SINTEF Teknologi og samfunn
Postadresse:
Postboks 4760 Sluppen
7465 Trondheim

Sentralbord: 73593000

ts@sintef.no
www.sintef.no
Foretaksregister:
NO 948 007 029 MVA

Notat

Utprøving av selvkjørende kjøretøy på vei

Innspill til utkast til ny lov

SAKSBEHANDLER / FORFATTER
Stig Ole Johnsen,
Terje Moen

GÅR TIL	BEHANDLING	UTTALELSE	ORIENTERING	ETTER AVTALE
Samferdselsdepartementet	X			
Roar Norvik, forskningssjef SINTEF Teknologi og samfunn	X			
Richard Liodden Sanders, forskningssjef SINTEF Digital	X			

PROSJEKTNR / SAK NR	DATO	GRADERING
102015192-3	2017-03-01	Åpen

1 Bakgrunn

Samferdselsdepartementet sendte den 13.12.2016 ut et høringsnotat med utkast til ny lov om utprøving av selvkjørende kjøretøy på vei. Høringsfristen er 1. mars 2017.
Det må stilles krav til innholdet i en søknad om tillatelse til utprøving av selvkjørende kjøretøy (via egen forskrift), hvor det bør spesifiseres et eget søknads-skjema hvor all nødvendig informasjon dokumenteres.
Vi har i det følgende kommentert lovteksten ved å diskutere utvalgte problemstillinger knyttet til sikkerhet samt gått gjennom merknader til lovteksten. I kapittel 3 har vi laget en tabell der vi gir spesifikke innspill til det foreslåtte lovforslaget for hver paragraf.

1.1 Hovedformål og område

Hovedformålet med lovforslaget er å fastsette et rettslig grunnlag for å kunne prøve ut selvkjørende kjøretøy uten en ansvarlig fører på tradisjonell førerplass. Ellers nevnes det at utvikling med selvkjørende kjøretøy forventes å påvirke ulykkesutviklingen i positiv retning, slik at den nye teknologien antas å kunne bidra til færre og mindre alvorlige ulykker. Områder for uttesting/forsøk er beskrevet kort, men en tenker på:

- Småbusser konstruert uten tradisjonell førerplass
- Selvkjørende kjøretøy uten tradisjonell førerplass for godstransport

- "Platooning", hvor flere lastebiler er koblet og blir ført av den første i rekken
- Personbiler konstruert med tradisjonell førerplass, med selvkjørende teknologi som ønskes testet, ved selvkjøring på motorveg og ved parkering uten fører.

En kan også inkludere nye funksjoner som selvkjørende kjøretøy for frakt av gående og syklende gjennom tunneler, der adgang for disse normalt er forbudt.

Utprøving av autonome kjøretøy i Norge kan gi industri og forskningsmiljø muligheter for vekst og konkurransefortrinn, ved at vi kan ligge i forkant av utviklingen ikke minst i grensesnittet mellom teknologi og samfunnets utnyttelse. Norge har i mange sammenhenger vært langt fremme på teknologiutvikling i et samfunnsperspektiv, noe som både gir kostnadsreduksjoner og økt konkurransekraft via innovasjoner. Det nevnes at variasjoner på vegnettet, krevende topografi (herunder bruk av tunneler), samt særlige klimatiske forhold i Norge kan være utfordrende å håndtere. Dette kan også være et konkurransefortrinn ved utvikling, ved at teknologi som fungere under så krevende forhold som i Norge, også vil fungere andre steder.

1.2 Problemstillinger knyttet til sikkerhet

Det er meget tilfredsstillende at det kommer et forslag til lov om utprøving av selvkjørende kjøretøy, ved å være proaktiv kan man bygge opp kompetanse og legge grunnlaget for å oppnå færre og mindre alvorlige ulykker. Loven må være såpass detaljert og forståelig at man slipper en runde innen rettssystemet hver gang det skjer noe. I det følgende har vi kommet med synspunkter på lovteksten ut fra et sikkerhetsperspektiv:

1) Det pågår utprøving av autonome fartøyer på sjø, i luft og på bane i Norge. Det er derfor fornuftig å utveksle erfaring og i en viss grad koordinere arbeidet med regelverk for alle områdene.
2) I forbindelse med forskning på selvkjørende kjøretøy, er det behov for en utvidet tilgang til informasjon og lagring av data, samtidig som personvernet ivaretas.
3) Et autonomt kjøretøy er programmert av en leverandør, ansvaret for en uønsket hendelse med selvkjørende kjøretøy (uten en ansvarlig fører på tradisjonell førerplass) må da ligge på leverandøren.
4) Sikkerhetsforskningen har vist at uønskede hendelser er en konsekvens av både tekniske, organisatoriske og menneskelige faktorer, samt at vellykket håndtering gir oss bedre innsikt i viktige faktorer for sikkerheten. Det er derfor viktig at en har et bredt systemperspektiv på analyse av uønskede hendelser og at en også dokumenterer vellykket gjenvinninger.
5) Et moderne kjøretøy består av mange datakomponenter og koplinger som er svært sårbar for bevisste hendelser som hacking (security) og tilfeldige hendelser (safety). Det er derfor viktig at en allerede nå benytter "føre-var-prinsippet" for produktgodkjenning og læring. En bør vurdere hvilke mekanismer som kan brukes for å godkjenne utstyr og hvordan en kan styrke læringsprosessen på nasjonalt nivå av hendelser via etablerte strukturer som CERT (Computer Emergency Response Team).
6) Forbedring av sikkerheten og tilpassede forsikringsordninger er helt avhengig av åpen transparent rapportering av hendelser. Hendelsene må gjøres kjent mellom alle

