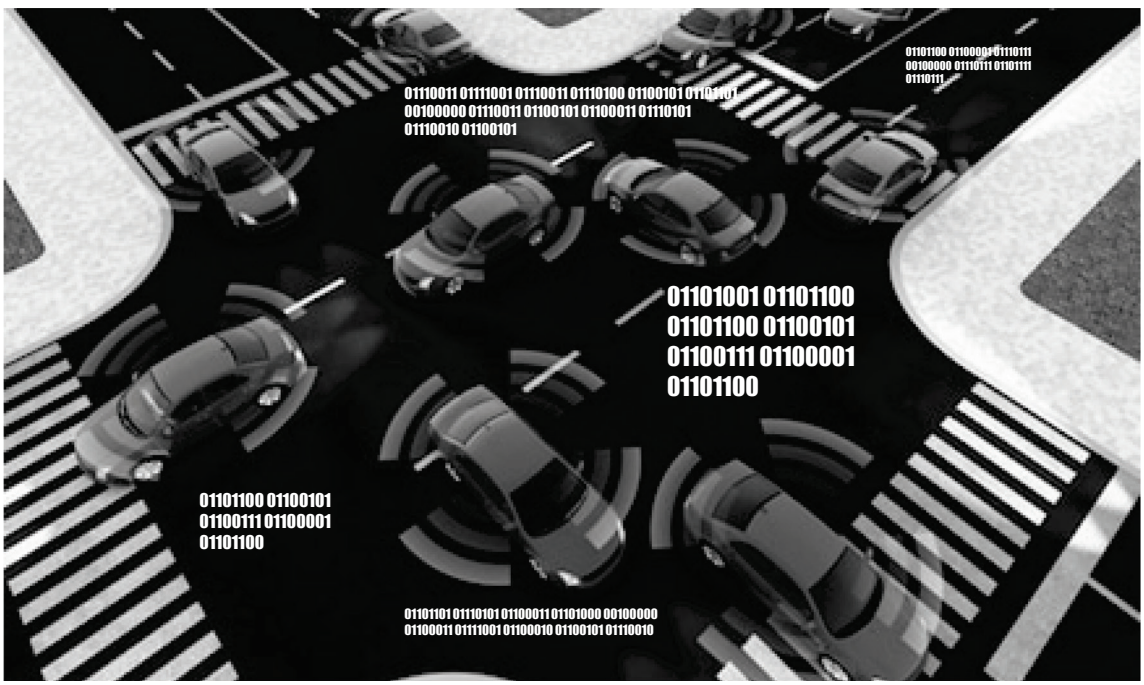
Lag och cybersäkerhet i smart vägtrafik

ERIK ZOUAVE, SABRINE WENNBERG, MARGARITA JAITNER



FOI-R--4811--SE
ISSN 1650-1942 December 2019

Erik Zouave, Sabrine Wennberg, Margarita Jaitner

Lag och cybersäkerhet i smart vägtrafik

Titel	Lag och cybersäkerhet i smart vägtrafik
Title	Cyber security regulation for smart traffic
Rapportnr	FOI-R--4811--SE
Månad	December
Utgivningsår	2019
Antal sidor	99
ISSN	1650-1942
Kund	Myndigheten för samhällsskydd och beredskap
Forskningsområde	Informationssäkerhet
FoT-område	Inget FoT-område
Projektnr	E13679
Godkänd av	Lars Höstbeck
Ansvarig avdelning	Försvarsanalys

