Rapport

Risker med uppkopplade och automatiserade fordon

Ansvar ur ett juridiskt perspektiv i Sverige idag

september 2020

INTERACTIVE LAW

Interactive Law

är ett konsultföretag specialiserat på att undersöka och analysera verksamheter och företeelser från en övergripande utgångspunkt för att identifiera framförallt juridiska nyckelfrågor. Syftet är att ge kunskapsunderlag och förbättra förutsättningarna för experter inom olika discipliner att tillsammans lösa utmaningar i komplexa sammanhang.

Vi har en bakgrund som bolagsjurister inom IT- och telekom och som rådgivare/advokat. I uppdragen drar vi fördel av erfarenheter från riskanalyser, revisioner inom dataskydd, due diligence-arbete i samband med företagsförvärv, rådgivande arbete inom produkt- och tjänsteutveckling, stöd till start-up verksamheter inom innovation och digitalisering. Ett av Interactive Laws specialistområden är dataskyddsförordningen (GDPR) och övrig dataskyddsreglering. Vi arbetar med IT- och informationssäkerhet ur ett juridiskt perspektiv.

www.interactivelaw.se
Christina Arrhult Björk, tel. 070 727 28 45
Helena Borglund, tel. 070 941 22 04

Förord

Denna rapport innehåller beskrivningar av ansvarsförhållanden ur ett juridiskt perspektiv för ett antal teknikrelaterade risker med uppkopplade och automatiserade vägfordon. Riskerna har identifierats av Trafikanalys som har försett oss med en lista med tolv frågor om hypotetiska händelser/incidenter som skulle kunna inträffa med uppkopplade och automatiserade fordon.

Tyngdpunkten i analyserna ligger på informationssäkerhet ur ett juridiskt perspektiv. Här framgår också på övergripande nivå i vilken utsträckning som riskerna regleras i dagens lagstiftning. Rapporten är framtagen för att skapa ett underlag för diskussion om hur en successiv uppkoppling och på längre sikt en automatisering kan ställa krav på en anpassning av regelverk.

Rapporten innehåller resultatet av ett arbete som har bestått av skrivbordsgenomgång av en stor mängd information, däribland studier, rapporter, författningstexter, förarbeten och annat material relaterat till regelgivning.

Rapporten är beställd av Trafikanalys och arbetet har utförts av konsultföretaget Interactive Law.

Stockholm i september 2020

Interactive Law

Christina Arrhult Björk & Helena Borglund

Senior legal advisors

Innehåll

Sammanfattning

Fordon med förarstödjande teknik ökar i antal och den förarstödjande tekniken blir mer och mer avancerad. Utvecklingen av automatiserade fordon går snabbt och infrastrukturen som finns i anslutning till fordonen digitaliseras. Den ökade digitaliseringen sätter fokus på informationssäkerhet.

För att ett tillfredsställande informationssäkerhetsarbete ska kunna bedrivas, behöver ansvaret för olika risker relaterade till automatiserade fordon identifieras. Varje aktör måste göra sin del av informationssäkerhetsarbetet. Det gäller både aktörer i privat och offentlig sektor. För adekvat regelgivning måste ansvaret myndigheter emellan vara tydligt.

I denna rapport finns beskrivningar av ansvarsförhållanden ur ett juridiskt perspektiv för ett antal teknikrelaterade risker med uppkopplade och automatiserade vägfordon som Trafikanalys har bett oss ta ställning till. Tyngdpunkten i analyserna ligger på informationssäkerhet ur ett juridiskt perspektiv. Här framgår också på övergripande nivå i vilken utsträckning som riskerna regleras i dagens lagstiftning.

Vi vill på ett allmänt plan lyfta fram följande förhållanden.

Det är endast i ett fåtal situationer möjligt att direkt av lagtexten utläsa vilken aktör som ansvarar för ett visst slags informationssäkerhetsarbete eller för informationssäkerhetsarbete rörande en viss produkt, tjänst eller process. Eftersom de händelser/incidenter och frågor som vi har undersökt inte ger någon närmare information om de orsakssamband som har lett fram till händelserna, är det många gånger inte heller möjligt att ge ett entydigt svar på frågan om juridiskt ansvar för den olycka som händelsen lett till.

Inte minst sedan den nya dataskyddsförordningen (GDPR) började tillämpas i maj 2018, finns ett ökat behov av att andra yrkesgrupper än jurister får möjlighet att ta till sig lagtext och rättsregler. Vi anser därför att jurister måste bli bättre på att kommunicera juridik och vi försöker i denna rapport bidra till detta. Inte minst när det kommer till frågor om ansvar är det viktigt att ha några juridiska utgångspunkter klara för sig. Det som särskilt kan betonas är vikten av att utgå från rättsordningens systematik och betydelsen av en strukturerad och korrekt analys av rättsregler.

Ökat fokus på informationssäkerhet gör kommunikationen mellan experter inom just informationssäkerhet och juridik prioriterad. Vi har i tabellform på ett schematiskt sätt försökt åskådliggöra skillnaden mellan den problemlösning och arbetsmetodik som, enligt vår uppfattning, experter inom informationssäkerhet respektive juridik tillämpar. Det finns sannolikt mer att tillägga och vi vill understryka att vår beskrivning inte gör anspråk på att vara vetenskapligt belagd. Under avsnittet ”Ansvar” redogör vi för vad som inom juridiken menas med ansvar och på ett övergripande plan vilka olika typer av ansvar som jurister brukar laborera med. Vi betonar att det är de faktiska orsakerna till det händelseförlopp som leder till en skada som avgör vem som tillskrivs ansvaret. Det betyder att det för att peka ut en straffrättsligt och civilrättsligt ansvarig, måste göras en grundlig analys som inkluderar de bakomliggande omständigheterna och kontexten i övrigt.

Vi vill också uppmärksamma den skillnad som i juridiskt hänseende finns mellan rättsregler och standarder, där rättsregler härstammar från en normgivare som är en nation eller en sammanslutning av flera nationer som Europeiska unionen (EU), Förenta nationerna (FN) och andra organisationer, det vill säga det som inom svensk rätt närmast kallas offentligrättsliga organ. Standarder däremot, sätts som utgångspunkt av privaträttsliga organ vilka i det fallet fungerar som normgivare. I dagens samhälle, suddas skiljelinjen mellan rättsregler och standarder i flera sammanhang ut. Även nationer och sammanslutningar av nationer står ibland bakom utarbetandet av koder och standarder och lagar ger uttryckliga mandat till privaträttsliga organ, sammanslutningar och intresseorganisationer att sätta standarder. För att en standard ska få juridisk betydelse måste den emellertid alltid ha fått juridisk legitimitet genom någon form av initiativ, hänvisning eller godkännande från en offentligrättslig aktör. Standarden kan till exempel av en domstol tillerkännas betydelse som branschpraxis. Det som nu har sagts om kravet för att en standard ska få juridisk betydelse hindrar givetvis inte att en standard, trots att den saknar juridisk tyngd, kan få betydelse på andra sätt.

För arbetet med denna rapport har utredningen Vägen till självkörande fordon – introduktion, Del 1 - 2, Slutbetänkande av utredningen om självkörande fordon på väg, SOU 2018:16 (”Utredningen SOU 2016:18”) och flera av remissyttrandena till densamma tjänat som viktiga källor.

När det gäller frågan om ansvar, inklusive ansvar för informationssäkerheten, kan våra slutsatser i korthet summeras enligt nedan.

Vi har resonerat kring vilket ansvar en förare har för en olycka som inträffar på grund av att föraren inte har förstått information eller inte fått information. En förare omfattas av ett allmänt aktsamhetskrav och föraren kan sannolikt inte undgå ansvar för en olycka genom att hävda att denne inte har förstått viss information. En underlåtelse att följa aktsamhetskravet, med en olycka som följd, får förmodas utgöra vårdslöshet i trafik. Ett ansvar för vårdslöshet i trafik kan sannolikt även göras gällande med hänvisning till det som kallas förarens garantställning.

Om föraren inte får information om systematiska fel, konstruktionsfel eller instruktionsfel och en olycka inträffar, ansvarar tillverkaren eller importören för dessa fel i enlighet med reglerna om produktansvar. Produktansvaret gäller bara konsumenter som drabbats av person- och sakskador. Näringsidkare behöver istället se till att reglera ansvaret i avtal med tillverkaren eller importören.

Vi har utgått från den nivåindelning avseende automatiseringsgrad som upprättats av amerikanska *Society of Automotive Engineers* (SAE) som Utredningen SOU 2018:16 använt sig av. Nivåerna är deskriptiva och tekniska. Här skulle det enligt vår uppfattning underlätta för tydliggörandet av ansvaret om även det juridiska perspektivet togs med i modellen. Detsamma har efterfrågats i Åklagarmyndighetens remissyttrande.

Skador till följd av olyckor som inträffar av olika mjukvarurelaterade orsaker som ursprungliga säkerhetsfel, brister i uppdatering och åtkomst till mjukvara omfattas av tillverkarens produktansvar (produktansvarslagen 1992:18). En tillverkare ska även inför försäljning säkerställa att fordonet uppfyller kraven på typgodkännande (fordonsförordningen 2009:211).

När det gäller hur en mjukvara eller annan teknologi, till exempel artificiell intelligens (AI), bör prioritera i svåra situationer brukar ett etiskt dilemma som kallas *the trolley problem* ibland tas upp som exempel. Det finns inga bestämmelser i Sverige som reglerar denna typ av situationer men det har tagits fram etiska riktlinjer för tillförlitlig AI inom EU.

Det pågår sedan flera decennier ett arbete med att utveckla och införa infrastruktur för kommunikation på vägtrafikområdet under samlingsnamnet *intelligent transportation systems,*

ITS. EU har antagit regler som syftar till åtgärder för att åstadkomma en hög gemensam nivå på säkerhet i nätverks- och informationssystem i unionen och som har implementerats i Sverige (lagen 2018:1174 om informationssäkerhet för samhällsviktiga och digitala tjänster är av betydelse på infrastrukturområdet, ”NIS-lagen”). Myndigheten för samhällsskydd och beredskaps (MSB) har en samordnande roll och tar fram övergripande regler för alla sektorer som omfattas av NIS-lagen. Regelverken kräver bland annat att det bedrivs ett systematiskt informationssäkerhetsarbete avseende samhällsviktiga tjänster rörande vägtransport där incidenter skulle medföra en betydande störning vid tillhandahållande av tjänsten. I MSB:s föreskrifter (2018:7) regleras endast larmcentraler för så kallad eCall och rikstäckande databaser med uppgifter om hastighetsgräns, vägbredd, bärighet, samt rekommenderad väg för farligt gods. Utvecklingen går mot en ökad insamling av information när det gäller automatiserade fordon och det kan därmed i framtiden uppkomma behov av mer utförlig reglering i Sverige.

I fordon med förarstödjande teknik och i de försöksverksamheter som pågår med självkörande fordon sker insamling av information. En del av den insamlade informationen utgör personuppgifter och GDPR:s bestämmelser behöver beaktas. I sitt remissyttrande till Utredningen SOU 2018:16 har Datainspektionen (DI) efterlyst en utförlig kartläggning och dataflödesanalys som inbegriper det uppkopplade och automatiserade fordonet och dess interaktion med omgivningen inklusive en komplett riskanalys och konsekvensbedömning. DI kommenterar även att utrymmet för nationella bestämmelser behöver övervägas utifrån internationell rätt och att en analys och anpassning utifrån GDPR och reglerna om kamerabevakning måste göras. Vi delar DI:s uppfattning och ser att dataflödesanalysen bör omfatta kartläggning och analys steg-för-steg av vilken information som samlas in, av vem och för vilka syften. Det är, som DI också påpekar, inte bara uppgifterna i sig, utan även metoderna för insamling, lagring och eventuell samkörning av information som behöver genomlysas.

Förkortningar

ACEA	the European Automobile Manufacturers´ Association
Artikel 29-gruppen	Article 29 data working party, förkortat: Art. 29 WP, ett avvecklat rådgivande EU-organ som skulle se till att de EU:s rättsakter som låg till grund bland annat för den svenska Personuppgiftslagen (1998:204) tillämpades likformigt i hela EU. Artikel 29-gruppen har ersatts av EDPB, Europeiska dataskyddsstyrelsen, i och med att GDPR började tillämpas 25 maj 2018
C-ITS	co-operative intelligent transportation systems
DI	Datainspektionen
ENISA	European union agency for network and information security, Europeiska unionens cybersäkerhetsbyrå
EDPB	European data protection board: Europeiska dataskyddsstyrelsen, ett oberoende europeiskt organ som bidrar till en enhetlig tillämpning av dataskyddsregler i hela Europeiska unionen och främjar samarbete mellan EU:s dataskyddsmyndigheter
GDPR	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)
ITS-direktivet	Europaparlamentets och rådets direktiv 2010/40/EU av den 7 juli 2010 om ett ramverk för införande av intelligenta transportsystem på vägtransportområdet och för gränssnitt mot andra transportslag
KOMET	Kommittén för teknologisk innovation och etik
Medlemsstater	EU:s medlemsstater
MSB	Myndigheten för samhällsskydd och beredskap

NIS-direktivet	Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen
NIS-lagen	lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
NHTSA	den amerikanska säkerhetsorganisationen National Highway Traffic Safety Administration
Rapporten	denna rapport om risker med uppkopplade automatiserade fordon
SAE	den amerikanska sammanslutningen Society of Automotive Engineers
SIS	svenska institutet för standarder
SOU	statens offentliga utredningar
UNECE	Förenta nationernas ekonomiska kommission för Europa
Utredningen SOU 2018:16	utredningen Vägen till självkörande fordon - introduktion, Del 1 - 2, Slutbetänkande av utredningen om självkörande fordon på väg (SOU 2018:16)
WP.29	en arbetsgrupp inom FN-organet UNECE

1 Inledning

1.1 Uppdrag och syfte

Trafikanalys har anlitat Interactive Law (”oss”, ”vi”) för att analysera i vilken utsträckning ansvar för ett antal risker relaterade till uppkopplade och automatiserade fordon, täcks av dagens lagstiftning. Tyngdpunkten i analysen bör enligt uppdragsbeskrivningen ligga på informationssäkerhet ur ett juridiskt perspektiv.

Riskerna har identifierats av Trafikanalys som har försett oss med en lista med tolv frågor om hypotetiska händelser/incidenter som skulle kunna inträffa med uppkopplade och automatiserade fordon. Vi har föreslagit en gruppering av händelserna i fyra teman: föraren, fordonet, infrastrukturen samt säkerhet och personuppgifter. Trafikanalys har godkänt detta.

Trafikanalys syfte med uppdraget är att det ska skapa ett underlag för diskussion om hur en successiv uppkoppling och, på längre sikt, en automatisering kan ställa krav på en anpassning och komplettering av gällande regelverk och myndighetsföreskrifter.

Vår analys har resulterat i denna rapport (”Rapporten”). Rapporten innehåller, förutom en inledande sammanfattning, detta avsnitt 1. Inledning, avsnitt 2. Informationssäkerhet – juridik, avsnitt 3. Ansvar och avsnitt 4. Svar till Trafikanalys.

Redovisningen av vår analys av de hypotetiska händelserna återfinns i avsnitt 4 där varje delavsnitt inleds med en text som litet grand sätter scenen varefter svaren på frågorna redovisas i tabellform.

Rapportens avsnitt 2 och 3 ger läsaren ytterligare underlag.

I denna rapport har vi använt ordet informationssäkerhet synonymt med cybersäkerhet eftersom vi inte bedömer att eventuell skillnad har någon betydelse för de frågor som avhandlas här.

1.2 Avgränsningar

Vi har utgått från och försökt besvara de frågor vi har fått av Trafikanalys. Frågorna innehåller en generell beskrivning av en händelse/incident. De ger inte någon närmare information om de orsakssamband som lett fram till händelsen. Våra svar är därför på en generell och resonerande nivå med ett försök att förmedla hur en jurist i det förevarande fallet skulle kunna angripa och besvara frågan om ansvar. Vi anger också lagstiftning som är relevant för bedömningen av händelsen och försöker peka på vilka förhållanden som är oreglerade i lag. Det har inte ingått i vårt uppdrag att komma med nyheter eller förslag utan vi har primärt fokuserat på att utifrån förutsättningarna presenterat en övergripande nulägesanalys.

Vår analys har varit av juridisk, praktisk natur. Vi har inte utfört granskningen ur tekniskt, kommersiellt eller finansiellt perspektiv och vi reserverar oss för att vi kan ha missuppfattat

något som relaterar till dessa områden. Rapporten är utarbetad utifrån och ska tolkas mot bakgrund av svensk rätt. Vår rådgivning omfattar inga andra jurisdiktioner än Sverige.

