien vil kunna endra på den kvardagslege åtferda til trafikantar. Om dette også vil skje i praksis er vanskeleg å seie noko om. I tilfellet at ei personvernvenleg løysing vert

teken i bruk er sannsynet også stor for at den opplevde overvakinga er til stades og vil ha same åtferdsendrande effekt. Difor vil openheit og innsyn om korleis data behandlast og slettast vera viktig for å motverka opplevinga av overvaking. Åtferdsending grunna auka overvaking kan ifølgje føregåande argumentasjon reknast som eit dramatisk inngrep i privatlivet (Clemet & Egeland, 2010. s.20). Vidare har det vorte påpeika at dynamisk vegprising på generelt grunnlag kan møta utfordringar i samband med sentrale prinsipp i personvernforordningen knytt til formålsutgliding, dataminimering og lagring. På den andre sida er det pålagt ved lov å byggja personvern inn i nye løysingar, difor er det sannsynleg at utfordringane nemnt ovanfor vil vurderast nøye ved utforming av ein modell for korleis dynamisk vegprising kan gå føre seg.

Altså ser ein at dynamisk vegprising og auka overvaking som følgje av denne modellen, har moglegheit til å få negative implikasjonar for eit tilstrekkeleg personvern for biltrafikanter. Samstundes kan også negative implikasjonar motverkast ved å byggja godt personvern inn i modellen, med omsyn til sentrale prinsipp. Om dynamisk vegprising kan skje i samsvar med godt personvern er nettopp avhengig av korleis ein ferdigstilt modell for dynamisk vegprising ser ut. Med dette sagt er det framleis mange moment som ein bør gjerast merksam på i forhold til vurderinga om dynamisk vegprising ved ei aller annan anledning kan få implikasjonar for personvernet.

### 4.3 Potensielle langsiktige utfordringar

Dersom ein i eit langsiktig perspektiv legg til faktoren tid vil ein ofte få større grad av uforutsigbarheit. Her vil eg trekkja fram to moment: Korleis staten kan endra på tilnærminga til dynamisk vegprising og korleis andre aktørar kan kome til å dra nytte av dynamisk vegprising i eit langtidsperspektiv.

#### 4.3.1 Staten

Ein personvernvenleg modell for dynamisk vegprising vil innebera at store mengder data samlast inn, men at den ikkje brukast til anna enn formålet, som berre vil vera å berekna avgift for køyring. Det er ingen tvil om at formålsutgliding kan førekoma i eit langtidsperspektiv. Det er store mengder av personopplysningar som kan nyttast til mykje meir enn berre berekning av avgifter. For det fyrste kan desse brukast på mange måtar som

kan vere lønsame for staten. Eit døme på dette kan vera å utvida formålet og bruken av dynamisk vegprising til å bøtleggja fartsovertredingar eller andre ulovlege køyremønster. Det vil frigje ressursar for politiet og arbeidet vil gå føre seg meir nøyaktig og effektivt - alle overtredelsar vil fangast opp. Frå eit lønsamheitsperspektiv er det lite som talar imot at det hadde vore ei fornuftig løysing. Ein må ikkje gløyma at også staten er driven av eit ønske om økonomisk innbringande system. For det andre kan staten nytta data frå dynamisk vegprising til tryggingstiltak. Staten kan til dømes, med grunngjeving i omsyn til tryggleik, nytta dynamisk vegprising som ein overvakingsmekanisme som kan avdekka eller førebygga til dømes terror og kriminalitet, men også smittesporing eller for å avgrensa innbyggjarane si ferd. Det som denne argumentasjonen dreier seg om, er frykta for at dersom dynamisk vegprising vert eit ledd i eit utvida overvakingssamfunn, vil dette før eller seinare kunne misbrukast av staten. Anten ved formålsutgliding, som kan oppstå over tid, eller total formålending, til dømes ved at staten vert totalitær.