aktørene som er involvert i verdikjeden for kjøretøy. Det er derfor viktig at en allerede nå legger vekt på åpenhet både for safety og security hendelser. Fartøy som er fjernstyrt og delvis autonom (eks. Droner) har hatt flere uhell enn bemannede bl.a. på grunn av utfordringer med grensesnittet mellom operatør og droner, det er viktig at erfaring mellom forskjellige områder deles for å få tilgang til større variasjonsbredde og volum av erfaringer.

2 Merknader til ny lov om utprøving av selvkjørende kjøretøy på veg

Vi har i det følgende reflektert og kommet med synspunkter på de momentene som var nevnt innledningsvis:

1. Å koordinere utprøving med autonome fartøyer på sjø, i luft og på bane
2. Informasjonstilgang og lagring av data, innenfor rammene for personvern
3. Leverandørens ansvar for selvkjørende fartøyer
4. Et systemperspektiv på uønskede hendelser og vellykket gjenvinninger
5. Behandling av bevisste hendelser (security) og tilfeldige hendelser (safety)
6. Åpen transparent rapportering av hendelser

I lovforslaget benyttes gjentatte ganger begrepet *tilsynsmyndighet*, uten at det er definert hvem dette er. Denne myndigheten bør defineres. Tilsynsmyndigheten har ansvaret for sikkerhet og sikring (dvs Safety og Security). Det må beskrives hvordan læring fra uønskede hendelser skjer som f.eks. via CERT funksjonen (Computer Emergency Teams). Utbredelsen av Intelligente transportsystemer (ITS) vil øke, det er derfor viktig at en bringer inn kompetanse på ny teknologi og håndtering av nye fremvoksende risikoer til tilsynsmyndighetene. Håndtering av risiko for nye hendelser (såkalt ”emerging risks", nye typer risikoer) og læring av nye hendelser har vært utfordrende.

2.1 Koordinere utprøving med autonome fartøyer på sjø, i luft og på bane

Det er pågående arbeid i Norge for å prøve ut autonome og ubemannede fartøy både på sjø, luft og bane - det kan være fornuftig at erfaring, rammebetingelser og lovverk koordineres i en viss grad mellom sjø, luft og bane. Det er snakk om forskjellige nivå av autonome fartøyer, dels med fjernstyring fra kontrollrom og/eller fullt autonome fartøy, hvor det er forskjellige grader av autonomi, hvor det er nyttig å samle erfaringer fra de forskjellige nivåene. Det er bl.a. etablert et test-område for autonome skip i Trondheimsfjorden, hvor Kystverket og Sjøfartsdirektoratet er involvert, se NFAS (2016) og Kystverket (2016).
Det er forskjellig grad av autonomi i luftfart, fra fly med piloter (med autopilot) til førerløse fly (droner). Droner kan være helt eller delvis autonome men det er vanligvis en operatør som sitter i et kontrollrom på bakken som styrer dronene. For droner styrt av operatør, RPAS (Remotely Piloted Aircraft Systems) er det laget en egen "Forskrift om luftfartøy som ikke har fører om bord mv." med ikrafttredelse 01.01.2016, se Luftfartstilsynet (2016). Der er det operatøren som har ansvaret ved hendelser. Med hensyn til opplæring av de som fører ubemannede droner, må man fra 2017 bli sertifisert for å kunne operere ubemannede luftfartøy, se Luftfartstilsynet (2017). Flygere av litt større droner må bestå en eksamen for å kunne utføre flyging og fra 2. januar 2017 kan eksamen gjennomføres ved trafikkstasjoner i Norge.

For sjø vil det være naturlig at eier av skipet har et (utvidet) objektivt ansvar for operasjonen, men også her bør en forvente at systemleverandør tar et utvidet ansvar for at systemet fungerer som spesifisert som en del av sin leveranse til eieren av skipet.

Lovgiving, rutiner og praksis har forskjellig modenhet, men det kan være nyttig å koordinere arbeidet og erfaringsinnhenting mellom veg, sjø, luft og bane.

2.2 Informasjonstilgang og lagring av data innenfor rammen av personvernet

I forbindelse med forskning på selvkjørende kjøretøy, er det behov for en utvidet tilgang til informasjon og lagring av data. Dette må skje innenfor rammen gitt av den eksisterende personopplysningsloven og den nye personopplysningsloven som trer i kraft i 2018, EU (2016:679). Vi foreslår at persondata skal kunnen avidentifiseres.