1.3 Metod

Arbetet har bestått av skrivbordsgenomgång av en stor mängd information, däribland studier av artiklar, rapporter, författningstexter, förarbeten och annat material relaterat till regelgivning, se källförteckning sist i Rapporten. Uppdraget inleddes med att vi den 18 mars 2020 närvarande vid seminariet *IT-säkerhet inom Transportsektorn* arrangerat av MSB. Uppdraget har därefter utförts under april - juni 2020 och ett par fotnoter har uppdaterats under september 2020. Under uppdraget har vi haft löpande avstämningar med företrädare för Trafikanalys.

2 Informationssäkerhet – juridik

Medan informationssäkerhet kan definieras som bevarande av konfidentialitet, riktighet och tillgänglighet hos information,[1] är juridiken läran om rättsreglernas tolkning och tillämpning.

Det bör också noteras att informationssäkerhet syftar till att skydda själva informationen, utifrån informationsklassning. Inom dataskydd är syftet att skydda den enskilde individen, i GDPR kallad den registrerade.

Jurister behöver i allt högre utsträckning arbeta med experter inom informationssäkerhet och vice versa. Vi tror därför att en beskrivning av vad som – enligt vår uppfattning – skiljer synsätten och arbetsmetodiken åt, kan bidra till att öka förståelsen mellan experter inom dessa respektive sakområden. Beskrivningen i tabellen nedan är vår egen och gör inte anspråk på att vara komplett. Vår expertis ligger främst inom juridik och illustrationen bör ses i det ljuset.

Informationssäkerhet	**Juridik**
Kommer från datasäkerhet och kryptering och är sprunget ur behovet att hålla information hemlig vid bland annat krigföring. Har fokus på krav (som i en kravspecifikation) vilka ska uppfyllas och levereras mot	Juridiken och mer beständiga rättsordningar uppkom när människan blev bofast. Det grundläggande synsättet är att allt i samhället sker ”under lagarna” och fokus ligger på rättsregler som det måste säkerställas efterlevnad till
Analyserar, tolkar och gör avvägningar genom att klassa information efter dess känslighetsgrad, t.ex. i) kvalificerat hemlig, 2) hemlig, 3) konfidentiell och 4) begränsat hemlig (Säkerhetsskyddslagen (2018:585) 2 kap. 5 §)	Identifierar och ”trattar ned” vilket som är den juridiska knäckfrågan i den specifika situation som juristen har framför sig
Fokuserar på flöden och processer, dvs. hur ett arbete steg för steg utförs inom verksamhetens olika funktioner samt på livscykelhantering	Frågar sig ”var i den rättsliga materian befinner vi oss?” Inom vilket rättsområden finns svaret på den juridiska knäckfrågan?
Analyserar genom verksamhetsanalys, omvärldsanalys (här ingår att identifiera rättsliga krav), riskanalys (identifierar hot, sårbarheter och risker) och gapanalys	Analyserar utifrån rättsordningens systematik. Identifierar grovt ett spann av lag- och andra rättsregler – svensk rätt, EU-regler, rättspraxis osv, som är relevanta för frågan. Granskar rättsreglerna, hur de förhåller sig till varandra hierarkiskt? Är lagen tvingande eller dispositiv? Har rättsregeln legitimitet (framtagen av relevant och behörigt normgivningsorgan)? Riskanalys ingår, även om det sällan benämns så
Identifierar informationstillgångar, dvs. information och resurser som används för att hantera information, t.ex. IT-system, IT-infrastruktur och fysiska tillgångar	Sållar och identifierar den rättsregel som ska användas för att besvara knäckfrågan
Arbetar med målsättningen att efter analysen vidta säkerhetsåtgärder, dvs. organisatoriska åtgärder – ett ledningssystem med en hierarki av policyer, riktlinjer och rutiner – samt tekniska säkerhetsåtgärder av olika slag, brandväggar, kryptering, loggning, behörighetsstyrning implementeras, med fokus bland annat på beredskaps- och kontinuitetsplanering	Tolkar formuleringar, som *skälig, lämplig, nödvändig, laglig, med hänsyn till omständigheterna* som rättsregeln innehåller utifrån rättsregelns syfte, det rättsområde som knäckfrågan rör, omständigheterna i det särskilda fallet, allmänna rättsprinciper som gäller för frågor av det slag det nu är fråga om samt baserat på den erfarenhet och kunnande som juristen har skaffat sig genom att utöva yrket
Övervakar och analyserar löpande. Säkerhetsåtgärderna ses över och ständiga förbättringar eftersträvas. Utvärderar, sätter nya mål. Drar slutsatser av incidenter osv.	Svaret blir ofta av det resonerande slaget ”förutsatt att, på grund av a, b, c gör vi bedömningen att det i detta fall bör vara x som är ansvarig”. Behöver analysera igen vid ändrad lagstiftning eller ändrade omständigheter

Figur 1: Figuren beskriver schematiskt några förhållande som vi har identifierat när det gäller den arbets- och problemlösningsmetodik som en expert inom informationssäkerhet respektive juridik använder sig av.

[1] MSBF (2020:06) föreskrifter om informationssäkerhet för statliga myndigheter, 3 §.

2.1 Informationssäkerhet – rättsliga krav

I MSB:s *Metodstöd för systematiskt informationssäkerhetsarbete – En översikt* (”MSB:s metodstöd”) finns vägledning för hur ett systematiskt informationssäkerhetsarbete kan bedrivas. Metodstödet uppges syfta till att hjälpa organisationer att komma igång med och förbättra informationssäkerhetsarbetet.[2] Eftersom ett systematiskt informationssäkerhets-arbete måste anpassas efter en organisations specifika omständigheter, behöver det arbetet, enligt MSB:s metodstöd, börja med att dessa omständigheter identifieras och analyseras. För ändamålet bör göras en verksamhets-, omvärlds-, risk- och gapanalys. Inom ramen för omvärldsanalysen ska de rättsliga kraven identifieras och i det sammanhanget behöver även externa intressenters – kunder, leverantörer, medborgare och granskare – behov, förväntningar och förutsättningar (som tekniska, sociala, miljömässiga, politiska) klarläggas.[3]

Med analys av rättsliga krav, förklarar MSB, avses krav i olika författningar, kopplade till den specifika organisationens “informationshantering eller direkt till informationssäkerhet, till exempel dataskyddsförordningen, säkerhetsskyddslagen, bokföringslagen, MSB:s och andra myndigheters föreskrifter och NIS-regleringen. Kraven kan handla om informationssäkerhet i sin helhet eller om vilket skydd vissa specifika informationsmängder behöver”. Ta hjälp av juridisk expertis, uppmanar MSB.[4]

MSB:s metodstöd bygger på de internationella standarderna i ISO/IEC 27000-serien. Den svenska standarden SS-EN ISO/IEC 27001 uppmanar den organisation som vill utarbeta ett ledningssystem för informationssäkerhet enligt standarden att bestämma vilka intressenter som är relevanta och dessa intressenters krav som är relevanta för informationssäkerhet med anmärkningen att berörda parters krav kan inkludera rättsliga och regelmässiga krav samt avtalsförpliktelser.[5]

Enligt vår uppfattning behöver här understrykas att lagen inte uteslutande består av krav utan även anger skyldigheter/åligganden. Påfallande ofta är lagregler också utformade inte som krav utan som övergripande målsättningar och principer. Detta gäller i synnerhet EU-rättsliga normer och det betyder att det inte räcker att gå till lagen och läsa för att få fram *de rättsliga kraven* utan det behöver bland annat göras en analys och en avvägning. Det är den analysen som juridisk expertis är utbildad att göra och det är med stor sannolikhet därför som MSB uppmanar till samarbete mellan informationssäkerhets- och juridisk expertis.

Juristen analyserar, tolkar utifrån rättsordningens systematik – rättskälleläran och normhierarkin – och försöker dra rimligt korrekta slutsatser. Dessa slutsatser bör sedan kunna användas som de *rättsliga krav* som efterfrågas inom informationssäkerhetsarbetet. En närmare redogörelse för rättskällor och normer finns under avsnitt 2.2 nedan.

[2] MSB (2019) *Metodstöd för systematiskt informationssäkerhetsarbete - En översikt*, s. 4
[3] MSB:s metodstöd s. 8-12.
[4] MSB:s metodstöd, sid. 10
[5] SIS, Swedish Standards Institute (2017) SS-EC ISO/IEC 27001:2017 (Sv), Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav, Stockholm, Sweden punkt 4.2.

2.2 Rättskällelära och normhierarki[6]

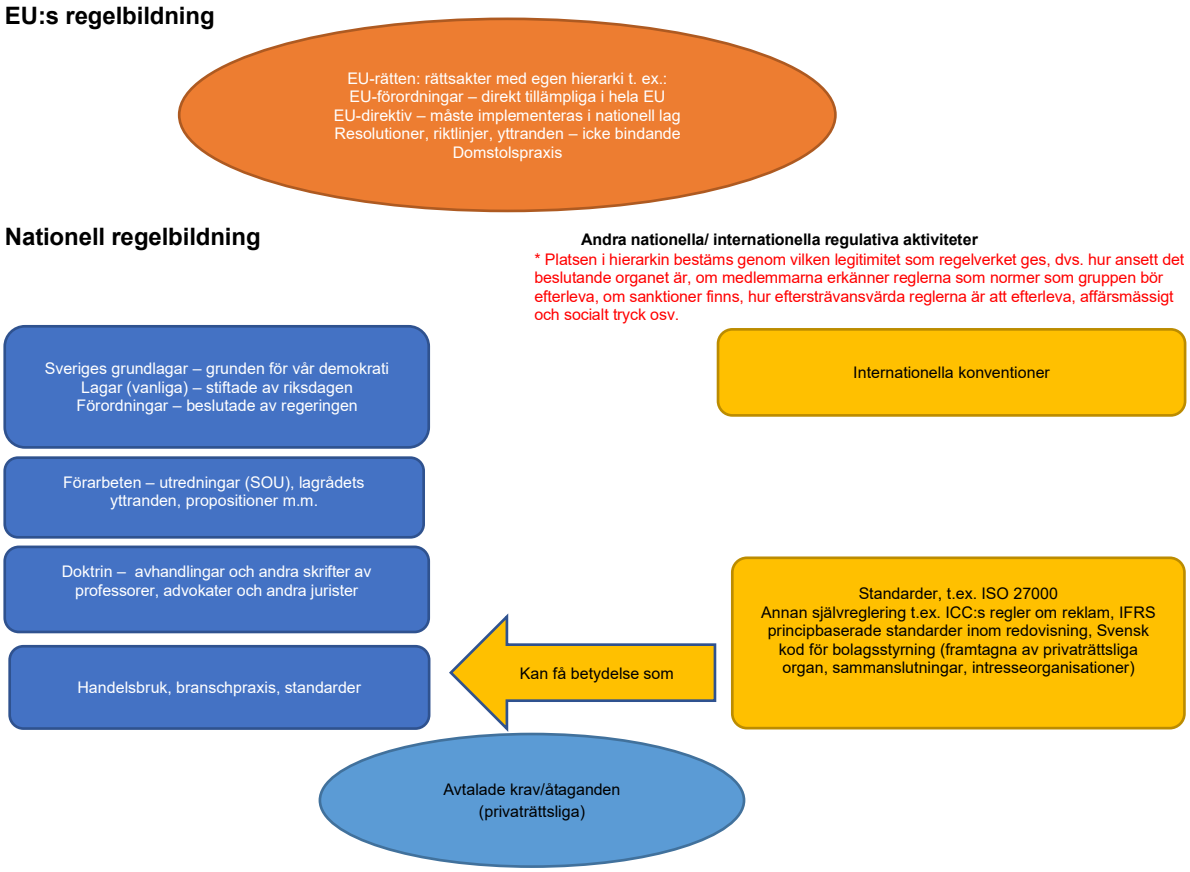
Det är viktigt att skilja mellan å ena sidan normer som beslutats från politiskt och offentligt håll av en lagstiftare, det vill säga av en nation eller av flera nationer tillsammans inom till exempel EU, och vars räckvidd avgörs av omfånget på nationens eller unionens jurisdiktion, alltså det område som lagstiftaren kan bestämma över, och å andra sidan normer och standarder framtagna av privaträttsliga organ, sammanslutningar och intresseorganisationer. En viktig aspekt på en lagstiftares normgivning är lagstiftarens särskilda möjlighet att genomdriva normerna, genom att utöva tillsyn och utkräva (straff-)ansvar i nationens eller nationernas namn.

Den som ska identifiera rättsliga krav och juridiskt ansvar, behöver vara medveten om att alla normer och standarder som har beslutats av privaträttsliga organ har lagregler ”ovanför sig” i normhierarkin. Lagreglerna återfinns alltså högre upp i normhierarkin. De sätt på vilka en standard kan få juridisk relevans är om en lag hänvisar till standarden eller om standarden vid tolkning bedöms utgöra praxis i branschen. Om en standard som har beslutats på privat väg strider mot en rättsregel, kan den underkännas av domstol.

Även nationella myndigheter är inbegripna i förhandlingar och diskussioner med internationella organisationer, andra staters myndigheter, standardiseringsorgan, intresseorganisationer, privata företag med flera.[7] Vilken juridisk tyngd som de normer arbetet resulterar i får, beror på vilken juridisk legitimitet/tyngd som det beslutande organet har.

För juristens arbete är rättskälleläran av betydelse. Rättskälleläran är läran om de källor som ska användas för att uttolka gällande rätt. Rättskällorna är ordnade i en hierarki där en rättskälla med högre rang har tolkningsföreträde framför (gäller före) en med längre rang.

[6] För information om juristens källmaterial och arbetsmetoder, se till exempel Bernitz, U. m fl (2017) *Finna rätt*. Wolters Kluwer Sverige AB, Stockholm.
[7] Wennström, B. *Rättens nya landskap*. Working Paper 2010:4, Juridiska fakulteten, Uppsala universitet.



Figur 2: Figuren beskriver schematiskt rättskällor (blå), andra regulativa aktiviteter (gula), avtal (grön) placerade uppifrån och ned i två spalter enligt gällande normhierarki i Sverige. Redovisningen är inte fullständig. För en beskrivning av myndigheters regelgivning, se till exempel DS 1998:43, Myndigheternas föreskrifter Handbok i författningsskrivning, som även innehåller en ordlista med förklaringar.

Lagar och förordningar har högst rang. EU-rätten (även kallad unionsrätten) har företräde framför svensk lag men EU har endast lagstiftningsmakt inom vissa områden. På andra plats finns förarbeten, det vill säga utredningar (statens offentliga utredningar, SOU) som genomförs innan en ny lag beslutas. Här innefattas remissyttranden från intressenter och lagrådets yttrande. I utredningens rapport (kallad betänkande) framgår kontexten och de avvägningar som gjorts innan lagförslaget läggs fram.

På tredje plats finns rättspraxis, det vill säga domstolarnas tolkning och avgöranden, domar och beslut, i olika mål, tvister och rättsliga ärenden. Det är bara avgöranden från högsta instans (Högsta domstolen, Högsta förvaltningsdomstolen och specialdomstolarnas överinsatser) som har prejudicerande verkan, även om lägre instans avgörande ibland åberopas när annat saknas.

På fjärde plats kommer doktrinen som utgörs av avhandlingar och andra skrifter författade av professorer och experter som advokater och andra jurister som tillämpar rätten i praktiken. Sist bland rättskällorna, framförallt på civilrättens område (för distinktion mellan rättsområden se avsnitt 2.3 nedan) kommer sedvänja, handelsbruk och branschpraxis. I den juridiska hierarkin blir det här som standarder och koder får betydelse.

Ett gemensamt namn för de regler som rättskällorna innehåller är *rättsregler* eller *normer*. Om man vill ange ett specifikt avsnitt i den skrivna rätten som ska tillämpas för en viss

frågeställning används ofta begreppet *lagrum*. I de flesta fall syftar lagrum på en enstaka paragraf.

Beskrivningen i detta avsnitt 2.2 avser Sverige. EU-rätten har sin egen struktur och rättskällor. Viktigaste distinktionen är den mellan en EU-förordning (inte att förväxla med en nationell förordning som beslutas av regeringen) som har direkt effekt och direkt gäller som svensk lag och ett EU-direktiv som måste implementeras i nationell lag. Varje nation har sina rättskällor och rättstraditioner eftersom rätten har utvecklats under mycket lång tid. Hur mycket ett lands lag skiljer sig från ett annat, beror till exempel på geografisk närhet, vilka influenser som funnits på administration och handel historiskt och i nutid. Lagarna i ett demokratiskt samhällsskick skiljer sig så klart från dem i ett mer auktoritärt system.