Altså er argumentet at dersom me byggjer ferdig ein infrastruktur av overvakingsmekanismer, vil den ha potensiale til å brukast til ulempe for innbyggjarane og for demokratiet. Eit motargument til dette er at det er lite som tyder på at staten er i ferd med å verte totalitær, i tillegg til at dersom me skal basera alle funksjonar og system i samfunnet på at dei før eller sidan kan brukast mot innbyggjarane, vil ein kanskje få eit meir teknologisk-skeptisk samfunn enn nødvendig. Samstundes er det kanskje nettopp denne underliggende skepsisen til nye og omfattande system som fører til fokus på personvern. Som igjen er nødvendig for å sikra at modellar for system som dynamisk vegprising, vert sett saman og oppbygde personvernorienterte snarare enn eit bidrag til ein infrastruktur av overvakingsmekanismer.

#### 4.3.2 Overvakingskapitalismen

Det andre aktuelle spørsmålet er om dei faktorane som driver utviklinga av overvakinga kan koma til å forma modellen for dynamisk vegprising, eller om dei på eit eller anna tidspunkt vil kunn dra nytte av data samla gjennom dynamisk vegprising. Som nemnt viser David Lyon at ønsket om kapitalistisk kontroll over marknaden, arbeidskraft og råvarer er ein sentral faktor i utvikling og oppretthalding av overvaking. Altså er det kapitalistiske aktørar som har stor økonomisk fortjeneste av data som vert innhenta ved bruk av overvaking. Shoshana Zuboff, forfattar av den internasjonalt anerkjente boka «The Age of Surveillance Capitalism»

går endå eit steg lenger i si vurdering av kor nært kapitalismen er knytt til overvaking i dagens samfunn. Ho kallar denne nye økonomiske modellen for overvakingskapitalisme og forklarar den som ein ny økonomisk orden, som tek menneskelege erfaringar som råvarer og brukar dette i skjulte reklamepraksisar for å utvinna, føreseia og selja. (Zuboff, 2019. s. 8) Zuboff seier at dette endrar på heile marknadsmodellen, der dei ikkje lenger ser på forbrukararen som ein forbrukar, men ein ressurs som gjev gratis råvarer til den nye marknadsmodellen som handlar om å føresjå åtferda til grupper og individ (Zuboff, 2019. s. 392-393). Varer og tenester som selgast har difor ofte funksjonar som samlar data om oss og vårt bruk og forbruk av desse. Overvakingskapitalistane sitt argument er at dette skal forbetra vår brukaroppleving av produktet, men ut frå Zuboff sitt perspektiv vil det tvert imot brukast til å forstå og føresjå menneskeleg åtferd. Her ser ein Facebook sin visjon som eit klart eksempel på dette. Ifølgje Facebook-sjef og grunnleggjar Mark Zuckerberg er Facebook sin visjon å knytta saman alle menneske til noko større enn oss sjølv – og dette noko vil vera Facebook. Facebook skal kunne løysa vår tids store utfordringar ved å byggja ein «langtids infrastruktur» som skal bringa menneskeheita saman og halda oss trygge ved bruk av kunstig intelligens som fort skjønar rørsleane i samfunnet. Dette systemet vil ifølgje Zuckerberg kunne oppdage truslar som ingen i det heile har tenkt på (Zuboff, 2019. s. 403). Ifølgje Zuboff går me frå alderen der maskinane vart brukte for å gjere oppgåver som me ikkje evna, til ei tid der maskinar skal føresjå og endra menneskeleg åtferd (Zuboff, 2019. S. 404). Her er det ikkje berre Facebook som er aktør, men stadig fleire internasjonale aktørar, men også mindre selskap og organisasjonar. Marknadsmodellen i overvakingskapitalismen inneber innsamling og bruk av data som genererast ved bruk av varer og tenester. Her kan ein stilla spørsmål ved om desse aktørane også kan ha interesse av data generert gjennom dynamisk vegprising. Eller kanskje endå meir aktuelt, om det i det heile vil vera mogleg å byggja og oppretthalda ein modell for dynamisk vegprising som ikkje gjev etter for den nye marknadsmodellen som er i emning?