Høringsnotatet beskriver i avsnitt 6.12 behovet for å lagre bilde- og lydopptak som erfaringsmateriale for å kunne videreutvikle systemene. Dette behovet gjelder også andre typer informasjon fra ulike sensorer både i og utenfor kjøretøyet. Lovteksten beskriver at bildemateriale skal avidentifiseres før det lagres. Dette er et generelt krav det er vanskelig å oppfylle. Det er for eksempel svært krevende å avidentifisere videoopptak av gående og syklende utenfor det selvkjørende kjøretøyet når en vil studere atferden disse har i møte med selvkjørende kjøretøy. Forskningsbedrifter har rutiner for å lagre og håndtere denne typen informasjon på en sikker måte og disse vil søke Datatilsynet om slik tillatelse.

Det kan være aktuelt at forsikringsbransjen får tilgang til noe data i forbindelse med prosjekter der vurdering av risikoer ved selvkjørende kjøretøy inngår, men det er ikke aktuelt å dele tilgang til bilde og lydmateriale. Dette beskrives nærmere i kapittel 2.6. Politi og påtalemyndighet må få tilgang til all informasjon der kjøretøyet har vært innblandet i en ulykke.

2.3 Leverandørens ansvar for selvkjørende fartøyer

I det følgende har vi fokusert på selvkjørende kjøretøy på veg (dvs. biler). Det sies: ”*I de tilfellene det i tillatelsen er gjort unntak fra føreransvaret, er den som har fått tillatelse, ansvarlig for at sikkerheten er ivaretatt under kjøring*”.

Society of Automobile Engineers (SAE) har laget en standard SAE J3016 (2016) hvor forskjellige nivå av automatisering defineres. Det er seks nivå: 0 (ingen automatisering), 1 (begrenset støtte til kjøreren), 2 (delvis automatisering), 3 (betinget automatisering), 4 (høy automatisering) og 5 (fullstendig automatisering).

Fører er ansvarlig og må ha full kontroll til og med nivå 2, slik nivåene er definert. Vi ser på SAE nivå 5 som et selvkjørende kjøretøy uten en ansvarlig fører på tradisjonell førerplass, hvor det bør være entydig at leverandøren har ansvaret. For nivå 3 og 4 er situasjonen litt mer kompleks hvor det vil være et glidende ansvarsfordeling mellom den som er kjører og håndterer situasjonen og en leverandør. Vi mener at det må defineres en ansvarlig operatør som har ansvaret under utprøving på nivå 4 og 5. I det følgende har vi foreslått en ansvarsfordeling ut

fra automatiseringsnivå. I tillegg til ansvarsfordeling generelt, legger vi også inne et spesielt ansvar knyttet til utprøving av selvkjørende kjøretøy.

Automatiseringsnivå	Ansvarsfordeling generelt	Ansvar ved utprøving
0 (ingen automatisering)	Fører	Fører
1 (begrenset støtte til kjøreren)	Fører	Fører
2 (delvis automatisering),	Fører	Fører
3 (betinget automatisering)	Fører er sentral (men flere faktorer kan spille inn)	Fører
4 (høy automatisering)	Leverandør er sentral (men flere faktorer kan spille inn)	Operatør som har fått ansvaret for å gripe inn
5 (fullstendig automatisering).	Leverandør av det autonome kjøretøyet	Operatør som har fått ansvaret for å gripe inn

I en testperiode kan det være relevant at den som tester er ansvarlig for sikkerheten, men dette må revurderes etter testperioden. Det er naturlig at leverandøren som krav-spesifiserer, bestemmer funksjonalitet, tester og godkjenner systemet i et autonomt fartøy er ansvarlig for sikkerheten, siden systemene har kontrollen slik at de velger og utfører aksjoner selv. At ansvaret ligger på leverandøren er i tråd med enkelte leverandørers syn; som fra Volvo, Google og Mercedes-Benz (Iozzio, 2016). Dette er også i tråd med leverandørens ”påse-plikt” fra andre bransjer.

I moderne tilsynsregimer er det lagt vekt på målorienterte og risikobasert myndighetsstyring med basis i internkontrollprinsippet. Hverken myndighetene eller de som anskaffer autonome kjøretøy kan forventes å sitte inne med den teknologikunnskap som leverandøren har – derfor er det naturlig at ansvaret legges på den kompetente part som har muligheten for å utvikle sikkerheten, dvs. leverandøren av autonome kjøretøy. Leverandørene ser også på systemet (”self-driving system”), som den kompetente fører. Spesifikt for autonom biltrafikk viser vi til kommunikasjon mellom Google og The National Highway Traffic Safety Administration (2016 Feb. 4):

> "*NHTSA will interpret 'driver' in the context of Google's described motor vehicle design as referring to the (self-driving system), and not to any of the vehicle occupants" "We agree with Google its (self-driving car) will not have a 'driver' in the traditional sense that vehicles have had drivers during the last more than one hundred years."*

En må plassere ansvaret korrekt dersom et uhell skulle oppstå, leverandørene sier at de tar ansvaret for ulykker forårsaket av en av deres biler i selvkjørende modus. Dette må gjenspeiles i loven, og man må definere hvordan man kan dokumentere at bilen var i selvkjørende modus. Med passasjer mener vi alle som ikke er definert som fører av fartøyet (og som ikke sitter på førerens plass). Føreransvaret bør være presisert, spesielt under utprøving, hvor det bør være en definert fører og en observatør. En passasjer som "trekker i nødbremsen" kan ikke få ansvaret som sjåfør slik det antydes i forslaget nå. Passasjerer mangler situasjonsforståelse og kan ikke lastes for uønskede hendelser.