2.3 Rättsområden och tolkning

Juridiken är indelad i olika rättsområden och på övergripande nivå skiljer man mellan offentlig rätt och civilrätt där offentlig rätt reglerar förhållandet mellan den enskilde och det allmänna (offentliga organ, staten, kommuner och så vidare), medan förhållandet mellan privata rättssubjekt regleras inom civilrätten. I offentlig rätt ingår statsrätt, förvaltningsrätt och straffrätt. Inom civilrätten finns till exempel avtalsrätt där konsumenträtten ingår, immaterialrätt, associationsrätt, arbetsrätt och familjerätt. Skiljelinjen mellan offentlig rätt och civilrätt och mellan olika rättsområden är inte knivskarp och det finns rättsregler som kan sägas tillhöra både offentlig rätt och civilrätt.

Till juridiken hör också lagtolkning och kunskap om tolkningsmetoder och -regler, som restriktiv/extensiv tolkning, tolkning genom analogier och motsatsslut, samt när olika metoder ska användas. I lagen anges ibland kriterier för tolkning. En praktiserande och specialiserad jurist är van att tolka rättsregler inom just sitt specialistområde. Det är också viktigt att se på syftet med en viss lag liksom att förstå för vem en viss rättsregel gäller (jämför skillnad offentlig rätt och civilrätt).

2.4 Standard, lag och informationssäkerhet – några reflektioner

Koder och standarder har stor betydelse, inte minst inom affärslivet. Standardiseringsorgan bedriver ett kvalificerat arbete där experter från industri, näringsliv och samhälle gör betydelsefulla insatser. SIS (svenska institutet för standarder) skriver så här på sin webbplats:

> ”En standard är en gemensam lösning på ett återkommande problem. Syftet med standarder är att skapa enhetliga och transparenta rutiner som vi kan enas kring. Det ligger ju i allas intresse att höja kvaliteten, undvika missförstånd och slippa uppfinna hjulet på nytt varje gång.”

När det gäller lag och informationssäkerhet, bör det enligt vår uppfattning understrykas att även om det saknas en specifik lag om informationssäkerhet för automatiserade fordon, finns

lagar som är generellt tillämpliga och som får betydelse även för automatiserade fordon. Ett exempel är GDPR.[8]

För en kartläggning och korrekt beskrivning av vilka lagar, rättsliga krav och regelverk som gäller inom området informationssäkerhet och automatiserade fordon behöver, som vi pekat på, rättskälleläran, normhierarkin och skillnaden mellan rättsområden beaktas. Den som förmedlar kunskap om lagar bör ange hur relevant en viss norm är utifrån rättskälleläran och de förhållanden som har beskrivits i detta avsnitt 2.

För riksdag, regering och myndigheter är den egna normgivningsmakten givetvis den mest betydelsefulla. När det har klarlagts vilka behov som finns, kan lagstiftning och föreskrifter utarbetas. På så vis kan politiska visioner för landet förverkligas.[9]

Lagstiftningsprocessen och det offentligas normgivning tar tid och för att inte hämma det som ibland kallas den fjärde industriella revolutionens teknologier och möjligheten att lösa samhällsutmaningar, diskuteras i flera sammanhang hur behoven av samordnad och accelererad regelgivning ska tillgodoses.[10] Regeringen har tillsatt en kommitté (Kommittén för teknologisk innovation och etik, KOMET) som arbetar med detta. Regeringens ansats är bred och arbetet ska stärka regeringens förmåga att hantera komplexa och sektorsövergripande frågeställningar. Med policyutveckling avses i direktivet ”utvecklingen av policyer, t.ex. regelverk i form av författningar och andra föreskrifter, EU-rätt och internationell rätt och dessas tillämpningar samt riktlinjer, standarder, finansiella styrmedel och processer”.[11] Ett av de områden som kommittén bistår regeringen inom är just uppkopplade och automatiserade fordon.

[8] Förordning (EU) 2016/679 (EU) 2016/679.
[9] Regeringskansliet (Diarienummer N2017/03643/D), *För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi*.
[10] Se till exempel Armstrong, Gorst & Rae. (2019) *Renewing Regulation ‘Anticipating regulation’ in an age of disruption*, Nesta foundation, United Kingdom.
[11] Dir. 2018:85, s. 3.

3 Ansvar

3.1 Vad menas med ansvar?

Trafikanalys har gett oss i uppdrag att identifiera ansvar ur ett juridiskt perspektiv. Uppdraget väcker ett antal frågeställningar hos oss: Vad menas med ansvar? Ansvar ur vilket perspektiv? För vilka skador? I detta avsnitt 3 redogör vi på ett förenklat sätt för vad man inom juridiken menar med ansvar och vilka olika typer av ansvar som jurister brukar laborera med.

Det finns ingen övergripande definition av begreppet ansvar. För Rapporten har vi bedömt att följande definition av ansvar passar bra:

> ”Skyldighet att se till att något utförs på angivet sätt inom ett avgränsat område. Till ansvaret hör befogenheter och beslutsmandat samt att stå till svars för om något inte utförts på angivet sätt.” (MSB, Terminologi och begrepp inom informationssäkerhet, Hur man skapar en språkgemenskap, s.15)

För att våra resonemang ska vara mer begripliga vill vi lyfta en kommentar som vi tycker på ett bra sätt beskriver hur det avgörs hur det juridiska ansvaret faller ut:

> ”Det är den faktiska orsaken till det händelseförlopp som leder till en skada eller ett tillbud som avgör vem som tillskrivs ansvaret.” (Europeiska kommissionen, Meddelande från kommissionen till Europaparlamentet, Rådet, Europeiska ekonomiska och sociala kommittén och regionkommittén, Vägen mot automatiserad rörlighet – en EU-strategi för framtidens rörlighet, COM (2018) 283 final av den 17 maj 2018, s. 11)

3.2 Straffrättsligt ansvar

I Utredningen SOU 2018:16, tas både det straffrättsliga och det ekonomiska (civilrättsliga) ansvaret upp i förhållande till automatiserade fordon.

Regelverket angående användande av vägar för trafik, sträcker sig långt tillbaka i tiden och har utvecklats kring begreppet förare och vad en förare är straffrättsligt ansvarig för. Introduktion av automatiserade fordon och automatiserad körning resulterar i en förändring av innebörden av begreppen förare och kör/för. De ställer frågan om var gränsen går för en mänsklig straffbar gärning i förhållande till ett automatiskt körsystem?[12]

För att ta ställning till det straffrättsliga ansvaret behövs klarläggas vad en förares uppgifter är. Uppgifterna en förare har handlar inte bara om att köra/föra ett fordon utan även andra uppgifter som att se till att fordonet är trafikdugligt och lastat på rätt sätt. Uppgifterna omfattar även att kunna styra, gasa och bromsa ett fordon (dynamiskt körarbete) och att föra fordonet på ett säkert sätt (taktiskt körarbete).[13]

[12] SOU 2018:16, s. 534 f.
[13] SOU 2018:16, s. 538.

Vem det är som bestämmer över ett visst förhållande och är ansvarig får betydelse för det straffrättsliga ansvaret, speciellt vid bedömning av uppsåt eller oaktsamhet.[14] En gärning anses utgöra ett brott om den begås uppsåtligen om inget annat är särskilt föreskrivet.[15] För vissa brott uppkommer ansvar även vid oaktsamhet.[16]

Juridiskt ansvar utgår från skuldprincipen och legalitetsprincipen. Skuldprincipen innebär att endast den som visat skuld bör drabbas av straff eller annan brottspåföljd. Utgångspunkten är att om någon handlar utan uppsåt eller oaktsamhet så ska den inte fällas till ansvar. Straffet bör inte heller vara strängare än individens skuld. Legalitetsprincipen innebär att en gärning är brottslig endast om den kriminaliseras genom lag. Principen skyddar mot godtycklig rättstillämpning.[17]

Det man kallar strikt ansvar finns som utgångspunkt inte inom straffrätten eftersom det skulle strida mot skuldprincipen. Med strikt ansvar avses ett ansvar som uppkommer utan att någon handlat med uppsåt eller oaktsamhet.[18] I vissa särskilda lagar förekommer dock strikt ansvar framförallt för ekonomisk skada vid verksamhet som anses särskilt farlig.

Ett automatiskt körsystem kommer att resa frågorna om vem som kan ha skulden och vem som kan vara oaktsam.[19]

3.3 Ekonomiskt (civilrättsligt) ansvar för skada

Det finns olika typer av skada och följande citat sammanfattar det på ett bra sätt:

> ”I skadeståndsrätten utgår vi från ett antal skadekategorier. Personskada är fysiska och psykiska skador på människor. Sakskador är skada på fysisk egendom (saker och fastigheter). Ren förmögenhetsskada är skada på ekonomiska värden. Kränkning är en störning av människovärdet.” (Schultz, M. Twitter, 7 juni 2017 som hänvisar till inlägg på Sveriges största juridikblogg, Modern skadeståndsrätt för dummies, 27 juni 2009)
>
> ”Skadeståndsrättens grundtanke är att om någon på ett otillbörligt sätt skadat en annan så skall den som orsakat skadan ersätta den skadade med skadans värde”. (Schultz, M. Sveriges största juridikblogg, Modern skadeståndsrätt för dummies, 27 juni 2009)

Till detta kommer indelningen i skada efter om den är inomkontraktuell, det vill säga orsakas inom ramen för ett avtalsförhållande, till exempel en säljares ansvar för skada vid ett köp av en vara eller tjänst, eller utomkontraktuell, till exempel när ett fordon kör på en oskyddad trafikant.

[14] SOU 2018:16, s. 541.
[15] Brottsbalken 1 kap. 2 §, första stycket.
[16] Brottsbalken 1 kap. 3 §.
[17] SOU 2018:16, s. 553 f.
[18] SOU 2018:16, s. 554.
[19] SOU 2018:16, s. 554.

Inom en avtalsrelation är det möjligt för parterna att komma överens om vilken ersättningsnivå som ska gälla mellan parterna. På konsumenträttens område finns däremot också lagar som skyddar konsumenten och som sätter gränser för avtalsfriheten.

En skadelidande kan få ersättning för skada även om det inte finns något avtal som reglerar ersättningsrätten. Skadeståndslagen är generell och ansvar utgår från någons oaktsamhet eller vårdslöshet (skuld) medan trafikskadelagens utgångspunkt är att ersättning utgår oavsett vem som är orsak till skadan och oavsett om försäkringspremien är betald eller ej.

3.4 Produktansvar

Det finns ett särskilt ansvar för produkter som regleras i produktansvarslagen (1992:18). Produktansvaret syftar till att skydda konsumenter och ger konsumenter rätt till ersättning för person- och sakskador för det fall en produkt orsakar skada genom att det finns en säkerhetsbrist i produkten. Den som är produktansvarig är ersättningsskyldig oberoende om denne varit vårdslös eller inte, det vill säga strikt ansvar.[20]

3.5 Fordonsförsäkring och regress

Vid en olycka kommer fordonsförsäkringen för det fordon som orsakat olyckan att tas i anspråk. Försäkringen har tre delar, trafikförsäkringen (täcker personskador och skador som fordonet vållar på annans egendom), halvförsäkring (frivillig, skyddar den egna egendomen och det som transporteras i fordonet, innefattar stöldskydd, räddning, rättsskydd och maskinskada) och helförsäkring (innehåller en halvförsäkring plus en vagnskadeförsäkring som täcker skador som ägaren vållar med sitt eget fordon, till exempel vid kollision med ett annat fordon eller djur). En ny personbil kommer ofta med 3 års vagnskadegaranti och under den tiden behöver ingen vagnskadeförsäkring tecknas.[21]

Ett försäkringsbolag som har betalat ut ersättning kommer i de allra flesta fall att i sin tur kräva ersättning av, s.k. ”regressa” mot, den aktör som hade ett åliggande som den inte uppfyllde eller ett åtagande om att inte nyttja på visst sätt, som den bröt mot. Fordonsägaren, fordons-respektive komponenttillverkaren, eller det försäkringsbolag som de i sin tur har tecknat försäkring hos, kommer i slutänden att bli den som får bära det ekonomiska ansvaret för skadan. Instruktioner (ägarhandboken), avtals- och försäkringsvillkor (avgränsningar och ansvarsbegränsningar) kommer att få betydelse för vilket ersättningsansvar som den felande aktören ska bära.

[20] SOU 2018.16, s. 592–600.
[21] SOU 2018:16, s. 596.

4 Svar till Trafikanalys

4.1 Föraren

I detta avsnitt behandlas ett antal frågor om föraren och ansvar ur straffrättsligt och skadeståndsrättsligt perspektiv.

Ett självkörande fordon är ett fordon med förarstödjande teknik eller ett uppkopplat och automatiserat fordon där förarens uppgifter tagits över av tekniken. Det självkörande fordonet kan vara automatiserat i olika grad. Vi har i svaret på Trafikanalys frågor använt den nivåindelning avseende automatiseringsgrad i självkörande fordon som upprättats av amerikanska Society of Automotive Engineers (SAE).

I de olika nivåerna beskrivs förarens roll. Nivåerna i SAE är deskriptiva och tekniska snarare än juridiska. SAE är indelat i sex automatiseringsnivåer, 0–5. Förenklat innebär nivå 0 ingen automatisering alls, nivå 0–3 att det finns en fysisk förare som kör eller är beredd att ta över om systemet begär det, medan nivå 4–5 innebär att fordonet körs uteslutande av det automatiserade systemet.[22] Förarens roll i de olika graderna av automatisering beskrivs nedan.

Tabell 1 Beskrivning av automatiseringsnivåer för självkörande bilar.
Källa: SOU 2018:16, förenklad och översatt, se SAE Internationals Rapport 13016

Nivå	Namn	Definition	Utför styrning acceleration/ inbromsning	Övervakar Körningen (körmiljön)	Garant för dynamisk köruppgift	System Kapacitet (funktioner)
Mänsklig förare övervakar körningen (körmiljön)						
0	Ingen automatik	Hela dynamiska köruppgiften utförs hela tiden av den fysiske föraren, även om det finns varnings- eller interventionssystem.	Fysisk förare	Fysisk förare	Fysisk förare	Ej tillämpligt
1	Förarstöd	Köruppgiften utförs av ett förarstödjande system, med antingen styrning eller acceleration/inbromsning, med användande av information om körmiljön, under förutsättning att den fysiske föraren utför alla övriga dynamiska köruppgifter.	Fysisk förare	Fysisk förare	Fysisk förare	Vissa körfunktioner
2	Viss automatik	Köruppgiften utförs av ett förarstödjande system, med både styrning och acceleration/inbromsning, med användande av information om körmiljön, under förutsättning att den fysiske föraren utför alla dynamiska köruppgifter.	System	Fysisk förare	Fysisk förare	Vissa körfunktioner
Det automatiserade systemet övervakar körningen						
3	Villkorad automatik	Hela den dynamiska köruppgiften utförs av ett automatiskt körsystem under förutsättning att en fysisk förare ska svara på systemets begäran att ingripa på ett adekvat sätt.	System	System	Fysisk förare	Vissa körfunktioner
4	Hög automatik	Hela den dynamiska köruppgiften utförs av ett automatiskt körsystem även om en fysisk förare inte svarar på systemets begäran att ingripa på ett adekvat sätt.	System	System	System	Vissa körfunktioner
5	Full automatik	Hela den dynamiska köruppgiften utförs hela tiden av ett automatiskt körsystem på alla vägar och under alla förhållanden som en fysisk förare klarar av.	System	System	System	Alla körfunktioner

[22] SOU 2018:16, s. 181.