Spørsmåla er meir enn aktuelle, dei er nødvendige i utforminga av dynamisk vegprising, eller vurderinga om denne modellen bør utformast i det heile. Konsekvensane av overvakingskapitalismen vil ifølgje Zuboff få store følgjer for demokratiet som institusjon. Når overvakingskapitalismens løysingar inneber at kunstig intelligens kan føresjå og endra menneskeleg åtferd vil dette ha potensiale til å gjere alle ting meir effektive og komfortable, vidare også eliminere uforutsigbarheit, spontanitet, truslar og kaos osv. (Zuboff, 2019. s. 404). Me gjev dermed ifrå oss kontroll og fridom til dei teknologiaktørane som kontrollerer



systema som føreser og endrar åtferd. Blant fleire av krenkingane mot demokratiet som Zuboff løfter fram er nokre sentrale av dei utvinning av menneskelege erfaringar, modifikasjon av menneskeleg åtferd og degraderinga av individet som kardinalpunktet i samfunnslivet (Zuboff, 2019. s. 406). Zuboff oppsummerar med at overvakingsskapitalismen virker å dominera meir enn det ein skulle tru det neoliberale demokratiet kan tillata. Den gjer krav på fridom og kunnskap og siktar seg inn på eit kollektivistisk samfunn med kunstig intelligens i kontroll (Zuboff, 2019. s. 406-407). Spørsmålet til slutt vert om me etablerer formål og konstruerer løysingsmodellar for dynamisk vegprising på ein slik måte at me på eit eller anna tidspunkt tillét at aktørane innanfor overvakingsskapitalismen får utnytta også dei data som samlast der.

## 4.4 Tiltærming til løysingar

### 4.4.1 Moglege løysingar

I dette avsnittet presenterast ulike løysingsmodellar for dynamisk vegprising, som kanskje kan vera aktuelle alternativ for personvernvenleg dynamisk vegprising. Datatilsynet, ved direktør Bjørn Erik Thon har gjennom datatilsynet sin blogg, personvernbloggen, i tillegg til innspel i open høyring i stortinget, gjeve klart uttrykk for sine synspunkt rundt dynamisk vegprising. Datatilsynet stiller seg i utgangspunktet positive til ei ny form for vegprising. Ei av årsakene til dette er ifølgje Thon at dagens bompenger-løysing ikkje er særleg personvernvenleg sidan opplysningar om passeringar lagrast i fem år (Bjørn Erik Thon, 2019. Åpen høring). Vidare gjer han det klart at ei løysing som nyttar seg av GPS- og springsteknologi kan vera mogleg å gjennomføra dersom personvernet vert ivarettatt. Thon skriv blant anna: *«I tillegg til riktig bruk av teknologi er full åpenhet om hvilke data som lagres, hva dataene brukes til og full innsynsrett for den enkelte helt vesentlig. Det må fastslås, gjerne i lovs form, at kjøredata kun kan brukes til ett formål, nemlig å beregne hvor mye vi skal betale for bilkjøringen vår»* (Thon, 2019).