2.3.1 Digital infrastruktur og C-ITS

I høringsnotatets avsnitt 5.2 forutsettes det i utgangspunktet at utprøving av selvkjørende kjøretøy gjøres med bruk av eksisterende infrastruktur. Den nye infrastrukturen som skal støtte opp om autonome kjøretøy bør også kunne inngå i testingen. Med den nye infrastrukturen mener vi V2V og V2I (eller C-ITS). Høringsnotatet nevner samvirkende ITS (C-ITS) men det vurderes at dette ikke er sentralt. Det åpnes imidlertid for utprøving av denne nye digital infrastrukturen. Det bør stilles krav til sikkerhet og datasikkerhet for den digitale infrastrukturen. Eksempel på anvendelse er ved uttesting av "platooning". Her vil det være aktuelt å teste ut selvkjørende biler på høy automatisering (SAE nivå 4 og SAE nivå 5, fra SAE J3016). Den digitale infrastrukturen som må anvendes kan sees på som kritisk infrastruktur når det gjelder sikkerhet. Likeledes dersom et kjøretøy fjernstyres av en operatør i et kontrollrom, så må det stilles krav til den digitale infrastrukturen mellom operatør og kjøretøy. Det bør derfor avklares hvem som har ansvaret dersom feil ved anvendelse av denne typen digitalinfrastruktur fører til ulykker.

I utgangspunktet bør leverandøren av det selvkjørende kjøretøyet ha definert både en ”safe” og ”secure” tilstand som kjøretøyet går til ved slike feil, slik at ansvaret i utgangspunktet bør ligge på leverandøren.

2.3.2 Krav i søknaden om tillatelse til utprøving relatert til SAE J3016

Standarden SAE J3016 beskriver begreper relatert til selvkjørende kjøretøy. To definisjoner er helt sentrale å adressere når det gjelder tillatelse til utprøving. Disse er:

1. Dynamic Driving Task (DDT)
2. Operational Design Domain (ODD)

DDT beskriver funksjoner relatert til hvordan kjøretøyet håndteres på strategisk, taktisk og operasjonelt vis, også omtalt som kjøreprosessen (Moe, D 1999). I praksis kan DDT håndteres f.eks. av en fører i kjøretøyet, av en operatør i et kontrollrom (fjernstyring) eller av et automatisert datasystem i kjøretøyet. Den som håndterer DDT bør også ha ansvar relatert til sikkerhet for å unngå ulykker. I søknad om tillatelse til utprøving av selvkjørende kjøretøy må det stilles krav til å beskrive DDT. Det må også kunne dokumenteres hvem som til enhver tid håndterer DDT ved lagring av informasjon fra kjøretøyets systemer.

ODD beskriver hvilke betingelser det selvkjørende kjøretøyet er laget for å operere under. Eksempler:

- Geografisk begrensninger, f.eks. innenfor et definert test-området
- Type veg, f.eks. kun motorveg med midtdeler
- Omgivelser inklusive vær og føre, f.eks. ikke på snødekket veg, ikke ved dårlig sikt
- Trafikkforhold, f.eks. ikke sammen med myke trafikanter.
- Hastighetsbegrensning, f.eks. definere en maksimal hastighet, fartssperre
- Tidsmessig begrensning

I søknad om tillatelse til utprøving av selvkjørende kjøretøy må det stilles krav til å beskrive ODD. Det må også kunne dokumenteres hvilket ODD kjøretøyet til enhver tid benyttes i ved lagring av informasjon fra sensorer og kamera i og utenfor kjøretøyet.

2.4 Systemperspektiv på uønskede hendelser og vellykket gjenvinninger

Ut fra målene som ble nevnt om å få kartlagt potensialet, utfordringer og begrensningene knyttet til infrastruktur, teknikk og regelverk, har man allerede i forslaget valgt et systemperspektiv på arbeidet. Det er en viktig forutsetning for å kunne forbedre sikkerheten, som diskutert i Cummings et al. (2014). Forskning knyttet til sikkerhet viser at den er avhengig av samspillet mellom menneskelige faktorer, teknologi og organisering (MTO). Det er ikke bare et autonomt kjøretøy i seg selv som må reguleres, det er et system. Systemet innbefatter mennesker, kjøretøy (med komponenter) og kommunikasjon på mange nivå f.eks. V2V-Vehicle to Vehicle; V2I -Vehicle to Infrastructure og mulig kommunikasjon vegtrafikksentraler. V2V og V2I er av og til inkludert i begrepet C- ITS (som står for Cooperative Intelligent Transport Systems/ Samvirkende Intelligente transportsystemer).