En förare har utöver uppgiften att köra själva fordonet en rad andra uppgifter. En del av dessa uppgifter omfattas av den så kallade garantställnigen där föraren vid underlåtenhet att utföra uppgiften riskerar ett straffrättsligt ansvar.[23]

Begreppet förare finns inte sedan tidigare definierat i svensk lagstiftning, utan det har överlåtits till rättstillämpningen att precisera.[24] Det finns ett fåtal rättsfall, om än något föråldrade, som tolkar förarbegreppet. I rättsfallet NJA 1969 s. 220 åtalades en militär befälhavare för vårdslöshet i trafik eftersom han under en militärövning hade beordrat tre militära fordon som körde efter varandra, att köra med släckta lyktor. En olycka inträffade när en bilist körde in i det sista fordonet och omkom. Den militära befälhavaren som var passagerare i det första fordonet ansågs vara trafikant och straffrättsligt ansvarig för de andra fordonen trots att han inte utförde något dynamiskt körarbete.[25]

För att möjliggöra försöksverksamhet med självkörande fordon i Sverige, infördes förordningen (2017:309) om försöksverksamhet med självkörande fordon. Förordningen innebär att det är möjligt att testa all körning av fordon på väg under förutsättning att det finns en förare i eller utanför fordonet vid färd. Enligt förordningen om försöksverksamhet med självkörande fordon krävs tillstånd för försöksverksamhet. Tillståndet är tidsbegränsat och sökanden måste kunna säkerställa trafiksäkerheten. Transportstyrelsen är den myndighet som utfärdar tillstånd. Den som uppsåtligen eller av oaktsamhet bedriver försöksverksamhet med självkörande fordon utan tillstånd eller i strid mot tillståndet kan dömas till böter.[26] I förordningen avseende försöksverksamhet finns inte någon straffbestämmelse avseende vårdslöshet vid olyckor. Däremot finns straffbestämmelser i lag (1951:649) om straff för vissa trafikbrott.

Förordningen möjliggör försöksverksamhet för fordon på automatiseringsnivå 0–3 med en förare som antingen kör eller är beredd att ta över. När det gäller fordon på automatiseringsnivå 4–5 finns tekniskt sett inte behov av någon förare men det vore felaktigt att dra slutsatsen att kravet avseende förare omöjliggör försöksverksamhet med sådana fordon. Så länge du uppfyller förordningens krav om en förare i eller utanför fordonet, anger förordningen ingenting om vilka automatiseringsgrader eller vilken teknisk funktionalitet som tillåts.[27]

Även i förslaget till lag (2019:000) om automatiserad fordonstrafik anges att föraren kan befinna sig i eller utanför fordonet, föra fordon på avstånd eller föra flera fordon samtidigt, så kallad kolonnkörning. Vissa fordon ska oavsett automatiseringsgrad ha en förare.[28] I lagförslaget föreslås även att föraren ska ansvara för att ta över under automatiserad körning om fordonet begär det. Inte heller i förslaget till lag om automatiserad fordonstrafik finns någon straffbestämmelse avseende vårdslöshet vid olyckor.

Europaparlamentets resolution (2015/2103/(INL) lämnar rekommendationer till kommissionen avseende civilrättsliga bestämmelser om robotteknik.[29] I punkt 26 i denna resolution påpekas att förarens reaktionstid vid ett oplanerat övertagande av ett fordon är av avgörande betydelse.

[23] SOU 2018.16, s.538-543
[24] SOU 2018:16, s. 565.
[25] SOU 2018:16, s. 568 f.
[26] Förordningen (2017:309) om försöksverksamhet med självkörande fordon 4 och 9 §§.
[27] SOU 2018:16, s. 319.
[28] SOU 2018:16, s. 629.
[29] Europarlamentets resolution av den 16 februari 2017 med rekommendationer till kommissionen om civilrättsliga bestämmelser om robotteknik (2015/2103/(INL), (2018/C 252/25).

4.1 Föraren och förarbegreppet	Resonemang kring ansvar i de olika frågeställningarna
Trafikanalys frågeställningar En olycka sker: 4.1.1 på grund av att en förare inte har förstått information om fordonets begränsningar[30] och i och med detta inte agerat för att förhindra en olycka; eller 4.1.2 på grund av att en förare inte har fått information om fordonets begränsningar och i och med detta inte agerat för att förhindra en olycka. Vi ser följande nyckelord: - förare/förarbegreppet - inte förstått information - inte agerat - inte fått information	**4.1.1 Vem ansvarar för en olycka som inträffar på grund av att en förare inte har förstått information om fordonets begränsningar?** En förare är skyldig att följa det allmänna aktsamhetskravet i trafikförordningen (1998:1276) (2 kap. 1 §). Det innebär bland annat att han/hon ska tillägna sig information om fordonet i fordonets ägarhandbok och annan information som krävs för att undvika trafikolyckor. Dessutom innebär garantställningen, som framgår av trafikbrottslagen (1951:649) (1 §) och trafikförordningen (2 kap.1 §), ett ansvar att tillägna sig information avseende förhållanden i omgivningen som kan innebära begränsningar för fordonet, bland annat det som kallas statisk information, som vägmärken, signaler och vägmarkeringar[31] men även säkerhetshetsrelaterad information om olyckor och trafikhinder som Trafikverket kommunicerar ut i olika kanaler.[32] En förare som i väsentlig mån brister i den omsorg och varsamhet som till förekommande av en trafikolycka betingas av omständigheterna gör sig skyldig till vårdslöshet i trafik enligt trafikbrottslagen (1 §). Enligt vår uppfattning bör bestämmelsen vara tillämplig när en förare underlåtit att tillägna sig information om fordonet eller information om förhållandena i omgivningen och därigenom orsakat en olycka. Frågan är om föraren är befriad från ansvar genom att en stor del av förarens uppgifter tagits över av det automatiserade systemet. Även i nivån med den högsta automatiseringsgraden (där det fortfarande finns en förare) – nivå 3 – har föraren alltjämt ett ansvar att tillägna sig information om fordonets begränsningar och begränsningar som förhållanden i omgivningen kan innebära. Om föraren brister i det ansvaret och om det leder till en olycka, kan han/hon dömas för vårdslöshet i trafik eller till grov vårdslöshet i trafik om försvårande omständigheter föreligger. När det gäller uppkopplade fordon bygger dagens system på att varningar ges till föraren och att denne har ett ansvar att agera om fordonets varningssystem larmar.[33] Varje fordon som är registrerat i vägtrafikregistret ska ha en trafikförsäkring enligt trafikskadelagen, (1975:1410) (2 och 3 §§). Ur trafikförsäkringen ersätts personskador och sakskador som vållats genom

[30] Dvs. vad fordonet kan göra per automatik utan att föraren behöver agera och när föraren behöver vidta en åtgärd för att fordonet ska göra det föraren vill.
[31] SOU 2018:16, s. 452.
[32] SOU 2018:16, s. 471 f.
[33] SOU 2018:16, s. 463.

	trafikolyckor. Trafikersättningen tar således över det personliga ansvar som fordonets ägare, förare eller brukare har för dessa skador. Se mer om trafikförsäkringen och regress under avsnitt 3. Ansvar. Även i skadeståndslagen (1972:207) finns generella principer avseende skadestånd som gäller oavsett om det finns ett avtal mellan skadevållaren och den skadelidande eller inte.[34] I Arbetsmiljöverkets föreskrifter (AFS 2008:3) om maskiner och allmänna råd om tillämpningen av föreskrifterna finns tydliga krav på både säkerhetsanordningar med en så kallad nödstoppsanordning och tydlig information om säkerheten för att underlätta för föraren. Information om hur maskinen stoppas vid ett nödläge torde omfattas av det allmänna aktsamhetskravet. Av Arbetsmiljöverkets föreskrifter (AFS 2008:3 6c §) framgår att tillverkaren eller tillverkarens representant som släpper ut en maskin på marknaden ansvarar för att det finns en bruksanvisning och annan nödvändig information till maskinen. Om information saknas kan sanktionsavgift dömas ut (AFS 2008:3 21 §). Det finns inte någon sanktionsbestämmelse för det fall informationen är svår att förstå. För den skada som en förare vållar i samband med yrkesutövning svarar förarens arbetsgivare, så kallat principalansvar.[35] **Slutsats** Skulle en olycka inträffa på grund av att en förare inte har förstått information om fordonets begränsningar kommer det att vara svårt för föraren att undgå ansvar då det allmänna aktsamhetskravet i trafikförordningen (2 kap. 1 §) bland annat omfattar ett krav på att tillägna sig information om fordonets begränsningar och en underlåtelse att följa detta krav som leder till en olycka torde utgöra vårdslöshet i trafik. Ett ansvar för vårdslöshet i trafik bedöms även kunna göras gällande med hänvisning till förarens garantställning. Trafikförsäkringen tar över det personliga ansvar som en förare har för skador som uppkommit genom trafikolyckor. För trafikskada som vållats av en yrkesförare svarar yrkesförarens arbetsgivare genom principalansvaret.

[34] SOU 2018.16, s. 596 ff.
[35] Arbetsmiljöverkets föreskrifter (AFS2008:3) om maskiner samt allmänna råd om tillämpningen av föreskrifterna.

	4.1.2 Vem ansvarar för en olycka som sker på grund av att föraren inte har fått information om fordonets begränsningar? Vi har utgått från tre scenarier där förare inte får information om fordonets begränsningar. I det första scenariot är det fråga om ett systematiskt fel i utformningen av fordonets informationssystem. Exempelvis om en förare inte får säkerhetskritisk information om fordonets begränsningar på grund av felkonstruktion av de säkerhetskritiska systemen i strid mot rådande tekniska standarder (ett konstruktionsfel). I det andra scenariot beror felet på slarv i tillverkningen (fabrikationsfel), till exempel om det är fel på en komponent som gör att information inte kommer fram till föraren. I det tredje scenariot föreligger fel i instruktionerna om hur informationssystemet ska användas (instruktionsfel). För olyckor till följd av samtliga dessa fel har tillverkaren, importören med flera ett skadeståndsansvar enligt produktansvarslagen (1992:18) (6 §) för de person-och sakskador som drabbar en konsument. Ansvaret är strikt men gäller inte om tillverkaren, importören med flera kan visa att säkerhetsbristen uppkommit i efterhand, till exempel genom att någon manipulerat informationssystemet. Enligt produktansvarslagen har tillverkaren, importören med flera inte något ansvar i de fall den skadelidande är en näringsidkare. Näringsidkare får istället förlita sig på avtalsregleringar, allmänna avtalsrättsliga, köprättsliga och skadeståndsrättsliga regler.[36] **Slutsats** För olyckor som sker till följd av att föraren inte fått information om fordonets begränsningar ansvarar tillverkaren, importören med flera enligt produktansvarslagen (6 §). Ansvaret är strikt. Tillverkaren eller importören kan undgå ansvar genom att visa att säkerhetsbristen inte var möjlig att upptäcka när produkten sattes i omlopp på marknaden, (8 §). Det finns i produktansvarslagen inget straffansvar för tillverkare med flera i den situationen. Produktansvarslagen är inte tillämplig när den skadelidande är näringsidkare. Ansvaret gentemot näringsidkare beror på vad som är reglerat i avtalet med tillverkaren eller importören. Vid tvist är utgångspunkten avtal och allmänna avtalsrättsliga, köprättsliga och skadeståndsrättsliga regler som gäller.[37]

[36] SOU 2018:16, s. 600 f.
[37] SOU 2018:16, s. 600.

4.2 Fordonet

I detta avsnitt behandlas ett antal frågor om ansvar vid olyckor som orsakas av olika slags mjukvarurelaterade risker/sårbarbarheter i det automatiserade körsystemet.

Det finns ett antal komponenter i ett fordon som styr fordonets funktionsområden. Exempel på en sådan styrenhet är CAN-buss. CAN-buss är särskilt viktig eftersom den sköter kommunikationen mellan styrenheter som är säkerhetskritiska. Styrenheterna är sammankopplade med datornätverk som möjliggör att de kommunicerar med varandra.[38] Varje styrenhet innehåller komponenter som innehåller olika mjukvaror. Dessa mjukvaror uppdateras kontinuerligt.

Fordonstillverkare kan styra uppdatering av mjukvarorna i de fordon som de har tillverkat. Uppdateringar kan även göras genom att fordonet kopplas upp mot fordonstillverkarens dator på en verkstad och ”over the air”. Om uppdateringen sker genom uppkoppling mot en fordonstillverkares dator går det mycket långsammare än om uppdateringen sker ”over the air”. Uppdatering ”over the air” möjliggör för fordonstillverkare att snabbt ändra mjukvaran i ett redan typgodkänt fordon. Det ställer frågor om vilken frihet tillverkare ska ha att ändra mjukvaror i ett redan typgodkänt fordon. Ett exempel är den uppdatering som Tesla genomförde av modell S, version 7.0, år 2015.[39]

Frågor kring uppdatering av mjukvara orsakar en del problem som behöver lösas på internationell nivå.[40] WP.29 – en arbetsgrupp inom FN-organet UNECE (Förenta nationernas ekonomiska kommission för Europa) – har kommit med ett utkast till regler om uppdateringar ”over the air”.[41]

För att ett fordon ska kunna säljas på en marknad i större skala krävs ett typgodkännande enligt 2 kap. 1 § fordonsförordningen. Ett typgodkännande är ett sätt att kontrollera att fordonet är tillförlitligt, säkert och lämpligt för trafik. En uppdatering av en mjukvara i ett fordon kan kräva ett nytt typgodkännande av fordonet, vilket kan påverka fordonets ägare såtillvida att denne kan behöva göra en särskild besiktning av fordonet, en registreringsbesiktning enligt 4 kap. 3 § fordonsförordningen.

[38] SOU 2018:16, s. 383 f.
[39] SOU 2018:16, s. 715 f.
[40] SOU 2018:16, s. 715 f.
[41] United Nations, Economic and Social Council, Economic Commission for Europe, Proposal (ECE/TRANS/WP.29/2020/79) for a new UN Regulation on uniform provisions concerning the approval of vehicles with regard to cyber security and cyber security management system av den 2 April 2020.

4.2 Fordonet och mjukvara	Resonemang kring ansvar i de olika frågeställningarna
Trafikanalys frågeställningar En olycka sker**:** 4.2.1 på grund av att det finns ursprungliga säkerhetsfel i fordonets mjukvara; 4.2.2 på grund av ett intrång eftersom det fanns brister i säkerheten vid uppdatering av någon av fordonets mjukvaror; 4.2.3 eftersom en icke-auktoriserad verkstad/ besiktningsfirma har modifierat/bytt ut mjukvarukomponenter i fordonet; eller 4.2.4 på grund av den prioritering som fordonets mjukvara gör vid kollision. Vi ser följande nyckelord: - ursprungliga säkerhetsfel i mjukvaran - brister i uppdatering av mjukvara - behörig modifiering /åtkomst av mjukvara - prioritering av mjukvara	**4.2.1 Vem ansvarar för en olycka som sker på grund av att det finns ursprungliga säkerhetsfel i mjukvaran?** Mjukvaran i ett automatiserat körsystem i ett självkörande fordon är en del av den produkt som fordonet utgör. Ursprungliga säkerhetsfel i mjukvaran är därmed ett fel i en produkt. För skador som uppkommit vid en olycka på grund av ursprungliga säkerhetsfel i mjukvaran ansvarar tillverkaren med flera enligt produktansvarslagen.[42] Produktansvaret gäller enbart gentemot konsumenter.[43] Produktansvaret enligt produktansvarslagen (1992:18) är strikt. Tillverkaren med flera kan undgå ansvar genom att visa att säkerhetsbristen inte var möjlig att upptäcka när produkten sattes i omlopp på marknaden, produktansvarslagen (8 §). Det finns inget straffansvar för fel i produkter i produktansvarslagen. Näringsidkare får reglera ansvaret i avtal och säkerställa att motparten har en fullgod ansvarsförsäkring, och vid tvist får näringsidkaren använda sig av allmänna avtalsrättsliga regler samt köprättsliga- och skadeståndsrättsliga regler.[44] **Slutsats** Skulle en olycka ske på grund av ursprungliga säkerhetsfel i mjukvaran så ansvarar tillverkaren och andra produktansvariga enligt produktansvarslagen (6 §) gentemot konsumenter. Ansvaret är strikt. Tillverkaren eller importören kan undgå ansvar genom att visa att säkerhetsbristen inte var möjlig att upptäcka när produkten sattes i omlopp på marknaden, produktansvarslagen (8 §). Det finns inget straffansvar i produktansvarslagen. Ansvaret gentemot näringsidkare beror på vad som är reglerat i avtalet med tillverkaren med flera. Vid tvist utgår domstolen från vad som är avtalat och från allmänna avtalsrättsliga, köprättsliga och skadeståndsrättsliga regler som gäller.[45]

[42] SOU 2018:16, s. 600.
[43] SOU 2018:16, s. 44.
[44] SOU 2018:16, s. 600.
[45] SOU 2018:16, s. 600.