Datatilsynet peikar på to moglege løysingar som dei meiner kan vera aktuelle. Den eine løysinga inneber at køyredata lagrast lokalt i køyretøyet før data aggregerast og sendast til ei sentral eining som reknar ut avgifter. Desse avgiftene reknast ut basert på til dømes kor mange kilometer ein har køyrt i sentrum, på landeveg osv. Det andre løysingsforslaget baserar seg på at køyretøyet har ei anonym digital lommebok som belastast fortløpande mens

ein køyrar, litt som eit kontantkort, utan at systemet registrerar kvar ein køyrar (Thon, 2019. Åpen høring). Begge desse løysingsforslaga er tydelege døme på korleis ein kan forsøka å bygga personvernomsyn inn i ein ny vegprisindemodell, som vil vera meir personvernvenleg enn løysinga me har i dag. Det å byggja personvern inn i løysingar er ein eigen politikk og bør baserast på ei rettighetstenking som handlar om at visse prinsipp ikkje kan handlast vekk (Sejersted, 2002. S. 58-59). Dette inneber at ein føreåt for utviklinga av løysinga set prinsipp for kva som er ønska og uønska frå teknologien. Samstundes som veit me ikkje korleis denne løysinga vil sjå ut på lang sikt, og om data kan nyttast til andre formål òg. Difor vil det kanskje vera nødvendig slik Thon foreslår, å slå fast i lovs form at køyredata berre skal brukast til eitt formål.

#### 4.4.2 Avsluttande refleksjon

Når ein ser på dei alternativa ein står att med, må ein anten fortsetja med den eksisterande forma for vegprising som har mindre grad av overvaking, men ifølgje datatilsynet eit svakare personvern, eller koma med ei ny løysing for vegprising, dynamisk vegprising, med større grad av overvaking, der personvernets integritet er heilt avhengig av kva løysing som vert teken i bruk. Her er det grunn til å vera optimistisk med tanke på moglegheita til å byggja inn eit sterkt personvern i dynamisk vegprising.

Me kan skimta i samfunnet i dag og spesielt i samband med den teknologiske utviklinga at det er ei forventning om at staten stadig skal levera fleire og meir effektive tenester til innbyggjarane. Dette ser ein i avdekking av kriminalitet, berekning av skatt og avgifter i tillegg til velferdsgodar. Svendsen påpeikar denne tendensen svært presist: «*Dagens ideologiske klima er slik at de prinsipielle argumentene for liberale rettigheter synes å komme til kort overfor en serie pragmatiske tiltak som skal løse presumtivt pressende problemer – og hvor det ikke er tid til å reflektere nevneverdig over hvordan alle disse forandrer samfunnet vi skal leve i* (Clemet & Egeland, 2010. s. 24). Omsynet til tryggleik og nytte vert ofte brukt i argumentasjonen rundt individet sitt krav på fridom, personvern og privatliv og kvifor dette kan lempast på til fordel for samfunnet sitt beste. Som me har sett er det minst to store aktørar som har eit ustansleg behov for data og opplysningar om menneske. Den eine er statlege aktørar som potensielt kan bruka og misbruka data generert frå dynamisk vegprising, dersom staten over tid endrar meining om kva formålet bør vere – noko som kan få innverknad på individuell fridom og personlegdomsutvikling. Den andre

aktøren er det Zuboff kallar for overvåkingskapitalistane, som brukar opplevingar og data som råvarer til å utvikla kunstig intelligens, der målet er å modifisera menneskeleg åtferd til fordel for menneskeheita. Kostnaden vert derimot ifølgje Zuboff ei svekking av demokrati, personvern, retten til privatliv og sjølve moglegheita til å gjere frie val (Zuboff, 2019).

## 5. Konklusjon

Innleiingsvis vart det reist tre spørsmål rundt dynamisk vegprising. Det første spørsmålet var om dynamisk vegprising kan påverka omfanget av overvaking i trafikken? I oppgåva vart det vist at konseptet dynamisk vegprising slik som det her har vorte presentert aukar omfanget av graden av overvaking i trafikken. Dette grunngjevast med at dynamisk vegprising registrerar og lagrar personopplysningar over tid i tillegg til at dynamisk vegprising vil registrera og lagra køyremønster på eit langt meir nøyaktig og omfattande vis, enn dagens vegprisingsmodell.