Dette innebærer at dokumentasjon av uønskede hendelser også må omfatte grensesnitt mot omverdenen. Det er derfor viktig å legge til rette for rapportering av uønskede hendelser (og vellykkede gjenvinninger) basert på menneskelige faktorer, teknologi i systemet rundt det autonome systemet og organisatoriske forhold, dvs.:

- Menneskelige faktorer: Sikkerhetsforskning har vist at menneskelige feilhandlinger ofte er et symptom på dårlig systemdesign; og at menneskelige feil ikke er en årsak i seg selv, se Dekker (2002). Dette er spesielt relevant ved autonom bilkjøring, hvor leverandøren må ha overveiende del av ansvaret.
- Teknologi: Teknologien består av et system, når vi ser på det autonome kjøretøyet vil det bestå av mekaniske komponenter men også av et omfattende system av programvare og grensesnitt mellom mange forskjellige systemer, som må være testet og godkjent av leverandøren som må ha en ”påse-plikt” for integrasjonsarbeidet internt og eksternt.
- Organisering/ Rutiner/ Praksis: Bruken av autonome systemer er avhengig av et systematisk og godt regelverk som sikrer at leverandøren har gode rutiner for internkontroll og kvalitetssikring, og at det er etablert overordnede funksjonelle mål. Samtidig er det viktig med systematisk erfaringsutvikling i samarbeid mellom internasjonale aktører og ved læring av hendelser via systematisk dokumentasjon av hendelser, som f.eks., via et nasjonalt CERT (Computer Emergency Response Team) for autonome kjøretøy og intelligente transportsystemer.

Et viktig område for bedre læring og forbedring av sikkerheten er å kunne lære av vellykkede gjenvinninger, og demonstrasjon av robusthet, det er derfor nyttig å inkludere det i erfaringsrapporter og hendelsesrapporteringen. Det foreslås derfor at dette nevnes i lovteksten.

2.5 Behandling av bevisste hendelser (security)

Intelligente transportsystemer og autonome kjøretøy har vært utsatt for både bevisste hendelser (security hendelser) og tilfeldige feil (safety hendelser). Begge områdene må ivaretas. I Koscher et al (2010) gjennomførte de en systematisk uttesting av systemene i en moderne bil (med flere kjørestøttesystemer), og identifiserte en lang rekke sårbarheter som gjorde at de kunne kontrollere bilen fra utsiden, dvs. kople ut bremsene, stoppe motoren,

kople ut og/eller kontrollere styringen. Det var enkelt å foreta angrep, og endre/slette data som er lagret i bilen og tilgjengelig etter en ulykke.

I andre rapporter fra konsulenter og myndigheter påpekes det at det er flere sårbarheter i systemene og i den tilknyttede infrastrukturen. I DHS (2015) gjennomgikk myndighetene i USA flere uønskede hendelser med dårlig sikkerhet i autonome biler (sårbare bremser, styresystemer etc.) og kritiske sårbarheter i infrastruktur V2V og V2I. Myndighetene foreslår at en utformer funksjonelt (adaptivt) regelverk, identifiserer beste praksis og fokuserer på systematisk opplæring. I Cerrudo (2015) systematiseres sårbarheter fra intelligente transportsystemer, hvor det påpekes store sårbarheter i systemer for trafikkstyring og i tilknyttet infrastruktur som f.eks. videokameraer. Det påpekes også et en mangler etablering av CERTèr som sørger for innsamling og analyse av angrep og manglende beredskapsplaner.

Behandling av security oppleves som umodent i forslaget, her må ansvaret plasseres på leverandøren for å få på plass gode systemer for internkontroll bl.a. testing ("penetration testing") slik at systemene som leveres er robuste mot bevisste angrep, som også er foreslått av GCIG (2016). Vårt forslag er her i tråd med føre-var-prinsippet i annen lovgivning ved innføring av ny teknologi, ref. *COMEST (2005).* Man må også ha en dokumentasjon (datagrunnlag) over hva som skjedde som er god nok for en rettsak. Det betyr blant annet at det ikke skal være mulig å manipulere denne dokumentasjonen uten at det kan spores.

2.6 Åpen transparent rapportering av hendelser

Det er usikkert hvordan autonome systemer vil påvirke sikkerheten, men studier rundt innføring av selvkjørende biler, viser at antall dødsfall vil kunne halveres (Cummings et al. 2014). Ellers er de rapportert fra leverandører som prøver ut teknologien at det har vært få ulykker. Google skal ha gjennomført over 1,1 millioner km med bilkjøring i autonom modus siden 2009 og med tre mindre uhell fram til 2015. Forskere har også analysert antall ulykker med delvis autonome luftfartøyer, og i Waraich et al. (2013) ble det dokumentert at antall uhell var 50-100 ganger høyere med delvis autonome luftfartøyer enn med luftfartøy hvor piloter styrte (Mye knyttet til dårlig design, utfordringer med grensesnittet mellom operatør på bakken og det ubemannede luftfartøyet, og utfordringer med at operatøren er ”out of the loop” og mangler situasjonsforståelse for å kunne håndtere situasjonen innen tidsrammene som er satt.) Det er også eksempler på fly som er bemannet, hvor autopiloten kunne ha berget situasjonen, men hvor piloten grep inn uten god nok situasjonsforståelse og det gikk galt – såkalt ”out of the loop” problemstillinger. Samtidig er det eksempler på luftfarts-ulykker som ble avverget på grunn av at piloten tok over fra automatikken. Dette området er sentralt tema for sikkerhetsforskere og designere av delvis autonome systemer.