	4.2.2 Vem ansvarar för en olycka som sker på grund av ett intrång som gjorts möjligt genom brister i säkerheten vid uppdatering av någon av fordonets mjukvaror? Fordon kan utsättas för intrång av olika slag. Vi har i vårt svar bedömt två slags intrång; intrång vid uppdateringar av mjukvarorna och intrång i ett system hos en underleverantör som tillverkar viktiga säkerhetsrelaterade komponenter till fordonet. Vid uppdatering av en mjukvara är mjukvaran exponerad för intrång. Det är särskilt viktigt att skydda mjukvaran i CAN-buss eftersom detta system kommunicerar med de styrenheter som är säkerhetskritiska för fordonets funktion.[46] Om någon gör intrång i ett system hos en underleverantör som levererar säkerhetskritiska komponenter till fordon kan konsekvenserna bli omfattande om tillverkningen sker för många fordonstillverkare över hela världen.[47] Fordonstillverkare i USA har kommit överens om att arbeta i enlighet med ett antal principer när det gäller informationssäkerhet. I Europa finns liknande överenskommelser mellan fordonstillverkare. Europeiska fordonstillverkare som är medlem i ACEA (The European Automobile Manufacturer´s Association) ska efterleva ACEA Principles of data protection in relation to connected vehicles and services, September 2015.[48] **Slutsats** I dagsläget finns ingen lagstiftning i Sverige som ställer krav på hur fordonstillverkare ska utforma sin informationssäkerhet avseende tjänster och produkter. Fordonstillverkare i Europa som är medlemmar i ACEA har kommit överens om att beakta informationssäkerhet när de utformar nya processer, tjänster och produkter. Detta är en frivillig överenskommelse som inte innehåller något straffrättsligt eller skadeståndsrättsligt ansvar. UNECE antog den 24 juni 2020 nya bestämmelser avseende cybersäkerhet och mjukvaruuppdateringar för att fastställa tydliga prestandakrav och revisionskrav för fordonstillverkare.[49]

[46] SOU 2018:16, s. 717.
[47] SOU 2018:16, s.716.
[48] SOU 2018:16, s. 408 f.
[49] ECE-TRANS-WP29_2020-079-Revised. ECE/TRANS/WP.29/2020/80.

	4.2.3 Vem ansvarar för en olycka på grund av att en icke-auktoriserad verkstad har modifierat/bytt ut mjukvarukomponenter i fordonet Enligt Europaparlamentets och rådets förordning (EU) 2019/2144 är det tillåtet att använda sig av en icke auktoriserad verkstad. Fordonstillverkaren har en skyldighet att till verkstaden lämna ut diagnostisk information och uppgifter som är relevanta för att reparera och underhålla fordonet.[50] Fordonsägaren har möjlighet att ingå avtal med valfri verkstad som ska utföra reparation och underhåll. Om fordonsägaren är konsument regleras vad som gäller mellan fordonsägaren och verkstaden av konsumenttjänstlagens (1985:716) bestämmelser som är ett slags grundskydd för konsumenten. Ett avtal får inte innehålla villkor som sätter konsumenten i ett sämre läge än vad som framgår av bestämmelserna i konsumenttjänstlagen.[51] Skulle verkstaden byta ut eller modifiera en mjukvara och orsaka skada blir verkstaden skadeståndsskyldig (konsumenttjänstlagen 31 §). Skadeståndsansvaret är ett så kallat kontrollansvar och omfattar i princip all ekonomiska skada som konsumenten drabbats av, inklusive skador som uppkommer vid en olycka, under förutsättning att konsumenten kan visa på ett adekvat orsakssamband mellan skadan och modifieringen/bytet av mjukvaran.[52] I EU:s förordning (EU) 2019/2144, skäl 27 pekas på behovet av att fastställa regler och tekniska krav avseende modifiering av mjukvara. Om fordonsägaren är en näringsidkare gäller inte konsumenttjänstlagen, utan verkstadens ansvar beror på vad som är reglerat i avtalet mellan näringsidkaren och verkstaden samt allmänna avtalsrättsliga, köprättsliga och skadeståndsrättsliga regler. **Slutsats** För en olycka till följd av att en icke auktoriserad verkstad modifierat eller bytt ut en mjukvarukomponent i fordonet, ansvarar verkstaden enligt konsumenttjänstlagen om den skadelidande är konsument. Om den skadelidande är näringsidkare tillämpas avtalet mellan parterna med utfyllnad av allmänna avtalsrättsliga, köprättsliga och skadeståndsrättsliga regler.

[50] Europaparlamentets och rådets förordning (EU) 2019/2144 av den 27 november 2019 om krav för typgodkännande av motorfordon och deras släpvagnar samt de system, komponenter och separata tekniska enheter som är avsedda för sådana fordon, med avseende på deras allmänna säkerhet och skydd för personer i fordonet och oskyddade trafikanter.
[51] SOU 2018:16, s. 590.
[52] SOU 2018:16, s. 592.

	4.2.4 Vem ansvarar för eventuell prioritering som mjukvaran gör vid kollision? Problemet med den prioritering som ska göras vid en kollision har ibland illustrerats genom det som brukar kallas ”the trolley problem” och presenteras som ett etiskt dilemma där en förare inför ett förestående olyckstillbud tvingas välja mellan människoliv. Frågor kring etik och moral avseende självkörande fordon har diskuterats av forskare och samhällsdebattörer och de har även tagits upp av den amerikanska säkerhetsorganisationen National Highway Traffic Safety Administration (NHTSA) i deras riktlinjer för automatiserade fordon från 2016.[53] I Tyskland kom en etikkommission med en rapport i juni 2017 med etikregler som autonoma fordon borde följa. Av dessa regler framgår bland annat att ett automatiserat fordon alltid ska rädda mänskligt liv framför infrastruktur och djur.[54] På EU-nivå har det tagits fram etiska riktlinjer för tillförlitlig artificiell intelligens (AI).[55] **Slutsats** Det finns inga lagregler i Sverige som reglerar vilken prioritering mjukvaran i ett fordon ska göra vid en kollision. På EU-nivå finns etiska riktlinjer för AI.

[53] SOU 2018:16, s. 1136. Se riktlinjer: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf
[54] SOU 2018:16, s. 1136. Se riktlinjer: https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2017/06/084-dobrindt-bericht-derethik-kommission.pdf
[55] Oberoende expertgrupp på hög nivå för AI-frågor inrättad av Europeiska kommissionen i juni 2018, *Etiska riktlinjer för tillförlitlig AI*, 8 april 2019. Se riktlinjer: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

4.3 Infrastrukturen

I det tredje avsnittet som vi har tittat på ställs ett antal frågor om ansvar och infrastrukturen.

Som på andra områden pågår en digitalisering av väginfrastrukturen. Från att det tidigare bara varit människor som behövt förstå och tolka vägmärken och efterleva regelverken, behöver detta numera kunna göras av fordon. Fordon utrustade med förarstödjande teknik och uppkopplade och allt mer automatiserade fordon ställer därmed nya krav, både digitala och fysiska, på väginfrastrukturen.

Det finns en tredimensionell nationell väg- och kartdatabas, NVDB, som täcker Sveriges vägnät och innehåller information om vilka trafikregler som gäller och hur en väg kan användas. Olika aktörer lämnar information till databasen, däribland Trafikverket, Transportstyrelsen, Lantmäteriet och kommunerna men som påpekas i Utredningen SOU 2018:16 behöver man vara medveten om att databasen idag inte innefattar juridiskt ansvar för informationen. När det till exempel gäller en lokal trafikföreskrift är det istället kommunen som genom sitt beslut ansvarar för den lokala trafikföreskriften och för att Lantmäteriet ska ta ansvar för en viss geografisk punkt på en karta behöver en lantmäteriförrättning ha hållits. Liknande databaser finns i flera andra europeiska länder och det finns också samarbeten på europeisk nivå. Det finns exempel på nationella databaser till vilka kommersiella aktörer bidrar med information men så sker inte till NVDB.[56]

Sedan flera decennier pågår ett intensivt arbete med att utveckla och implementera ITS, *intelligent transportation systems,* som är ett samlingsnamn för kommunikationssystem på vägtrafikområdet. C-ITS, *co-operative intelligent transportation systems*, handlar om samverkan och interaktion mellan fordon, trafikanter och väginfrastrukturen. På så vis kan fordon lämna och få information om sin egen och andra fordons status liksom information om väg- och trafikdata. Syftet är bland annat att öka trafiksäkerheten och på sikt ge oss det som ibland kallas smarta städer.[57] Sedan 2018 måste alla personbilar inom EU vara utrustade med eCall, det vill säga en funktion som vid olycka automatiskt sänder information för att påkalla hjälp. eCall är en del av EU:s ITS-koncept.[58] Från EU:s håll har man drivit på och velat besluta om ett gemensamt ramverk och fastställda standarder för ITS.

Kommunikation fordon till fordon brukar benämnas ”V2V” *vehicle to vehicle,* fordon till infrastruktur ”V2I” *vehicle to infrastructure* och fordon till fotgängare eller andra oskyddade trafikanter ”V2P” *vehicle to person*. Vidare finns uppkoppling mellan fordon och nätverk ”V2N” *vehicle to network*. Det talas också om ”V2X” *vehicle to anything communication* som innebär uppkoppling till i princip vad som helst, ett sakernas internet, ”*Internet of things, IoT*”.[59]

Stor betydelse när det gäller informationssäkerhet och infrastrukturen, har NIS-direktivet som implementerats i Sverige genom NIS-lagen. Med samhällsviktiga tjänster rörande vägtransport där incidenter skulle medföra en betydande störning vid tillhandahållandet av tjänsten avses enligt MSB:s föreskrifter (MSBFS 2018:7) bland annat intelligenta transportsystem för tjänsterna larmcentraler för eCall och rikstäckande statliga databaser som innehåller uppgifter om hastighetsgräns, vägbredd, bärighet, samt rekommenderad väg för farligt gods.[60] NIS-

[56] SOU 2018:16, s. 454-458.
[57] SOU 2018:16, s. 242-245, 462-469. För begreppet smarta städer, se t. ex. SIS Svenska Institutet för standarder, https://www.sis.se/standarder/omrade/smarta-stader/
[58] SOU 2018:16, s. 399.
[59] SOU 2018:16, s. 188, 460–461.
[60] Myndigheten för samhällsskydd och beredskaps (MSB) föreskrifter MSBFS 2018:7, 4 kap. 4 §.

direktivet hänvisar till EU-parlamentets och rådets direktiv nr 2010/40 (”ITS-direktivet”)[61] där definitionen av intelligenta transportsystem lyder ”system i vilka informations- och kommunikationsteknik tillämpas på vägtransportområdet, inklusive infrastruktur, fordon och användare, och för trafikledning och mobilitetshantering, samt för gränssnitt mot andra transportslag”.[62]

Trafikverket har för perioden 2018–2029 beskrivit mål och åtgärder för att åstadkomma den digitala infrastruktur som uppkopplade och automatiserade fordon kräver, det vill säga främst de IT-lösningar i form av mjuk- och hårdvara som behövs för att information ska samlas in och kunna tillgängliggöras. Det handlar om grunddata om trafikregler, trafikföreskrifter, trafiksituationen och data om vägnätet i standardiserat format och via lämpliga gränssnitt. Detta för att uppnå regeringens vision om att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter. Här ingår översyn av NVDB, adekvat vägsidesutrustning för kommunikation och Trafikverket lyfter frågor om analys av enorma datamängder, så kallad *Big data*, samt behovet av informationssäkerhet och kravet på integritetsskydd.[63]

När väginfrastrukturen förändras, kommer nya perspektiv på ansvar. Med ökat informationsflöde och komplexa system, finns många aktörer och åtskilliga led där brister kan finnas och saker gå fel. Vilket ansvar ska staten ta för informationen? Väghållaren, det vill säga i Sverige primärt kommuner och staten genom Trafikverket, bär idag ansvar för bristande underhåll av infrastrukturen. Exakt vilket underhåll och skick som krävs är inte klarlagt utan får avgöras från fall till fall. Om tekniken brister och ett fordon inte förstår att tolka infrastrukturen rätt, är det fordonstillverkaren eller tillhandahållaren av infrastrukturens olika delar som bär ansvar? Var går gränsen mellan olika aktörers ansvar? Ansvar måste avgöras mot något slags måttstock för vad som är objektivt riktigt agerande och vad som är otillräckligt eller vårdslöst. Här finns också frågan om ansvar i några situationer bör vara strikt. Vi delar Trafikanalys uppfattning att det behöver göras en kartläggning av risker och en analys av hur riskerna inom C-ITS bör hanteras.[64] Detta skulle ge kunskap för det offentligas fortsatta arbete och eventuella beslut om hur ansvaret bör fördelas. När det gäller säkerhet och datahantering, särskilt hantering av personuppgifter, resonerar vi kring personuppgiftsansvar i avsnitt 4 nedan.

Säkerhetskrav på fordon, fordonskomponenter, privata enheter utgår i många fall från standarder. När lagstiftning hänvisar till en viss standard, lyfts standarden och får en officiell roll som måttstock mot vilken ett förhållande eller agerande kan bedömas och eventuellt ansvar fastställas. Vad en beställare kräver av en leverantör och vilka krav en leverantör åtar sig att leva upp till, kommer parterna överens om genom avtal. Fordonstillverkarens avtal och instruktioner (ägarhandboken) till fordonsägaren sätter ramar och beskriver vars och ens ansvar och begränsning av ansvar. Vid en ansvarsbedömning i domstol kan i branschen tillämplig praxis och de av privaträttsliga standardiseringsorgan på frivillig väg satta standarder få betydelse.

---

[61] Europaparlamentets och rådets direktiv (EU) 2010/40 av den 7 juli 2010 om ett ramverk för införande av intelligenta transportsystem på vägtransportområdet och för gränssnitt mot andra transportslag.
[62] NIS-direktivet Bilaga II, Typer av enheter enligt artikel 4.4, 2 d Vägtransport, – Operatörer av intelligenta transportsystem enligt definitionen i artikel 4.1 i Europaparlamentets och rådets direktiv 2010/40/EU av den 7 juli 2010 om ett ramverk för införande av intelligenta transportsystem på vägtransportområdet och för gränssnitt mot andra transportslag, artikel 4.1.
[63] Trafikverket (2017) *Digitaliseringens möjligheter, PM till Nationell plan för transportsystemet 2018–2029*. Regeringskansliet (Diarienummer N2017/03643/D), *För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi*. För begreppet big data, se t. ex. Computer Sweden IDG, IT-ord, Ord och uttryck i It-branschen, https://it-ord.idg.se/ord/big-data/
[64] Trafikanalys (Rapport 2019:8), s. 83.

Förutom NIS-direktivet, NIS-lagen och ITS-direktivet, där det senare har implementerats i svensk rätt genom Lag (2013:315) om intelligenta transportsystem vid vägtransporter (”ITS-lagen”) och Förordning (2016:383) om intelligenta transportsystem vid vägtransporter, kan följande lyftas fram när det gäller regelverk för infrastrukturen.

I mars 2019 antog Kommissionen en så kallad delegerad förordning (EU), C (2019) 1789 final[65] som Europeiska unionens råd (Ministerrådet), sedan invände mot enligt den process som gäller för delegerade förordningar, vilket förhindrade att förordningen trädde i kraft. Därmed kom regleringar som troligen skulle ha fått betydelse för ansvarsfrågan, inte till stånd på EU-rättslig nivå. De föreslagna reglerna var avsedda att harmonisera och underlätta utbyggnaden av C-ITS. Arbetet har bedrivits i samråd med företrädare för industrin. Den delegerade förordningen innehöll EU-övergripande specifikationer och standarder, rättsliga minimikrav för interoperabilitet och tilldelade rättsliga organ styrande funktioner. Den delegerade förordningen angav vilken kommunikationsteknik som skulle användas inklusive en översynsklausul för att lägga till framtida teknik, krav på CE-märkning och satte en gemensam tillitsmodell, PKI-kryptering med öppen nyckel, på plats. Parallellt har industrin genom de europeiska standardiseringsorganen arbetat med standardisering på frivillig väg. Organisationer som företräder fordonsindustrin och telekomindustrin har uttryckt sig positivt till att Ministerrådet motsatte sig den delegerade förordningen och att denna inte antogs.[66]

Ansvarsfrågor berörs också i Kommissionens meddelande COM (2016) 766 final[67] samt Kommissionens meddelande COM (2018) 283 final.[68]

[65] Kommissionens delegerade förordning (EU) C (2019) 1789 final av den 13 mars 2019 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller införande och operativ användning av samverkande intelligenta transportsystem.
[66] GSMA Europe (2019) *Statement on the rejection of the Delegated Act C-ITS*, hämtad 24 juni 2020. 5GAA Press Release 12/07/2019) *5GAA welcomes Council objection against C-ITS Delegated Act*, hämtad 24 juni 2020.
[67] Kommissionens Meddelande till Europaparlamentet, rådet, europeiska ekonomiska och sociala kommittén och regionkommittén av den 30 november 2016 om en europeisk strategi för samverkande intelligenta transportsystem, en milstolpe mot samverkande, uppkopplad, automatiserad rörlighet, COM (2016) 766 final.
[68] Kommissionens Meddelande till Europaparlamentet, rådet, europeiska ekonomiska och sociala kommittén och regionkommittén av den 17 maj 2018 om vägen mot automatiserad rörlighet – en EU-strategi för framtidens rörlighet, COM (2018) 283 final.