Det andre spørsmålet, om løysinga vil få fleire formål enn berre berekning av avgifter visast i argumentasjonen om formålsutgliding som ein overhengande fare. Ved å innføra ein dynamisk vegprisingsmodell vert store mengder data generert. Personopplysningar vil samlast, systematiserast og lagrast. Akkumulering av slike data kan over tid gje grobotn for formålsutgliding som igjen mogleggjer at myndigheiter eller andre aktørar brukar data generert gjennom vegprising til andre formål. På den andre sida kan sannsynet for formålsutgliding reduserast ved tydelege rammer og lovvedtak. Dei andre formåla denne mengda med data kan nyttast til er i hovudsak motivert av økonomisk forteneste og tryggingstiltak.

Det tredje spørsmålet, om moglege implikasjonar på personvernet forklarast først ut frå prinsippa rundt personvern. Det peikast på at dynamisk vegprising står i fare for slita med å oppfylle tre sentrale prinsipp i personvernforordningen. Dette er prinsipp om formålsutgliding, dataminimering og lagring. Det er på desse områda det kan identifiserast svakheiter med dynamisk vegprising som vil få implikasjonar for personvernet dersom desse ikkje utformast etter gjeldane lov og rammer. På den andre sida er det ingen tvil om at potensielle utfordringar ved desse prinsippa kan løysast ved å ta på alvor prinsippet om å byggja personvern inn i løysingane. Det som konkret vil vera avgjerande for om dynamisk

vegprising har implikasjonar for personvernet er korleis løysingsmodellen for dynamisk vegprising vert konstruert og eksekvert. Dersom modellen omfattar personvernvenlege løysingar på områda dataminimering og lagring og førebygger sjansen for formålsutgliding vil den kunna ivareta eit godt personvern.

Svaret på problemstillinga er altså at innføring av dynamisk vegprising vil auka grada av overvaking i trafikken. Vidare vil ein modell for dynamisk vegprising som i liten grad tek omsyn til sentrale personvernprinsipp og moglege langsiktige konsekvensar kunna gje negative implikasjonar for personvernet. Samstundes vil ein løysingsmodell som byggjast med fokus på personvern og omsyn til sentrale prinsipp og potensielle langsiktige konsekvensar kunna unngå negative implikasjonar for personvernet i trafikken.

Alt dette gjev oss eit bilete av korleis dei grunnleggjande tankane og ideane som har vorte presentert i oppgåva heng saman med dei potensielle konsekvensane av lite personvernvenlege løysingar. Tanken om at meir kunnskap og kjennskap til brukarar gjev dei som har opplysningane kontroll over desse, ser ut til å bekreftast av korleis store multinasjonale aktørar brukar menneske sine opplevingar som råvarer. Dei søker å føresja menneskeleg åtferd i tillegg til å kunna modifisera åtferda. Som vist i oppgåva kan overvaking som fenomen påverka menneskeleg åtferd og som følgje av dette står det frie individet, ytringsfridom og dermed også demokratiet på spel. Denne problematikken er samstundes identifisert tidligare, noko som ein ser i eksisterande lovar som retten til privatliv, personopplysningsloven og personvernforordningen.

Det avgjerande er om me klarer å retta oss etter prinsippa me har satt og ta inn over oss alvorret i desse prinsippa. Personvern må byggjast inn i løysinga frå botn, det er difor desto viktigare å vera tidleg ute med dei djuptgåande spørsmåla og den nødvendige faglege diskusjonen, allereie i konseptualiseringa av dynamisk vegprising.