Det er derfor viktig at en etablerer et system for innrapportering av uønskede hendelser, men også at en rapporterer om hendelser som dokumenterer vellykket forsøk. Systemet bør benytte standardiserte data fra hendelser. Dette er viktig for læring og oppbygging av erfaring. Det bør derfor utarbeides et formålstjenlig rapporteringsskjema som benyttes ved utprøving av selvkjørende kjøretøy.

Det er viktig at denne rapporteringen blir åpen og transparent, slik at også ”security” hendelser rapporteres. Det er viktig for forsikringsbransjen at de kan få data som gjør at de kan etablere gode modeller. Dette er forså vidt i tråd med GCIG (2016) som diskuterer styring (Governance) av ny teknologi hvor det påpekes at leverandørene har et ansvar for å utforme løsninger hvor sikring og personvern er ivaretatt, og at leverandøren må ta ansvar for egen teknologi ved en ulykke. Myndighetene må sørge for åpen og transparent rapportering av alle hendelser (både safety og security) for å sikre at forsikringsmarkedet kan fungere godt.

3 Forslag til endringer til lovteksten

Vi har i det følgende gitt innspill til den foreslåtte lovteksten, knyttet til hver individuell paragraf. Vi har vurdert viktigheten av kommentaren via prioriteringen Høy(H), Middels(M) eller Lav(L).

Paragraf	Kommentar	Viktighet av endring
§ 1 Formål:	Dekkende	-
§ 2 Virkeområdet	Dekkende	-
§ 3 Definisjoner	Dekkende	-
§ 4 Tillatelse	Dekkende – vi forstår "Juridisk person" som et rettssubjekt som ikke er en fysisk person (f.eks. foretak)	-
§ 5 Vilkår	Dekkende	-
§ 6 Ansvarlig for utprøvingen	Vi antar at ansvarlig fysisk person er som nevnt i § 4 (eller er en del av enhet benevnt som "juridisk person", dvs. en juridisk person som søker etter § 4 må utpeke en person som ansvarlig.) En bør vurdere om begrepet "juridisk person" bør benyttes i stedet for "person"/"fysisk person" da det bør være et foretak som har ansvaret for HMS (Helse, Miljø og Sikkerhet) under uttestingen. Forslag til reformulering: *Det skal i søknaden og tillatelsen utpekes en juridisk person som skal være ansvarlig for at utprøvingen gjennomføres innenfor gjeldende bestemmelser og i henhold til vilkår.*	L
§ 7 Tilbakekall og midlertidig stans	Dekkende	-
§ 8 Tiltak	8.1: Den som er ansvarlig bør forebygge og hindre – men også kunne dokumentere hendelsene som leder til evt. skaden. 8.2: Den som er ansvarlig bør i forkant ha gjennomført en risikovurdering av utprøvingen via f.eks. et "safety case". Forslag til reformulering: *Den som gjennomfører utprøving av selvkjørende*	M

	kjøretøy, skal i forkant ha gjennomført en risikovurdering av utprøvingen via f.eks. et "safety case". Likeledes skal den som gjennomfører utprøving av selvkjørende kjøretøy både forebygge og hindre – men også kunne dokumentere hendelsene som leder til evt. skaden.	
§ 9 Informasjonstilgang	Det nevnes registrering av data/informasjon fra "sensorer"; og registrering og lagring av lyd og bilder. Informasjon fra sensorer, evt. lyd og data er alle viktige datakilder som bør kunne behandles i § 9. Vi synes informasjon fra sensorer, lyd og data bør kunne lagres i samme periode (i tråd med personvernregler.) Det bør skilles mellom persondata og andre data. Data fra kjøretøyets sensorer kan også være persondata, f.eks. lokasjonsdata når kjøretøyet benyttes på ad hoc turer – hvor personer hentes på og kjøres til gitte adresser. Bruk av begrepet "data fra sensor" kan også omfatte lyd og billedopptak som jo skjer via sensorer – begrepet bør derfor presiseres f.eks. ved å si "data fra sensor" som ikke omfatter lyd og billedinformasjon. Forslag til reformulering: *Ved utprøving av selvkjørende kjøretøy skal informasjon i form av film, bilde, lyd samt "data fra sensorer" lagres i tråd med personvernregler og i minst to år.* *Den som har fått tillatelsen plikter etter begjæring å:* *a) gi forsikringshaveren til det selvkjørende kjøretøyet informasjon som er behov for i en pågående forsikringssak* *b) gi politi- og påtalemyndigheten informasjon som det er behov for i en pågående etterforskning der kjøretøyet har vært innblandet.* *Plikten gjelder ikke tilgang til informasjon som nevnt i § 15. Den som har fått tillatelsen skal gi informasjonen uten kostnad.*	M
§ 10 Rapportering	Standardisert data fra hendelser er viktig for læring og oppbygging av erfaring. Det er derfor viktig at en raskt utarbeider et formålstjenlig rapporteringsskjema som skal brukes i forbindelse med utprøving av selvkjørende kjøretøy. Dataene må i størst grad være åpne og tilgjengelige. Forslag til reformulering: *Den som har fått tillatelsen skal avgi en standardisert rapport med en redegjørelse for utprøvingen til myndigheten som har gitt tillatelsen. Den som har fått tillatelse skal når en ulykke inntreffer, snarest utrede ulykken og gi standardisert rapport til den myndigheten som har gitt tillatelse.*	H
§ 11 Ansvarlig for opplysninger	Dekkende	-
§ 12 Lyd- og bildeopptak	Dekkende	-