4.3. Angrepp utifrån	Resonemang kring ansvar i de olika frågeställningarna
Trafikanalys frågeställningar En olycka sker: 4.3.1 till följd av intrång i fordonets system via passagerare eller förares personliga enheter kopplas upp mot fordon; 4.3.2 som en följd av cyberattacker mot servrar (placerade i Sverige, i annat land inom EU, utanför EU) eller mot en molntjänst (tillhandahållna av företag med moderbolag som är underställt tredje lands jurisdiktion); 4.3.3 till följd av bristande teknisk interoperabilitet mellan ett uppkopplat autonomt fordon och den digitala transportinfrastrukturen i Sverige. Vi ser följande nyckelord: - intrång via personlig enhet - cyberattack server + placering server - cyberattack molntjänst + jurisdiktion som molntjänstföretaget lyder under - bristande interoperabilitet	**4.3.1 Intrång via personliga enheter** Det är fordonstillverkaren som avgör och ger instruktioner för hur en personlig enhet får anslutas till ett fordon. Tillverkaren behöver se till att fordonet är konstruerat så att det skyddas mot obehörig åtkomst och attacker genom att vidta lämpliga tekniska åtgärder, till exempel att brandväggar finns, för att säkerställa en tillräcklig säkerhetsnivå.[69] De elektroniska styrsystem i fordonet som kategoriseras som kritiska eller viktiga system måste vara åtskilda från icke-kritiska system. Tillverkaren måste skydda fordonet mot otillbörlig access till säkerhetskritiska styrenheter som skulle kunna ske via fordonets infotainmentingång eller via den så kallade OBD-porten (diagnosuttaget, som kan vara fysiskt eller trådlöst) som primärt finns till för service och för uppdatering av mjukvara.[70] En passagerare som tittar på Netflix får inte riskera att samtidigt släppa in en angripare som begår intrång i fordonet. Det är upp till fordonstillverkaren att kravställa och utvärdera säkerhet när fordonskomponenter beställs och inkorporeras i fordonen. Tillverkare av komponenter svarar för säkerheten i komponenterna utifrån avtalade krav och tillämpliga standarder. Tillverkare av personliga enheter, mobiltelefoner, läsplattor etcetera, svarar för att enheterna är säkra. En fordonstillverkare måste avgöra om enheterna är kompatibla med fordonets system och kraven som ställs där. Fordonsägaren ansvarar för att inte ansluta och för att se till att den som fordonsägaren låter använda fordonet inte ansluter personliga enheter till fordonet på ett sätt som är otillåtet enligt avtalet och instruktionerna (ägarhandboken) för fordonet. **Slutsats** Skulle en olycka uppkomma till följd av intrång i fordonets system via en personlig enhet, måste det klarläggas hur bristen kunnat uppkomma och vilken aktör som har brustit i sina åligganden. De gäller såväl civilrättsligt som straffrättsligt. Se avsnitt 4.1 om förarens ansvar och att det inte riktigt finns juridiskt definierat vad förarens ansvar omfattar i de olika SAE-nivåerna. De instruktioner som fordonstillverkaren har lämnat och de avtal som den som förvärvar fordonet har ingått vid förvärvet och senare, kommer att få betydelse för hur det civilrättsliga (ekonomiska) ansvaret mellan aktörerna fördelas. I avtalen finns ofta villkor om ansvarsbegränsning men skulle den som brustit i sina skyldigheter ha visat prov på

[69] SOU 2019:16, s. 409.
[70] SOU 2018:16, s. 383-385.

	uppsåt eller grov vårdslöshet kan ett sådant villkor under vissa omständigheter vara ogiltigt. Se också om trafikförsäkring och regress under avsnitt 3. Ansvar.
	4.3.2 Cyberattacker mot servrar (placerade i Sverige, i annat land inom EU, utanför EU) eller mot en molntjänst (tillhandahållen av företag med moderbolag som är underställt tredje lands jurisdiktion Förarstödjande teknik och självkörande fordon förutsätter en omfattande infrastruktur som möjliggör säker och tillförlitlig kommunikation, allt i ett omfattande ekosystem av aktörer som väghållare, tillhandahållare av väginfrastruktur, fordonstillverkare, förare och andra trafikanter. En cyberattack skulle kunna rikta sig mot en fordonstillverkares servrar mot vilka fordonen av tillverkarens märke är uppkopplade eller mot molntjänster som fordonstillverkaren använder. Om Kommissionens delegerade förordning C (2019) 1789 final hade trätt i kraft hade man kunnat tänka sig en cyberattack mot tillitsmodellen för C-ITS-stationer baserad på infrastruktur för kryptering med öppen nyckel (PKI) som på högsta nivå skulle bestå av ett antal rot-CA vilka ”aktiverats” när Förvaltaren av förteckningen över betrodda certifikat (TLM) fört upp deras certifikat i en europeisk förteckning över betrodda certifikatsinstanser (ECTL). Förordningen skulle ha varit bindande för alla rättssubjekt som deltar i det betrodda C-ITS-systemet i Europa.[71] En rot-CA skulle enligt Kommissionens delegerade förordning C (2019) 1789 final kunna skötas både av en offentlig och en privat organisation.[72] Vid upptäckt av en sådan incident skulle TLM och rot-CA ha behövt underrättas.[73] Både vägmyndigheter (enligt definition i Kommissionens delegerade förordning 2015/962, artikel 2.12)[74] med ansvar för trafikstyrning och trafikledning och operatörer av intelligenta transportsystem (enligt definition i ITS-direktivet, artikel 4.1)[75] är sådana leverantörer av samhällsviktiga tjänster som omfattas av NIS-lagens krav att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete och skyldighet att rapportera incidenter som har betydande inverkan på kontinuiteten i den samhällsviktiga tjänst som de tillhandahåller (NIS-

[71] Kommissionens delegerade förordning (EU) C (2019) 1789 final av den 13 mars 2019, Annex 3, Bilaga III, s. 9, punkt 1.1.
[72] C (2019) 1789 final, Annex 3, Bilaga III, s. 14, punkt 1.3.
[73] C (2019) 1789 final, s. 14 och Annex 3, Bilaga III, s. 58, punkt 5.7 Hantering av påverkan och haverier.
[74] Kommissionens delegerade förordning (EU) 2015/962 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller tillhandahållande av EU omfattande realtidstrafikinformationstjänster av den 18 december 2014.
[75] Enligt definitionen i artikel 4.1 i Europaparlamentets och rådets direktiv 2010/40/EU.

	lagen 11, 18 §§). Vid outsourcing måste säkerhet kravställas. Medlemsstaterna ska säkerställa att leverantörer av samhällsviktiga tjänster vidtar föreskrivna åtgärder och Transportstyrelsen är tillsynsmyndighet[76]. Lagen gäller inte för verksamhet som omfattas av säkerhetsskyddslagen (NIS-lagen 8 §). Det är inte i första hand brister i driftsäkerhet eller teknisk säkerhet som föranlett att offentlig sektors användning av molntjänster har debatterats utan diskussionen gäller om användningen är lämplig och om svensk rätt och EU-rätt förhindrar att viss information lagras i en molntjänst som tillhandahålls av en leverantör som är underkastad tredje lands jurisdiktion (det vill säga land utanför EU eller Europeiska ekonomiska samarbetsområdet ”EES”), till exempel på grund av att sådant tredje lands lag gör det möjligt för en myndighet i tredje landet att begära ut information även om informationen fysiskt lagras på en server inom EU. Både Kina, Indien och USA har enligt uppgift sådan lagstiftning. Här finns också behovet av att tillse att de villkor enligt vilka molntjänsten tillhandahålls överensstämmer med kraven i GDPR och att lagring av informationen i en molntjänst är förenlig med svensk rätt. Hur informationen klassas, det vill säga vilken typ av information som det är den offentliga aktören har för avsikt att lagra på en server i tredje land eller hantera i molntjänsten som tillhandahålls av ett företag som lyder under tredje lands lag, om det till exempel är säkerhetsklassad information eller alldaglig och mindre känslig information, kan spela roll vid bedömningen[77]. **Slutsats** Den som bestämmer ändamål och medel med den behandling av personuppgifter som utförs (den personuppgiftsansvarige) måste, innan beslut fattas om att personuppgifterna ska behandlas på en server utanför Sverige, inom eller utanför EU eller i en molntjänst, tillse att de villkor enligt vilka tjänsten tillhandahålls överensstämmer med GDPR och att behandlingen av personuppgifterna är förenlig med svensk rätt och med de åtaganden som den personuppgiftsansvarige har gjort gentemot de registrerade. Som ovan angetts spelar det också in hur informationen klassas, till exempel om det är säkerhetsklassad information. Skulle en olycka uppkomma till följd av en attack mot en server, en molntjänst, måste det klarläggas hur bristen kunnat

[76] Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster, 17 §.
[77] Försäkringskassan (2019) *Vitbok Molntjänster i samhällsbärande verksamhet – risker, lämplighet och vägen framåt*, innehåller en genomgång av olika aspekter på användning av molntjänster som tillhandahålls av privata aktörer. Genom Dir 2019:64 har regeringen tillsatt en särskild utredare. Cirio Advokatbyrås skrift (2020) *Molntjänster, offentlighet och sekretess i offentlig sektor* belyser några särskilda frågor. eSam, Skatteverket och Försäkringskassan (2020) bemöter Cirios skrift i *Kommentar till kritisk rapport om molntjänster i offentlig sektor*. En grupp leverantörer av svenska molntjänster ger sin syn i Computer Sweden, IDG, (2020) Christenson J. m.fl., *Molntjänster måste värna Sveriges digitala suveränitet*. Se också EU-domstolens avgörande Schrems II (C-311/18) som till exempel kommenteras av Wendleby, M. (2020), Passacon AB, JP Juridiskt bibliotek, JP Infonet, *Livet efter Schrems II – kommer vi att kunna överföra personuppgifter till USA?*

	uppkomma och vilken aktör som har brustit i sina åligganden samt vilket slags information det rör sig om. De leverans- och avtalsvillkor som serverdrift, molntjänst med mera tillhandahålls enligt, kommer att få betydelse för vilket civilrättsligt (ekonomiskt) ansvar den aktör som tillhandahåller tjänsten har. I villkoren finns ofta ansvarsbegränsningar men skulle den som begått ett fel eller brustit i sina åtaganden ha visat prov på uppsåt eller grov vårdslöshet kan ett sådant villkor under vissa omständigheter vara ogiltigt. Även om den tillitsmodell för och infrastrukturen av C-ITS-stationer som föreslogs genom den delegerade förordningen C (2019) 1789 final, hade kommit på plats, skulle det för att fastställa ansvar ha behövt klarläggas hur en attack kunnat inträffa, mot vilken sårbarhet och vilken aktör som brustit i sina åligganden.
	4.3.3 Bristande teknisk interoperabilitet mellan ett uppkopplat autonomt fordon och den digitala infrastrukturen i Sverige Ett automatiserat fordon är utrustat med sensorer kopplade till processorer för att möjliggöra automatiserad körning. Syftet är att bilda sig en uppfattning om miljön runt fordonet men även sensorer som mäter förhållanden i själva fordonet behövs för att fordonet ska kunna köra självt.[78] Kommunikationen V2V, V2P samt V2I och V2X skulle enligt den delegerade förordningen C (2019) 1789 final (vilken stoppats av Ministerrådet och alltså inte trätt i kraft) ske via vägsides, fordonsbaserade respektive handhållna C-ITS-stationer som bidrar med uppgifter till C-ITS-nätet. För att säkerställa interoperabilitet föreskrevs att både C-ITS-stationerna och C-ITS-tjänster skulle ha en särskild konfiguration av standarder, kallat system- respektive tjänsteprofil. EU-kommissionen skulle för detta ändamål anta rättsligt bindande EU-specifikationer med funktionella och tekniska minimikrav. Kommunikation var tänkt att ske genom en hybridkommunikationsmetod (både teknik för kortdistanskommunikation och teknik för kommunikation på längre distans). Enligt den delegerade förordningen C (2019) 1789 final gav EU standardiseringsorganen CEN, Cenelec och Etsi mandat inom området för informations- och kommunikationsteknik för att stödja interoperabiliteten mellan samverkande system för ITS. En medlemsstats marknadskontrollmyndighet skulle ha mandat att förbjuda eller begränsa tillhandahållandet av C-ITS-stationer som inte höll måttet.[79]

[78] SOU 2018:16, avsnitt 8.2.3.
[79] C (2019) 1789 artikel 17 punkt 4.

	Slutsats Skulle en olycka uppkomma till följd av bristande interoperabilitet, måste det klarläggas hur bristen kunnat uppkomma. För det fall den delegerade förordningen C (2019) 1789 final hade trätt i kraft, och det framkom tydliga brister i regelgivningen kunde ansvar för något av standardiseringsorgan CEN/CENELEC eller Etsi ha aktualiserats. Om det brustit i efterlevnad av CE-märkningskraven när det gäller konstruktion eller tillverkning av C-ITS-stationerna, hade det behövt utrönas om det var tillverkaren, importören eller distributören som brustit i sina åligganden. Att C (2019) 1789 final inte trätt ikraft betyder inte att ansvaret är oreglerat utan allmänna regler om inom- och utomkontraktuellt skadeståndsansvar gäller fortsatt. Genom den delegerade förordningen skulle åligganden och ansvar ha tydliggjorts, fördelats och sannolikt blivit mer förutsägbart.

4.4 Säkerhet och personuppgifter

I det fjärde avsnittet behandlas ett antal frågor om säkerhet och personuppgifter.

Det övergripande ramverket på området personuppgifter är GDPR. GDPR är en generell lag som även reglerar informationssäkerhet. Ett annat relevant ramverk är EU:s ePrivacydirektiv som innehåller regler om skydd för själva kommunikationen och har implementerats i svensk rätt genom lagen (2003:389) om elektronisk kommunikation. UNECE antog den 24 juni 2020 ett nytt regelverk för cybersäkerhet och mjukvaruuppdateringar.[80]

I januari 2020 gav Europeiska dataskyddsstyrelsen (European Data Protection Board, EDPB) ut riktlinjer om personuppgiftsbehandling i anslutning till uppkopplade fordon mm (”EDPB:s riktlinjer 1/2020”).[81] Under den offentliga konsultationen fram till 4 maj 2020 har EDPB tagit emot en stor mängd synpunkter på riktlinjerna. Genom sina synpunkter bidrar industrin och andra intressenter med kunskap, pekar på vilka ytterligare behov som finns och efterlyser förtydliganden. När EDPB tagit ställning till synpunkterna, publicerar man riktlinjerna i slutlig version och då brukar även en svensk översättning komma. Riktlinjerna hänvisar i text och i fotnoter till flera av EDPB:s och föregångaren Artikel 29-gruppens övriga riktlinjer, till exempel de om transparens respektive samtycke. Här finns även referenser till en mängd andra utredningar, artiklar, publikationer från Europeiska unionens cybersäkerhetsbyrå (ENISA, European union agency for network and information security), från medlemsstaternas nationella tillsynsmyndigheter och intresseorganisationer.