## 6. Litteraturliste

### 6.1 Teoretiske kjelder

- Bye, R., & Sjøe, F. (2008). *Overvåket*. Oslo: Gyldendal Akademisk.
- Clemet, K., & Egeland, J. O. (red.) (2010). *Til forsvar for personvernet: Hvorfor personvern?* Oslo: Universitetsforlaget.
- Hayek, F. (1960). *The Constitution of Liberty*. Chicago: University of Chicago Press.
- Jarbekk, E., & Sommerfeldt, S. (2019). *Personvern og GDPR i praksis*. Oslo: Cappelen Damm Akademisk.
- Kymlicka, W. (2002). *Contemporary Political Philosophy*. Oxford: Oxford University Press.
- Lyon, D. (2007). *Surveillance Studies: An Overview*. Polity Press.
- Schartum, D. W. (red) (2010). *Overvåking i en rettsstat*. Bergen: Fagbokforlaget.
- Sejersted, F. (2002). *Er det mulig å styre utviklingen?* Oslo: Pax forlag.
- Solove, D. J. (2008). *Understanding Privacy*. Harvard University Press.
- Solove, D. J. (2011). *Nothing to Hide: The False Tradeoff between Privacy and Security*. Yale University Press.
- Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Berlin: Springer Nature.
- Zuboff, S. (2019). *The Age of Surveillance Capitalism: The fight for a human future at the new frontier of power*. London: Profile Books.

### 6.2 Rettskjelder

- Europaparlamentet. (2016, 05 04). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. From EUR-Lex: <http://data.europa.eu/eli/reg/2016/679/oj>
- Menneskerettsloven – mrl. (1999). Lov om styrking av menneskerettighetenes stilling i norsk rett. (LOV-1999-05-21-30). Lovdata. <https://lovdata.no/lov/1999-05-21-30>
- Personopplysningsloven. (2018). Lov om behandling av personopplysninger. (LOV-2018-06-15-38). Lovdata. <https://lovdata.no/lov/2018-06-15-38>

Den europeiske menneskerettskonvensjon (1953) (EMK)

### 6.3 Andre kjelder

- Ballangrud, A. (2022, 3 25). *Ingenting å skjule: formålsutglidning og nedkjølingseffekt*. Frå Datatilsynet: <https://www.datatilsynet.no/regelverk-og-verktoy/personvernpodden/2022/7-ingingting-a-skjule-formalsutglidning-og-nedkjolingseffekt/>
- Kommunal- og distriktsdepartementet. (2019, 10 30). *Regjeringen.no*. Frå Ny personopplysningslov: <https://www.regjeringen.no/no/tema/statlig-forvaltning/personvern/ny-personopplysningslov/id2340094/>
- Lund, K. Et. al. (1996). Dokument nr. 15 (1995-1996). *Rapport til Stortinget fra kommisjonen som ble oppnevnt av Stortinget for å granske påstander om ulovlig overvåking av norske borgere («Lund-rapporten»)*. <https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Dokumentserien/1995-1996/Dok15-199596/?lvl=0>
- Simpson, C. (2014, 1 20). *Amazon Will Sell You Things Before You Know You Want to Buy Them*. From The Atlantic: <https://www.theatlantic.com/technology/archive/2014/01/amazon-thinks-it-can-predict-your-future/357188/>
- Solove, D. J. (2011, 7 7). *Nothing to Hide: The False Tradeoff Between Privacy and Security*. Retrieved from Truthout: <https://truthout.org/articles/nothing-to-hide-the-false-tradeoff-between-privacy-and-security/>
- Thon, B. E. (2019, 1 8). *Privatliv langs veien*. Frå Personvernbloggen: <https://www.personvernbloggen.no/2019/01/08/privatliv-langs-veien/>
- Thon, B. E. Direktør i Datatilsynet, Åpen høring i stortingets transport- og kommunikasjonskomité tirsdag 8. Januar 2019 kl. 10.55. Open høring i følgane saker: Dokument 8:26 S (2018-2019), Dokument 8:35 S (2018-2019). <https://www.stortinget.no/no/Hva-skjer-pa-Stortinget/Videoarkiv/Arkiv-TV-sendinger/?mbid=/2019/H264-full/Hoeringssal1/01/08/Hoeringssal1-20190108-105256.mp4&msid=2144&dateid=10004257>