Bild: Shutterstock/Karsten Neglia, Erik Zouave

Sammanfattning

Automatisering i trafiken är en trend som har fått fart under de senare åren och troligtvis kommer att ha en stor inverkan på vårt samhälle. Trenden bär med sig förändringar, anpassningar och nya utmaningar för vägtrafiken. Den framskridande automatiseringen av fordon innebär både en allt svårare överskådlig komplexitet, men även att teknologin ytterst kommer att direkt påverka människans liv och hälsa. Detta sätter i sin tur frågan om cybersäkerheten, och dess reglering i nytt fokus. Denna studie har kartlagt ett flertal lagrum och bestämmelser som är relevanta för cybersäkerheten i uppkopplade, automatiserade fordon. Lagrummen identifierades utifrån tidigare utredningar om lagstiftning och reglering. Följande lagrum låg i fokus för studien: civilrätten för smart robotteknik, dataskyddsbestämmelser, nätverks- och informationssäkerhet i samhällsviktig verksamhet (NIS), säkerhetsskyddsbestämmelser, förslag om IKT-standardiseringsbestämmelser, bestämmelser om intelligenta transportsystem (ITS & och C-ITS), produktansvars- och produkt-prövningsbestämmelser, fordonskontrollsbestämmelser samt försäkrings-bestämmelser. Cybersäkerhetsregleringen för transportsektorn i sin helhet utgörs av en fragmenterad och komplex lagstiftning. Olika lagrum fyller olika syften, med krav som ofta riktas till olika typer av aktörer och verksamhet. Medan det inte finns harmoniserade cybersäkerhetskrav mellan olika lagrum finns det ett antal åtgärder som är återkommande. Dessa innefattar att anmäla verksamhet till behöriga myndigheter, bedöma risker och vidta säkerhetsåtgärder, samt rapportera säkerhetsincidenter.

Nyckelord: smart vägtrafik, smarta fordon, smarta vägnät, intelligenta transportsystem, automatisering, självkörande fordon

Summary

Autonomous vehicles are a trend that has gained momentum in recent years and is likely to have a major impact on our society. This trend presents new challenges for road traffic. The progressive automation of vehicles entails both increasing complexity, but also that technology will ultimately have a direct impact on human life and health. This, in turn, puts the issue of cyber security and its regulation into sharp focus. This study maps a number of legislation and regulations that are relevant to cyber security in connected, automated vehicles. The legislations were identified on the basis of previous investigations into legislation and regulation. The following areas were the main focus of the study: the civil law for robotics, data protection regulations, network and information security regulations (NIS), protective security regulations, proposals for cyber security act, regulations on intelligent transport systems and cooperative intelligent transport systems (ITS and C-ITS), product liability and motor vehicle type approvals, vehicle inspection regulations and insurance regulations. The cyber security regulation as a whole consists of fragmented and complex laws. Different legal regimes fulfil different purposes, with requirements addressed to varying actors and activities. While there are no harmonized security requirements between different regimes, some security measures are recurrent. These measures include reporting activities to competent authorities, assessing risks and taking security measures, as well as notifying of security incidents.

Keywords: smart traffic, smart cars, intelligent transport systems, autonomous vehicles, automation

Innehållsförteckning

Förkortningar

EU	Europeiska Unionen
CEN	Europeiska standardiseringskommittén
CENELEC	Europeiska kommittén för elektronisk standardisering
CERT/CSIRT	Computer Emergency Response Team/Computer Security Incident Response Team, incidenthanteringsorganisationer inom informationssäkerhet
(C-)ITS	(Cooperative) Intelligent Transport Systems
CSMS	Cyber Security Management Systems
DDoS	Distributed Denial of Service attack
ECE	United Nations Economic Commission for Europes
Enisa	Europeiska unionens byrå för nät- och informationssäkerhet
FN	Förenta Nationerna
GDPR	Europeiska unionens allmänna dataskyddsförordning
GRVA	FN-arbetsgruppen för automatiserade/autonoma och uppkopplade fordon
IKT	Informations- och kommunikationsteknologi
ISA	Intelligent Speed Assistance
ISO	Internationella standardiseringsorganisationen
ITS	Intelligenta Transport System
MSB	Myndigheten för samhällsskydd och beredskap
NCS3	Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet
PKI	Public Key Infrastructure
SWEDAC	Styrelsen för ackreditering och teknisk kontroll
TRAFA	Trafikanalys
UNECE	FN:s ekonomiska kommission för Europa

1 Introduktion

Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett samarbete mellan Totalförsvarets forskningsinstitut (FOI) och Myndigheten för samhällsskydd och beredskap (MSB). Samarbetet syftar till att öka nationell kunskap om cybersäkerhet i industriella informations- och styrsystem. Enligt ”Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022” ska MSB ”arbeta med medvetandehöjande insatser och stärka det förebyggande arbetet rörande IT-säkerhet under uppbyggnaden av de nya intelligenta transportsystemen” tillsammans med FOI. En väsentlig del av arbetet med IT-säkerheten inbegriper efterlevnad av rättsliga bestämmelser om cybersäkerhet. Denna rapport är en övergripande kartläggning av bestämmelser som reglerar cybersäkerheten i smarta fordon och vägnät. Rapporten ger även en överblick av det relaterade arbetet.