I EDPB:s riktlinjer 1/2020 identifieras risker och ges generella rekommendationer om dataskydd och vilka åtgärder rörande säkerhet som bör övervägas av tillverkare av fordon och fordonskomponenter, tjänsteleverantörer och andra som uppträder som personuppgiftsansvariga och personuppgiftsbiträden. Saker som EDPB trycker på är att man bör sträva efter processer som inte inbegriper överföring av personuppgifter utanför fordonet, det vill säga data bör så långt möjligt istället behandlas i fordonet.[82] Se även Utredningen SOU 2018:16 avseende lagringskrav i Tyskland.[83] I Frankrike har dataskyddsmyndigheten tagit fram ett så kallat *compliance package* avseende personuppgiftsbehandling i anslutning till uppkopplade fordon m.m.[84] I det svenska förslaget till ny lag (2019:000) om automatiserad fordonstrafik, 3 kap. 2 § stycke 3, är det däremot ett krav att uppgifterna ska lagras utanför fordonet.[85] EDPB lyfter även frågan om lämplig laglig grund för olika typer av behandling av personuppgifter (GDPR artikel 6 och 9-10). Laglig grund berörs i Utredningen SOU 2018:16.[86]

DI, som är tillsynsmyndighet för frågor om behandling av personuppgifter, pekar i sitt remissyttrande till Utredningen SOU 2018:16 (”DI:s remissyttrande”) på aspekter av samtycke enligt GDPR, bland annat kravet att samtycket måste vara en frivillig viljeyttring och den registrerades rätt att när som helst återkalla samtycket (GDPR artikel 4. 11 och artikel 7 punkt 3), som gör det till en olämplig laglig grund för vissa typer av behandling.[87] DI rekommenderar

[80] SOU 2018:16, s. 728. Proposal (ECE/TRANS/WP.29/2020/79) av den 2 april 2020.
[81] EDPB Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 1.0, 28 January 2020, Adopted – version for public consultation.
[82] EDPB:s Guidelines 1/2020, s. 14, punkt 70 och s. 22 punkt 108.
[83] SOU 2018:16, s. 393.
[84] CNIL, (October 2017), Connected vehicles and personal data, compliance package, s. 11.
[85] SOU 2018:16, s. 98. Datainspektionen, Remiss av slutbetänkandet Vägen till självkörande fordon (SOU 2018:16), DI-2018-3943, s. 9.
[86] SOU 2018:16, avsnitt 13.15 Insamling och lagring av data och Bilaga 6, Axhamn J. *Event data recorders*, Stockholms universitet.
[87] Datainspektionens remiss (DI-2018-3943), s. 11-12.

fortsatt utredning i lagstiftningsärendet av frågan om lämplig laglig grund. DI pekar vidare på oklarheter i förslaget när det gäller fördelning mellan DI och Transportstyrelsen av möjligheten att meddela föreskrifter samt rekommenderar en djupare utredning när det gäller möjligheten och lämpligheten i att utfärda föreskrifter angående säkerhet.[88]

Trafikanalys har tidigare konstaterat att det inte finns någon övergripande nationell lägesbild av risker och åtgärder i transportsektorn och att ansvaret för spridning av information och kunskap är delat mellan MSB, Transportstyrelsen och Trafikverket.[89]

Enligt vår uppfattning är det tänkbart att den lagliga grunden samtycke bör användas för viss behandling, till exempel den som sker inom infotainmentsystem och i fall personuppgifter rörande körbeteende ska lämnas vidare till ett försäkringsbolag för att ge möjlighet till en särskilt låg premie men, när det gäller personuppgiftsbehandling som är nödvändig för att fordonet ska fungera på avsett vis och sådan insamling av personuppgifter i en så kallad svart låda (EDR) som Utredningen SOU 2018:16 föreslår, bör sannolikt en annan laglig grund identifieras. Man kan till exempel tänka sig att behandlingen anses nödvändig för att utföra en uppgift av allmänt intresse (GDPR artikel 6 punkt 1e) eller att den kan ske med stöd av intresseavvägning (GDPR artikel 6 punkt 1 f) men eftersom den registrerade har rätt att invända (GDPR artikel 21) mot behandlingar som sker med stöd av dessa lagliga grunder, finns just anledning att överväga lagstiftning för att kunna stödja delar av behandlingen av personuppgifter på den lagliga grunden rättslig förpliktelse (GDPR artikel 6 punkt 1 c). För att en personuppgiftsansvarig ska kunna luta sig mot grunden rättslig förpliktelse måste det röra sig om en förpliktelse/skyldighet som åvilar den personuppgiftsansvarige (ingen annan) och skyldigheten ska vara fastställd i enlighet med EU-rätten eller den nationella rätt (alltså inte en förpliktelse fastställd i enlighet med lagen i ett tredjeland) som den personuppgiftsansvarige omfattas av (GDPR artikel 6 punkt 3).[90]

Trafikanalys har pekat på behovet av kartläggning av all skyddsvärd information (vilken information som anses skyddsvärd behöver avgöras från fall till fall), inte bara personuppgifter.[91] Enligt vår uppfattning, skulle en komplett dataflödesanalys där aktörer och personuppgiftsbehandlingar identifieras utifrån de behov som i dagsläget finns och kan överblickas, ge värdefull kunskap. Det är därvid inte endast en övergripande illustration av informationsflödena som behövs utan en detaljerad kartläggning och analys steg-för-steg av de inblandade aktörernas respektive behandling av informationen och klassning av informationen som bland annat måste till.

EDPB:s Guidelines 1/2020 lyfter också hur informationskraven enligt GDPR ska tillgodoses, till exempel i förhållande till andra än fordonets ägare som tillfälliga förare och passagerare, liksom hur radering ska möjliggöras när ett förhyrt fordon återlämnas eller vid ägarbyte och EDPB ger förslag på hur dessa saker kan underlättas.[92]

EU-kommissionen, Artikel 29-gruppen och EDPB har konstaterat att införande och användning av ITS-tillämpningar och -tjänster innebär behandling av personuppgifter och att medlemsstaterna måste säkerställa att den behandling av personuppgifter som sker genomförs i enlighet med EU:s regler om skydd av individens grundläggande fri- och

[88] DI:s remissyttrande, s. 6–7.
[89] Trafikanalys rapport (2019:8), s. 80.
[90] Öman, S. (2019) Dataskyddsförordningen *(GDPR) m.m. En kommentar*, Norstedts Juridik AB, Stockholm, s. 158-159.
[91] Trafikanalys rapport (2019:8), s. 83.
[92] EDPB Guidelines 1/2020, s. 10 och 31.

rättigheter och givit ut flera yttranden där det även berörs vilken laglig grund som är lämplig för behandling av personuppgifter inom C-ITS området.[93]

När det gäller tillgång till information om fordon och trafik konstaterar Trafikanalys att den tekniskt sett kan vara mycket god men att tillgången i stor utsträckning avgörs av hur datatillgången regleras. Även i andra rapporter lyfts vikten av att överväga behovet av tvingande lagstiftning för delning av viss information.[94] Vi kan bara instämma i dessa iakttagelser och vill i sammanhanget understryka att förutsättningarna och villkoren för hur den del av information som utgör personuppgifter tillgängliggörs styrs av GDPR, det vill säga det finns en omfattande mängd principer och krav att efterleva och förhålla sig till.

[93] ITS-direktivet, skäl 12 och artikel 10 punkt 1. Kommissionens delegerade förordning (EU) nr 886/2013 av den 15 maj 2013 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller data och förfaranden för kostnadsfritt tillhandahållande, när så är möjligt, av ett minimum av vägsäkerhetsrelaterad universell trafikinformation för användare, skäl 5. WP 252, Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS), adopted on 4 October 2017. SOU 2018:16, Bilaga 6, s. 1151.

[94] Trafikanalys rapport (2019:8), s. 95. WSP Sverige AB (2019) *Styrmedel vid automatisering, analys av hur behovet av transportpolitiska styrmedel påverkas av uppkoppling, samverkan och automatisering*, s. 25.

4.4 Säkerhet och personuppgifter	Resonemang kring de olika frågeställningarna
Trafikanalys frågeställningar 4.4.1 Förares eller passagerares personuppgifter (hälsouppgifter, uppgifter om misstänkt brottslighet) stjäls, eller hanteras på servrar placerade i Sverige, i annat EU-land eller utanför EU. 4..4.2 Hur tillgodoses förarens/ passagerares/ övrig trafikanters rätt att bli raderad? 4.4.3 Vad gäller för fordonets inspelning av sin omgivning? 4.4.4 Vad gäller för informationen i den s.k. svarta lådan (EDR), vem äger, vem har man rätt att dela med sig till, försäkringsbolag? Vi ser följande nyckelord: - bristande säkerhet vid behandling av personuppgifter - geografisk plats för behandling av personuppgifter, överföring av personuppgifter till land utanför EU/EES och adekvat - fordonets inspelning av omgivningen - EDR, den svarta lådan	**4.4.1 Förares eller passagerares personuppgifter (hälsodata, uppgifter om misstänkt brottslighet) stjäls eller hanteras på servrar placerade i Sverige, i annat EU-land eller utanför EU** Uppgifter om att föraren håller på att somna eller information om en förares funktionsnedsättning är exempel på uppgifter som kan kvalificera som hälsouppgifter och ses som känsliga personuppgifter som det enligt GDPR krävs särskilt stöd för att behandla (GDPR artikel 9). Information som bilen registrerar till exempel vid en olycka skulle kunna utgöra uppgifter om misstänkt brottslighet och sådana uppgifter får endast behandlas under kontroll av myndighet eller då behandling är tillåten enligt unionsrätten eller nationell rätt (GDPR artikel 10). Det är inte tillåtet att behandla uppgifter om lagöverträdelser med stöd av samtycke.[95] Frågan om lämplig laglig grund för den behandling av personuppgifter som sker i och i anslutning till ett uppkopplat och automatiserat fordon har diskuterats i flera sammanhang. Eventuellt behov av kompletterande lagstiftning är inte klarlagt.[96] Innan en personuppgiftsansvarig behandlar känsliga personuppgifter i stor omfattning eller personuppgifter som rör fällande domar i brottmål eller lagöverträdelser, krävs att den personuppgiftsansvarige analyserar de risker som behandlingen kan leda till för den registrerades rättigheter och friheter (en riskanalys) och genomför en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter (en konsekvensbedömning) (GDPR artikel 35). I bedömningen ska den personuppgiftsansvariges överväganden och säkerhetsåtgärder när det gäller risker tas med och var servrar är geografiskt placerade bör sannolikt ingå där. Detta bland annat för att man vid en incident och en stöld av personuppgifter ska kunna titta på vilka bedömningar som gjordes innan behandlingen inleddes. När ny lagstiftning på nationell nivå tas fram, skulle där kunna övervägas och eventuellt beslutas att konsekvensbedömningen istället genomförs som ett led i lagstiftningsarbetet och att den personuppgiftsansvarige på så vis befrias från skyldigheten att genomföra en konsekvensbedömning.[97] En stöld av personuppgifter innefattar att konfidentialiteten för uppgifterna bryts. Den som enligt GDPR är personuppgiftsansvarig, men också ett anlitat personuppgiftsbiträde, ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna så att deras konfidentialitet bevaras (GDPR artikel 32.1

[95] Datainspektionens webbplats, Personuppgifter som rör lagöverträdelser. hämtad 24 juni 2020.
[96] SOU 2018:16, Bilaga 6, Axhamn J. *Event data recorders*, Stockholms universitet, s. 1173-1179. Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (Dataskyddslagen). EDPB Guidelines 1/2020, s. 13-14.
[97] DI:s remissyttrande, s. 8-9.

	och b). Det är den som bestämmer ändamål och medel med behandlingen av personuppgifter som är personuppgiftsansvarig. Om ändamål och medel bestäms av flera tillsammans är de gemensamt personuppgiftsansvariga. Den som anlitas för att behandla personuppgifter på den personansvariges vägnar är personuppgiftsbiträde. Den som utfört stölden är givetvis den som primärt bör hållas ansvarig men det ligger i sakens natur att det i många fall är svårt att identifiera denne. Därför kommer fokus att ligga på vem som brustit i sina åligganden eller åtaganden när det gäller säkerheten och konkret hur konfidentialiteten kunnat röjas. Vem som kan hållas ansvarig kommer att avgöras av i vilket moment som någon kommit åt att stjäla personuppgifterna. Tänkbara ansvariga är till exempel fordonstillverkaren, tillverkaren av en komponent, den som tillhandahåller en tjänst eller operatören av infrastrukturen vars tjänst eller produkt uppvisar säkerhetsbrister.[98] Om en aktör vid en oaktsamhetsbedömning befinns inte ha levt upp till kraven i GDPR har föraren och de passagerare för vilkas personuppgifter konfidentialiteten brutits, rätt till ersättning för den materiella och immateriella skada de därigenom lidit (GDPR artikel 82 punkt 1). Den som sprider uppgifter om någon annans hälsotillstånd kan ställas till ansvar för brottet olaga integritetsintrång (brottsbalken (1962:700) 4 kap. 6c §). I DI:s remissyttrande efterlyser myndigheten en grundligare integritetsanalys än den som betänkandet innehåller. Att som utredningen hänvisa till att marknaden kan genomföra den praktiska implementationen av säkerhetsåtgärder och skydd för registrerade anser DI otillräckligt. En analys, skriver DI, kan med fördel gå igenom möjliga upplägg för personuppgiftsbehandlingen så att risker kan konkretiseras och diskuteras på ett icke-abstrakt sätt. Integritetsrisken påverkas, skriver DI, inte bara av uppgifterna i sig, utan även metoderna för insamling, lagring och samkörning av information. Också eventuella oförutsedda och oönskade effekter bör analyseras.[99] Vi konstaterar att det DI efterlyser är en utförlig kartläggning och dataflödesanalys som inbegriper det uppkopplade och automatiserade fordonet och dess interaktion med omgivningen inklusive en komplett riskanalys och konsekvensbedömning. DI betonar även att utrymmet för nationella bestämmelser behöver övervägas utifrån internationell rätt och förslagen analyseras och anpassas utifrån GDPR och kamerabevakningslagen (2018:1200).[100] När det gäller betydelsen av var servrar är placerade, se våra kommentarer om molntjänster under avsnitt 4.3. Genom GDPR anses alla länder inom EU/EES ha en gemensam skyddsnivå och det är vid överföring till länder utanför området, så kallade tredjeländer, som man utöver

[98] EDPB riktlinjer 1/2020, s. 19, punkt 90.
[99] DI:s remissyttrande s. 4-5.
[100] DI:s remissyttrande, s.2.

	lagens övriga krav, även måste säkerställa att adekvat skyddsnivå uppnås. Det är inte alltid möjligt att vid en offentlig upphandling kravställa att IT-drift ska ske från Sverige. Detta ämne reser frågor som kräver närmare utredning.[101] Notera också diskussionen om ett statligt moln, liksom Frankrike och Tysklands utveckling av en gemensam europeisk molninfrastruktur.[102] Vi kan konstatera att oavsett plats, om behandling sker lokalt i fordonet, under överföring, på en fysisk eller virtuell server, inom EU/EES eller i tredje land, kommer risken för att informationen stjäls vara beroende av vilka åtgärder som vidtagits för att skydda personuppgifterna.
	4.4.2 Hur tillgodoses förarens/ passagerares/ övrig trafikants rätt att bli raderad? En förare/passagerare/övrig trafikant ska ha rätt att i egenskap av registrerad, av den personuppgiftsansvarige, få sina personuppgifter raderade, till exempel i det fall personuppgifterna inte längre behövs för de ändamål de har samlats in eller på annat sätt behandlats eller om den registrerade återkallar det samtycke på vilket behandlingen grundar sig (GDPR artikel 17, punkt 1). I EDPB:s riktlinjer 1/2020 lyfts till exempel den registrerades möjlighet att i ett fordon permanent radera personuppgifter inför en försäljning.[103] Radering av personuppgifter ska också kunna begäras hos en återförsäljare eller verkstad.[104] När det gäller hyrbilar, rekommenderar EDPB:s riktlinjer 1/2020 att fordonstillverkaren tillhandahåller funktionalitet, till exempel en raderingsknapp (*delete button*) som möjliggör för den registrerade att enkelt själv radera sina personuppgifter.[105] Rätten till radering är inte absolut och gäller inte under vissa omständigheter. Den registrerade har till exempel inte rätt att radera personuppgifter som behandlas med stöd av den lagliga grunden rättslig förpliktelse. Om en lagenlig skyldighet införs att under 6 månader bevara vissa fordonsuppgifter, kommer den registrerade inte ha möjlighet att få personuppgifter som omfattas av lagringsskyldigheten raderade under den tiden (GDPR artikel 7 punkt 3, artikel 17 punkt 1b).[106] Rätten till radering är en av de rättigheter som GDPR benämner den registrerades rättigheter och som återfinns i GDPR artikel 12-22. Enligt artikel 23 finns möjlighet att i unionsrätten eller i nationell rätt begränsa den registrerades rättigheter och en lagstiftningsåtgärd ska,

[101] Computer Sweden, IDG (2017) *Därför hamnade transportstyrelsens data utanför Sverige*, hämtad
[102] Dir. 2019:64. Computer Sweden IDG (2019) *Första steget mot ett EU-moln är taget – vad händer nu,* hämtad 24 juni 2020. Politico (2020) *Germany, France launch Gaia-X platform in bid for 'tech sovereignty'*, hämtad 24 juni 2020.
[103] EDPB Guidelines 1/2020, s. 16, punkt 74.
[104] EDPB Guidelines 1/2020, s. 16 punkt 75.
[105] EDPB Guidelines 1/2020, s. 31.
[106] SOU 2018:16, s. 32, 49, 97-103 och avsnitt 13.15 Insamling och lagring av data.

	enligt skäl 41, vara tydlig, precis och förutsägbar för de personer som omfattas av bestämmelserna. I DI:s remissyttrande efterlyser myndigheten en mer utförlig analys av förslagens inverkan på den enskildes personliga integritet, däribland hur det kan säkerställas att den registrerade kan utöva sina rättigheter.[107]
	4.4.3 Vad gäller för fordonets inspelning av sin omgivning? I dagens fordon finns backkameror och i ett automatiserat fordon kommer det att finnas flera sorters kameror. En dator analyserar bildmaterialet så att fordonet kan tolka och förstå det. Kamerorna zoomar enligt uppgift inte och de följer inte en enskild människa.[108] Ur ett integritetsperspektiv är det givetvis att föredra att ingen människa kan identifieras eftersom det betyder att det inte rör sig om en behandling av personuppgifter och GDPR därmed inte blir tillämplig. Utredningen SOU 2018:16 lämnar vissa förslag rörande kamerabevakning. Sedan Utredningen publicerade sitt slutbetänkande har en ny kamerabevakningslag trätt i kraft och enligt den måste myndigheter och andra som utför uppgifter av allmänt intresse ansöka om tillstånd för kamerabevakning. Tillstånd krävs dock inte för bevakning som sker för säkerheten i trafiken från ett fordon för att förbättra sikten för föraren eller användaren.[109] Utredningen föreslår en utökning av undantaget från tillståndsplikten. Som DI påpekar i sitt remissyttrande, måste kamerabevakningen dock fortfarande vara förenlig med såväl GDPR som annan tillämplig författning. Det betyder till exempel att de grundläggande principerna enligt GDPR artikel 5 måste följas, det vill säga den vars personuppgifter behandlas måste informeras om behandlingen, principen om uppgiftsminimering och lagringsminimering måste tillämpas. All inspelning som innefattar behandling av personuppgifter måste baseras på en laglig grund och DI kommer att utöva tillsyn över sådan inspelning utifrån de krav och principer som gäller för personuppgiftsbehandling.[110] I sitt remissyttrande framför DI upplysningsvis att samtycke knappast är en lämplig grund för behandling av personuppgifter i samband med automatiserade fordon och anger skälen för sin uppfattning.[111]
	4.4.4 Vad gäller för informationen i den s k svarta lådan (EDR), vem äger, vem har man rätt att dela med sig till? Vad gäller för försäkringsbolag?