§ 13 Opplysningsplikt	Dekkende	-
§ 14 Viderebehandling	Bør endre navn til *§ 14 Bruk av innhentede data*. Forslag til reformulering: *Den som filmer, tar opp lyd eller avlytter, samt lagrer "data fra sensorer" får bare behandle denne typen innhentede data til forsknings- og utviklingsarbeid knyttet til utprøving av selvkjørende kjøretøy.* Det bør påpekes at forsikringsbransjen er en viktig aktør som bør få tilgang til relevante data for å kunne vurdere risikoer ved selvkjørende kjøretøy.	M
§ 15 Tilgang til materiale innhentet under utprøving	Bør endre navn til *§ 15 Tilgang til innhentede data.* Forslag til reformulering: *Tilgang til bilde- og lydmateriale samt "data fra sensorer" fra utprøving av selvkjørende kjøretøy kan bare gis til de formål dataene er innhentet for. Eksempler på dette er gjennomføring av tilsyn, forskning samt utviklingsarbeid knyttet til selvkjørende kjøretøy.* Det bør påpekes at forsikringsbransjen er en viktig aktør som bør få tilgang til relevante data for å kunne vurdere risikoer ved selvkjørende kjøretøy – ikke nødvendigvis lyd og billedinformasjon med mindre det er avtalt.	M
§ 16 Avidentifisering	Dette punktet er meget krevende og det bør vurderes om en skal ha dette som krav. Avidentifisering bør kun være et krav dersom persondata skal gjøres tilgjengelig. Dersom dataene behandles som persondata (sikker oppbevaring, tilgangskontroll og sletting av dataene etter angitt tid, etc.), så bør det ikke være krav om avidentifisering. Forslag til reformulering; *Før bildematerialet lagres, skal det avidentifiseres der det er i strid med personopplysningsloven. Dette gjelder ikke om det er innhentet samtykke til å lagre identifiserbart materiale fra den som avbildes.*	M
§ 17 Sikkerhet	Bør endre navn til *§ 17 Konfidensialitet*. Graden og behovet for konfidensialitet bør vurderes opp mot behovet for åpen deling av informasjon for å kunne vurdere risiko.	M
§ 18 Lagring av bilde- og lydmateriale	Dekkende	-
§ 19 Tilsyns-myndigheten	Det bør spesifiseres hvem som har tilsynsmyndighet som beskrevet i kapittel 2 i dette notatet.	M
§ 20 Gjennomføring av tilsyn	Bør samkjøres med begrepsbruken i § 9, slik at data fra sensorer også bør nevnes. Forslag til reformulering: *Den som har fått tillatelse til utprøving plikter å gi tilsynsmyndigheten tilgang til områder, lokaler og kjøretøy tilknyttet utprøvingen. Vedkommende plikter*	H

	også å gi tilgang til opplysninger nødvendig for å gjennomføre tilsynet, herunder lyd- og bildemateriale samt "data fra sensorer".	
§ 21 Påbud	Dekkende	-
§ 22 Ansvar	Leverandører sier at de tar ansvaret for ulykker forårsaket av en av deres biler i selvkjørende modus. Dette må gjenspeiles i loven, og man må definere hvordan man kan dokumentere at bilen var i selvkjørende modus. Forslag til reformulering: *Person som befinner seg på tradisjonell førerplass, anses som kjøretøyets ansvarlige fører med mindre det i tillatelsen er gjort unntak fra føreransvaret i medhold av § 2.* *Ved utprøving der det ikke befinner en person på tradisjonell førerplass, må man ha oppnevnt en ansvarlig operatør som har ansvaret for sikkerheten.* *Der det i tillatelsen er gjort unntak fra føreransvaret, er den som har fått tillatelsen eller er utpekt som ansvarlig, jf. § 6, også ansvarlig for at sikkerheten er ivaretatt under kjøring.*	H
§ 23 Bestemmelser om straff	Bør ses i sammenheng med § 22.	-
§ 24 Erstatning for krenkelser av den personlige integritet	Dekkende	-
§ 25 Taushetsplikt	Er det behov for dette punktet? Dekkes av personopplysningsloven.	L
§ 26 Forskriftsmyndighet	Dekkende	-
§ 27 Klage	Dekkende	-
§ 28 Ikrafttredelse	Dekkende	-

Referanser:

Brown, A. M. (2016). Blame It on the Machines: How Autonomous Vehicles Will Impact Allocation of Liability Insurance and the Resulting Impact on the Legal Community. *NCL Rev. Addendum*, *95*, 29.