Cybersäkerhetslagstiftning för uppkopplade och autonoma fordon är ett ämne som diskuteras allt mer, i Sverige liksom globalt. Beslutsfattare och industri lägger ökad vikt vid cybersäkerhet inom uppkopplade fordon och vid att det ska finnas fullvärdig lagstiftning och reglering. Följderna av uppkopplade fordons sårbarhet har på kort tid haft betydande konsekvenser för fordonsindustrin. Över 3,5 miljoner bilar har fått återkallas när de kunnat utsättas för dataintrång och obehöriga kunnat manipulera fordonens system till den mån att de inte längre varit körbara, eller till och med har styrts på distans av obehöriga.[1] Enisa (Europeiska unionens byrå för nät- och informationssäkerhet) uppskattar att så många som 100 miljoner bilar kan påvisa cybersäkerhetsbrister.[2] Farhågan med tekniskt sårbara fordon har även fått en större internationell profil i och med försök att utveckla självkörande fordon, som till högre grad är beroende av tekniska system för drift. Enligt Europeiska kommissionen kan självkörande fordon vara kommersiellt tillgängliga redan 2020, och

[1] ENISA. *Cyber Security and Resilience of smart cars.* 2017. Från: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars/at_download/fullReport Senast 01/10/2019; O’Donnell. *Chris Valasek and Charlie Miller: How to Secure Autonomous Vehicles.* Threat Post 2018. Från: https://threatpost.com/chris-valasek-and-charlie-miller-how-to-secure-autonomous-vehicles/134937/ Senast 01/10/2019; Rosdahl. *Car Hacks 101 – an overview of noticed automotive (in)security cases 2010-2016.* 2017. Från: https://www.knowit.se/contentassets/ec982080c156461a9582b7bfc8858850/anders-rosdahl---car-hacks-101.pdf Senast 01/10/2019.

[2] ENISA. *Cyber Security and Resilience of smart cars.* 2017. Från: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars/at_download/fullReport Senast 01/10/2019.

det är troligt att dessa fordon kan vara vanligt förekommande på den kommersiella marknaden före 2030. Även i Sverige, har man genom utredningen *SOU 2018:16 Vägen till självkörande fordon*[3] uppmärksammat farhågan med sårbarheter i självkörande fordon. Återkommande diskuteras risker kring automatiserade fordon, men det är viktigt att ha i åtanke att även fordon som assisterar föraren eller är uppkopplade genom tekniska system är sårbara. Kommissionen förmodar att alla nyproducerade bilar förväntas vara mer eller mindre internetuppkopplade 2022. Fram till dess bör medlemsstaterna hantera cybersäkerhet, produktsäkerhets-, och andra säkerhetsaspekter som påverkar allmän tillit för uppkopplade, smarta och självkörande fordon.[4] Trots att riskerna stundvis uppmärksammats på relativt hög policynivå, exempelvis bland lagstiftare, saknas i dagsläget en överblick över vilka bestämmelser som gäller för smarta fordon och vägnät.

1.1 Syfte

Denna studie kartlägger vilka av de rättsliga principer och regler som utvecklas för cybersäkerhet, som ska tillämpas på smarta fordon och vägnät, samt vilka aktörer som kan komma att beröras och hur. Studien omfattar även en kartläggning av utvecklingen av standarder och vägledningar för cybersäkerhet i smart vägtrafik. Kartläggningen i denna rapport ska höja medvetenheten om bestämmelserna hos berörda aktörer såsom behöriga myndigheter, fordonsindustrin, och industrins underleverantörer, samt att den bidrar med en översikt för dessa aktörers jurister, it- och säkerhetsansvariga, samt beslutsfattare.

Det finns ingen harmoniserad definition för cybersäkerhet som gäller samtliga (eller ens flera) lagrum. Således hanterar rapporten bestämmelser som utformats ur många olika säkerhetsperspektiv, såsom nationell säkerhet, informations- och nätverkssäkerhet, integritet och privatliv med mera. Det är snarare bestämmelsernas tillämpning på tekniska system som i denna rapport avser cybersäkerhet. I denna studie innebär smart vägtrafik informations- och kommunikationsteknologi som

[3] Regeringen. *SOU 2018:16. Vägen till självkörande fordon*. Stockholm. 2018.