[107] DI:s remissyttrande, s. 6-8.
[108] SOU 2018:16, s. 386.
[109] Kamerabevakningslagen (2018:1200) 9 § punkt 9.
[110] DI:s remissyttrande, s. 10.
[111] DI:s remissyttrande, s. 11-12.

	Många fordon har numera en så kallad svart låda, en event data recorder, EDR. EDR är en minnesenhet som löpande sparar information från vissa sensorer i fordonet. Syftet är att fånga upp onormala händelser i fordonet för att möjliggöra analys till exempel vid en olycka. I Sverige idag är det inte obligatoriskt för fordon att ha en svart låda. Inte heller är det reglerat särskilt i lag vem som har tillgång till informationen i en EDR. Polisen kan få tillgång till informationen i en svart låda genom reglerna om beslag (Rättegångsbalken (1942:740), 27 kap.). Informationen i en EDR kan utgöra personuppgifter.[112] Utredningen SOU 2018:16 gör bedömningen att det bör införas en skyldighet för fordon som kan användas för både manuell och automatiserad körning att lagra vissa uppgifter, bland annat fordonets identitet och tidpunkterna för när automatiserad körning aktiveras och inaktiveras och när fordonet begärt att föraren ska överta körningen. Vid en särskild händelse ska fordonets hastighet också lagras. Lagring av uppgifterna föreslås ske under som längst sex månader och sedan ska personuppgifterna i princip utplånas av den lagringsskyldige.[113] Förslaget innebär att fordonstillverkaren (eller importören som tillhandahåller fordonet och likställs med fordonstillverkaren) samtidigt som fordonet registreras i vägtrafikregistret ska söka tillstånd att lagra uppgifter och därmed bli lagringsansvarig och personuppgiftsansvarig.[114] Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om de uppgifter som ska lagras.[115] Utredningen hänvisar även till EU:s arbete med EDR och typgodkännande.[116] Utredningen SOU 2018:16 ger inte svar på Trafikanalys fråga vem som äger informationen som lagras men konstaterar att fordonstillverkaren och fordonsägaren behöver ha tillgång till uppgifterna för att möjliggöra utredning av civilrättsligt ansvar.[117] Här förtydligas dock att fordonstillverkaren inte får använda uppgifterna för exempelvis marknadsföring såvida inte fordonsägaren samtycker till det. Utredningen konstaterar att fordonstillverkaren, för det fall informationen utgör personuppgifter, enligt GDPR har rätt att få tillgång till informationen.[118] Motsvarande rätt gäller som vi ser det, som utgångspunkt enligt GDPR även för andra registrerade. Det kan ju tänkas att fordonet förts av en annan än ägaren eller att en passagerare behöver informationen för ett rättsligt anspråk. Utredningen slår fast att personuppgifterna ska lagras för att utreda ett rättsligt ansvar, såväl i tvistemål som brottmål och att det innebär

[112] SOU 2018:16, avsnitt 8.2.4.
[113] SOU 2018:16, s. 97-103 och 723.
[114] SOU 2018:16, s. 49. Personuppgiftsansvaret framgår av förslag till lag (2019:000) om automatiserad fordonstrafik, 3 kap. 3 §, SOU 2018:16, s. 98.
[115] SOU 2018:16, s. 98.
[116] Förordning (EU) 2019/2144, skäl 13-14 talar om registreringsapparater för händelsedata.
[117] SOU 2018:16, s. 754.
[118] SOU 2018:16, s. 760.

	att uppgifterna ska vara tillgängliga för de personer som kan var part i en rättegång.[119] Den lagringsskyldige ska på begäran lämna uppgifterna till Polismyndighet eller någon annan myndighet som får ingripa mot brottet under förutsättning att det finns misstanke om brott (ansökande myndighet).[120] Utredningen besvarar inte frågan om försäkringsbolag ska ha tillgång till den lagrade informationen. Som vi ser det kan det så klart tänkas att parterna ger sina respektive försäkringsbolag tillgång till informationen. När det gäller tillgång till informationen i den svarta lådan, kan som jämförelse nämnas att det i USA finns en federal lag enligt vilken det i första hand är fordonsägaren alternativt leasingtagaren som har tillgång till informationen i en EDR. Informationen kan bara göras tillgänglig för andra med fordonsägarens samtycke eller efter domstolsbeslut att informationen ska göras tillgänglig i bevissyfte eller i anonymisera form för viss angiven forskning. Även i Tyskland finns bestämmelser om insamling av information och där ska informationen sparas i sex månader i normalfallet och i tre år vid trafikolycka och fordonsägaren är skyldig att tillse att informationen görs tillgänglig för utredning av en trafikolycka. Avidentifierad information får lämnas där ut för forskningsändamål.[121]

[119] SOU 2018:16, s. 759.
[120] SOU 2018:16, s. 100, skyldigheten att lämna ut uppgifter framgår av förslag till lagen om automatiserad fordonstrafik, 3 kap. 14 §.
[121] SOU s. 393-394.

5 Källförteckning

ACEA, Principles of data protection in relation to connected vehicles and services, September 2015, hämtade 3 juli 2020.
https://www.acea.be/uploads/publications/ACEA_Principles_of_Data_Protection.pdf

Arbetsmiljöverkets föreskrifter (AFS2008:3) om maskiner samt allmänna råd om tillämpningen av föreskrifterna.

Armstrong, Gorst & Rae (2019) Renewing Regulation 'Anticipating regulation' in an age of disruption, Nesta foundation, United Kingdom, hämtad 26 juni 2020
https://www.nesta.org.uk/report/renewing-regulation-anticipatory-regulation-in-an-age-of-disruption/

Bernitz, Ulf, Carlsson Mia, Heuman Lars, Leijonhufvud Madeleine, Magnusson Sjöberg Cecilia, Sepiel Peter, Warnling-Nerep Wiweka, Vogel Hans-Heinrich (2017) Finna rätt. Wolters Kluwer Sverige AB, Stockholm.

Brottsbalken (1962:700).

Cirio Advokatbyrå AB (2020) Molntjänster, offentlighet och sekretess i offentlig sektor, Utredning om och förslag till lagstiftning rörande offentlig sektors möjligheter att använda publika molntjänster hämtad 3 juli 2020.

Computer Sweden IDG opinion (2020) Christenson J. m.fl., Molntjänster måste värna Sveriges digitala suveränitet, hämtad 26 juni 2020.
https://computersweden.idg.se/2.2683/1.735762/molnutredningen-digital-suveranitet

Computer Sweden IDG (2017) Därför hamnade transportstyrelsens data utanför Sverige, hämtad 26 juni 2020 https://computersweden.idg.se/2.2683/1.687038/transportstyrelsen-data-utomlands

Computer Sweden IDG (2019) Första steget mot ett EU-moln är taget – vad händer nu, hämtad 24 juni 2020. https://computersweden.idg.se/2.2683/1.726130/forsta-steget-eu-moln

Commission nationale de l'informatique et des libertés (CNIL) (October 2017) Connected vehicles and personal data, compliance package.

Datainspektionen, Remiss av slutbetänkandet Vägen till självkörande fordon (SOU 2018:16).

Datainspektionens webbplats, Personuppgifter som rör lagöverträdelser, hämtad 24 juni 2020.

Dir. 2018:85 Samordnad och accelererad policyutveckling kopplad till den fjärde industriella revolutionens teknologier.

Dir. 2019:64 Säker och kostnadseffektiv it-drift för den offentliga förvaltningen.

DS 1998:43 Myndigheternas föreskrifter, handbok i författningsskrivning.

eSam, Skatteverket och Försäkringskassan (2020) Kommentar till kritisk rapport om molntjänster i offentlig sektor.

EDPB Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 1.0, 28 January 2020, Adopted – version for public consultation.

EU-domstolens avgörande Schrems II (C-311/18).

Europaparlamentets och rådets direktiv 2010/40/EU av den 7 juli 2010 om ett ramverk för införande av intelligenta transportsystem på vägtransportområdet och för gränssnitt mot andra transportslag.

Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

Europaparlamentets och rådets förordning (EU) 2019/2144 av den 27 november 2019 om krav för typgodkännande av motorfordon och deras släpvagnar samt de system, komponenter och separata tekniska enheter som är avsedda för sådana fordon, med avseende på deras allmänna säkerhet och skydd för personer i fordonet och oskyddade trafikanter.

Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Europarlamentets resolution av den 16 februari 2017 med rekommendationer till kommissionen om civilrättsliga bestämmelser om robotteknik (2015/2103/(INL), (2018/C 252/25).

5GAA Press Release 12/07/2019) 5GAA welcomes Council objection against C-ITS Delegated Act, hämtad 24 juni 2020 https://5gaa.org/news/5gaa-welcomes-council-objection-against-c-its-delegated-act/

Fordonsförordningen (2009:2119).

Förordningen (2017:309) om försöksverksamhet med självkörande fordon.

Förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Förordningen (2016:383) om intelligenta transportsystem vid vägtransporter.

Förordningen om vägtrafikregister (2001:650).

Förslag till lag (2019:000) om automatiserad fordonstrafik.

Försäkringskassan (2019) Vitbok Molntjänster i samhällsbärande verksamhet – risker, lämplighet och vägen framåt.

GSMA Europe (2019) Statement on the rejection of the Delegated Act C-ITS, hämtad 24 juni 2020 https://www.gsma.com/gsmaeurope/whats-new/gsma-statement-on-the-rejection-of-the-delegated-act-c-its/

Kamerabevakningslagen (2018:1200).

Kommissionens delegerade förordning (EU) nr 886/2013 av den 15 maj 2013 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller data och förfaranden för kostnadsfritt tillhandahållande, när så är möjligt, av ett minimum av vägsäkerhetsrelaterad universell trafikinformation för användare.

Kommissionens delegerade förordning (EU) C (2019) 1789 final av den 13 mars 2019 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller införande och operativ användning av samverkande intelligenta transportsystem (vilken Europeiska unionens råd (Ministerrådet), invände mot och därmed förhindrade att den trädde i kraft).

Kommissionens Meddelande till Europaparlamentet, rådet, europeiska ekonomiska och sociala kommittén och regionkommittén av den 30 november 2016 om en europeisk strategi för samverkande intelligenta transportsystem, en milstolpe mot samverkande, uppkopplad, automatiserad rörlighet, COM (2016) 766 final.

Kommissionens Meddelande till Europaparlamentet, rådet, europeiska ekonomiska och sociala kommittén och regionkommittén av den 17 maj 2018 om vägen mot automatiserad rörlighet – en EU-strategi för framtidens rörlighet, COM (2018) 283 final.

Konsumenttjänstlagen (1985:716).

Myndigheten för samhällsskydd och beredskap (MSB) (2019) Metodstöd för systematiskt informationssäkerhetsarbete - En översikt.

MSBF (2020:06) föreskrifter om informationssäkerhet för statliga myndigheter.

MSBFS (2018:7) föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster.

MSBFS (2020:6) föreskrifter om informationssäkerhet för statliga myndigheter.

National Highway Traffic Safety Administration riktlinjer hämtade 1 juli 2020 https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

NJA 1969 s. 220.

Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (Dataskyddslagen).

Lagen (2013: 315) om intelligenta transportsystem vid vägtransporter.

Oberoende expertgrupp på hög nivå för AI-frågor inrättad av Europeiska kommissionen i juni 2018, Etiska riktlinjer för tillförlitlig AI, 8 april 2019, hämtade 1 juli 2020 https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

Politico (2020) Germany, France launch Gaia-X platform in bid for 'tech sovereignty', hämtad 24 juni 2020 https://www.politico.eu/article/germany-france-gaia-x-cloud-platform-eu-tech-sovereignty/

Produktansvarslagen (1992:18).

Regeringskansliet (Diarienummer N2017/03643/D), För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi.

Rättegångsbalken (1942:740).

Schultz, Mårten Sveriges största juridikblogg, Modern skadeståndsrätt för dummies, 27 juni 2009, hämtad 26 juni 2020.

Skadeståndslagen (1972:207).

SOU 2018:16, Vägen till självkörande fordon – introduktion, Slutbetänkande.

Säkerhetsskyddslagen (2018:585).

Trafikanalys (Rapport 2019:8).

Lagen (1951:649) om straff för visa trafikbrott, (Trafikbrottslagen).

Trafikförordningen (1998:1276).

Trafikverket (2017) Digitaliseringens möjligheter, PM till Nationell plan för transportsystemet 2018–2029.

Twitter, Schultz Mårten, 7 juni 2017 som hänvisar till inlägg på Sveriges största juridikblogg, Modern skadeståndsrätt för dummies, 27 juni 2009), hämtad 26 juni 2020, https://twitter.com/martenschultz/status/1004724750768377862

Tyskland, Etikkommission, juni 2017 riktlinjer hämtade 1 juli 2020. https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2017/06/084-dobrindt-bericht-derethik-kommission.pdf

United Nations, Economic and Social Council, Economic Commission for Europe, Proposal (ECE/TRANS/WP.29/2020/79) Revised. for a new UN Regulation on uniform provisions concerning the approval of vehicles with regard to cyber security and cyber security management system, antogs den 24 juni 2020.

United Nations, Economic and Social Council, Economic Commission for Europe, Proposal) ECE/TRANS/WP.29/2020/80) for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to software update and software updates management system, antogs den 24 juni 2020.

Wendleby, M. (2020), Livet efter Schrems II – kommer vi att kunna överföra personuppgifter till USA?, Passacon AB, JP Juridiskt bibliotek, JP Infonet, hämtad 23 september 2020 https://www.jpinfonet.se/kunskap/nyheter4/livet-efter-schrems-ii--kommer-vi-kunna-overfora-personuppgifter-till-usa/

Wennström, Bo, Rättens nya landskap. Working Paper 2010:4, Juridiska fakulteten, Uppsala universitet.

WP 252, Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS), adopted on 4 October 2017.

WSP Sverige AB (2019) Styrmedel vid automatisering, analys av hur behovet av transportpolitiska styrmedel påverkas av uppkoppling, samverkan och automatisering.

Åklagarmyndigheten, Yttrande över remissen ”Vägen till självkörande fordon – introduktion”, SOU 2018:16.

Öman, Sören (2019) Dataskyddsförordningen (GDPR) m.m. En kommentar, Norstedts Juridik AB, Stockholm.