Cerrudo, C. (2015). An emerging US (and world) threat: Cities wide open to cyber attacks. *Securing Smart Cities – White paper - IOActive.* www.ioactive.com/pdfs/IOActive_HackingCitiesPaper_cyber-security_CesarCerrudo.pdf

COMEST (2005) The Precautionary Principle utarbeidet av UNESCOs World Commission on the Ethics of Scientific Knowledge and Technology.

Cummings, M. L., & Ryan, J. (2014). Who is in charge? The promises and pitfalls of driverless cars. TR News, 292, 25-30.

Dekker, S. W. A. (2002). Reconstructing the human contribution to accidents: The new view of human error and performance. *Journal of Safety Research*, 33(3), 371- 385.)

DHS (2015) Department of Homeland Security, Office of Cyber and Infrastructure Analysis
The Future of Smart Cities: Cyber-Physical Infrastructure Risk

EU (2016:679) On the protection of natural persons with regard to the processing of personal data and on the free movement of such data; Regulation of the European Parliament and of the Council of 27 April 2016

GCIG (2016) Global Commission on Internet Governance, "One Internet" www.ourinternet.org

Iozzio, C. (2016). Who's Responsible When a Car Controls the Wheel?. *Scientific American*, *314*(5), 12-13.

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S.,& Savage, S. (2010, May). Experimental security analysis of a modern automobile. In *2010 IEEE Symposium on Security and Privacy* (pp. 447-462). IEEE.

Kystverket (2016) www.kystverket.no/Nyheter/2016/september/apner-for-test-av-autonome-skip/

Luftfartstilsynet (2016) "Forskrift om luftfartøy som ikke har fører om bord mv." med ikrafttredelse 01.01.2016. https://lovdata.no/dokument/SF/forskrift/2015-11-30-1404

Luftfartstilsynet (2017) http://luftfartstilsynet.no/selvbetjening/allmennfly/Droner/

NFAS (2016) ref: nfas.autonomous-ship.org/projects.html

Moe, D 1999: Dybdeanalyse av møte- og utforkjøringsulykker på rette strekninger i 80 – og 90 soner med død eller alvorlig skade. SINTEF Rapport STF A99559

SAE J3016 On-Road Automated Vehicle Standards Committee. (September 2016). Taxonomy and definitions for terms related to on-road motor vehicle automated driving systems. Society of Automotive Engineers.

National Highway Traffic Safety Administration (2016 Feb. 4) retreived from https://isearch.nhtsa.gov/files/Google%20--%20compiled%20response%20to%2012%20Nov%20%2015%20interp%20request%20--%204%20Feb%2016%20final.htm

SOU 2016:28 "Vägen till självkörande fördon" ref www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2016/03/sou-201628/

Waraich, Q. R., Mazzuchi, T. A., Sarkani, S., & Rico, D. F. (2013). Minimizing human factors mishaps in unmanned aircraft systems. *ergonomics in design*, *21*(1), 25-32.

VEDLEGG

Rammer gitt i lovteksten

Formålet med loven er å legge til rette for utprøving av selvkjørende kjøretøy på veg, innenfor rammer som særlig ivaretar trafikksikkerhets- og personvernhensyn. Utprøvingen skal skje gradvis, særlig ut fra teknologiens modenhet og med formål om å avdekke hvilke effekter selvkjørende kjøretøy kan ha for trafikksikkerhet, effektivitet i trafikkavviklingen, mobilitet og miljø.
Norge har sluttet seg til Amsterdamerklæringen "*Cooperation in the field of connected and automated driving*" (2016), hvor det bl.a. presiseres at en bør identifisere, og om mulig fjerne, rettslige hindringer for utprøving av autonome kjøretøy. Det er alminnelig enighet om at vegtrafikkonvensjonene ikke er til hinder for utprøving av selvkjørende kjøretøy, så lenge fører kan ta over kontrollen av kjøretøyet men situasjonen er ikke like klar for utprøving av selvkjørende kjøretøy der det ikke er en fører som kan ta over kontrollen.

Definisjoner og begreper

Begrepene "kjøretøy" og "veg" skal forstås på samme måte som i vegtrafikkloven.
Mht. automatiseringsnivåer brukes inndeling fra SAE (Society of Automotive Engineers), hvor SAE J3016 kategoriserer kjøretøyene i nivåer fra 0 til 5, hvor 0 er ingen og 5 er full automatisering. "*Selvkjørende kjøretøy*" benyttes om motorvogn der en fører kan overlate kjøringen til et teknisk system som automatisk fører motorvognen, og motorvogn som er konstruert for å kjøre uten en fører.

Typegodkjenningsdirektivet 2007/46 er ikke tilpasset selvkjørende kjøretøy, men er under arbeid i EU. Det finnes muligheter for medlemsstatene til å gi unntak fra dette rammedirektivet.