[4] Regeringen. *SOU 2018:16. Vägen till självkörande fordon – introduktion. Del 1. Slutbetänkande av utredningen om självkörande fordon på väg.* Stockholm. 2018.; Regeringen. *Skr. 2016/17:213. Nationell strategi för samhällets informations- och cybersäkerhet.* 2017.; Regeringskansliet. *Nationell inriktning för artificiell intelligens.* 2018; Europeiska Kommissionen. *COM (2018) 283 final. On the road to automated moility: An EU strategy for mobility of the future.* 2018. Från: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0283 Senast 01/10/2019.

tillämpas på vägtransport och innefattar främst infrastruktur, fordon och användare. Denna definition är vald på grund av att den är bred nog att omfatta såväl svenska som europeiska synsätt och begreppsapparater för smarta fordon och intelligenta transportsystem.[5] Studien har en bred syn på smarthet som omfattar allt ifrån uppkopplade system till artificiellt intelligenta och autonoma system.[6]

Målet är att tydliggöra vilka aktörer som kan beröras av cybersäkerhetskrav i smart vägtrafik, och är främst inriktat mot svenska myndigheter och företag. Studien bygger på fem frågor:

1. Vilka är de relevanta lagrummen, standarderna och vägledningarna avseende cybersäkerhet i smart vägtrafik?
2. Vilka säkerhetsprinciper och bestämmelser finns för smarta fordon och vägnät?
3. Vilka aktörer berörs av bestämmelserna och deras utveckling?
4. Hur bör eventuell framtida lagstiftning och vägledningar tillämpas organisatoriskt på nationell nivå i Sverige enligt de berörda aktörerna?
5. Finns det behov av kompletterande bestämmelser om cybersäkerhet för smarta fordon och vägnät?

Fråga ett till fyra besvaras i del två av denna rapport. Medan regleringen av standardisering och vägledning också behandlas i del två och organisationen bakom standardisering redovisas i del tre, redovisas identifierade standarder och vägledningar i bilagorna till rapporten. Fråga fyra till fem behandlas i del fyra av rapporten.

1.2 Metod

Studien är i skrivande stund den första av sitt slag. Författarna har inte identifierat någon tidigare, sammanhållen bild av vilka lagrum som påverkas eller påverkar utvecklingen av cybersäkerhetsnormer i en alltmer digitaliserad transportsektor, vare sig i Sverige eller inom

[5] Se Vägen till självkörande fordon - introduktion: Slutbetänkande av Utredningen om självkörande fordon på väg. SOU 2018:16; 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 Text av betydelse för EES. EUT L 207, 6.8.2010, s. 1–13; ENISA. (2005-2019). *Smart transport.* Från: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/smart-transport. Senast 15/04/2019.

[6] Vägen till självkörande fordon - introduktion: Slutbetänkande av Utredningen om självkörande fordon på väg. SOU 2018:16; ENISA. (2005-2019). *Smart transport*. Från: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/smart-transport. Senast 15/04/2019.

Europeiska unionen (EU). För att identifiera de relevanta bestämmelserna används litteraturstudier, granskning av rättsliga källor (EU-förordningar, EU-direktiv, nationella lagar, föreskrifter, rättsliga vägledningar med mera) samt studier av standarder och vägledningar. Litteraturgenomgången av tidigare forskning identifierar de relevanta lagrummen. Denna del av studien inbegriper både akademisk litteratur och rapportering från nationella och internationella organisationer som är verksamma inom ämnesområdena smart vägtrafik och cybersäkerhet. Granskningen av rättsliga källor, standarder och vägledningar identifierar säkerhetsprinciper, bestämmelser och åtgärder som fastställts eller utvecklas för cybersäkerhet i smart vägtrafik.

Därutöver hölls en workshop i syfte att klargöra hur reglering bör implementeras och vilka eventuella behov av kompletterande regler som skulle kunna uppstå. Workshopen samlade företrädare från behöriga myndigheter och industrin med erfarenhet av rättslig tillämpning, erfarenhet av det internationella regleringsarbetet, eller erfarenhet av standardiseringsarbetet.

1.3 Avgränsningar

Studien avgränsar inte kartläggningen av lagar utifrån någon särskild definition av (cyber)säkerhet. Snarare identifieras lagar med bestämmelser som ska tillämpas på de tekniska systemen som utvecklas eller tas i bruk inom transportsektorn. Såvida litteraturen inte specifikt pekar ut behov av att uppdatera något äldre lagrum, avgränsar sig studien till den rättsliga utvecklingen de senaste tio åren och de förslag som för närvarande ligger hos lagstiftande instanser. Ett exempel på äldre lagrum där arbete med uppdateringar mot cybersäkerhet pågår, är bestämmelser om produktansvar för fordon och särskilt typgodkännande av fordon. I vissa fall kan det alltså vara nödvändigt att inte bara kartlägga bestämmelserna i de nyare delarna av (eller nya förslag inom) lagrummet, utan även observera utvecklingen som lett dit. Studien är också avgränsad till transportsystemen i sig och går därför inte in på cybersäkerhets-bestämmelser för interoperabla system eller andra teknologier som vägtransporten är beroende av, exempelvis cybersäkerhet i satellit-kommunikation. Studien omfattar inte heller speciallagar för kris och krig.

2 Lag och cybersäkerhet i smart vägtrafik

Bristen på tidigare utredningar och förstahandskällor är särskilt tydlig i fråga om rättstillämpning och utvecklingen av nya lagar. December 2016 uppmärksammade Enisa behovet av att klargöra rättsligt ansvar för cybersäkerhet i fordon.[7] Rekommendationen riktade sig främst till fordonsindustrin utan att föreslå vilka typer av ansvar (vilka lagrum) som särskilt bör utredas. Under 2018 färdigställde Statens offentliga utredningar *Slutbetänkande av Utredningen om självkörande fordon på väg (SoU 2018:16)*. Medan slutbetänkandet uppmärksammade viktiga aspekter som fordons beskaffenhet och utrustning samt teknisk kompetens, kvalitetssäkring och certifiering vid besiktning, uppmärksammades inga utpräglade krav angående cybersäkerhet.[8] Internationellt har forskare som utrett rättsliga aspekter av cybersäkerhet i smart vägtrafik ofta fastnat i att utredda det relaterade och mer utvecklade arbetet med standarder och vägledningar snarare än faktisk lag.[9]

Trots detta finns det relevant lag och policy på området. För en studie som kartlägger smart teknologi är Europeiska parlamentets resolution om civilrättsliga aspekter av (smart) robotteknik en betydande källa. Resolutionen har hittills förbisetts i studier om cybersäkerhet i smart vägtrafik, detta trots att den lägger fram förslag avseende både säkerhet i intelligenta system och autonoma transportmedel.[10] Flera studier har uppmärksammat det så kallade NIS-direktivets tillämpning på området,

[7] Enisa (2016) Cyber Security and Resilience of smart cars Good practices and recommendations. doi: 10.2824/87614

[8] Vägen till självkörande fordon - introduktion: Slutbetänkande av Utredningen om självkörande fordon på väg. SOU 2018:16

[9] Mark Schaub. (2018). *Cybersecurity: Achilles' Heel for Self-driving Cars?* Från: https://www.lexology.com/library/detail.aspx?g=516d38b3-df85-4293-871a-bb461c572769. Senast 15/04/2019; European Automobile Manufacturers Association. (2017). *ACEA Principles of Automobile Cybersecurity.* Från: https://www.acea.be/uploads/publications/ACEA_Principles_of_Automobile_Cybersecurity.pdf. Senast 15/04/2019; ENISA (2016) Cyber Security and Resilience of smart cars Good practices and recommendations. doi: 10.2824/87614

[10] Europaparlamentets resolution av den 16 februari 2017 med rekommendationer till kommissionen om civilrättsliga bestämmelser om robotteknik (2015/2103(INL))

inte minst då direktivet omfattar krav på nätverks- och informationssäkerhet i samhällsviktig verksamhet.[11] Ett antal forskare har dessutom kopplat cybersäkerhetsproblematiken till dataskyddet.[12] När Enisa skriver om cybersäkerhet och resiliens avseende smarta fordon innefattar studien även intelligenta transportsystem som regleras särskilt i den europeiska unionsrätten.[13] Trafikverket tar också upp de svenska reformerna med anledning av den nya säkerhetsskyddslagen (2018:585) i sin omvärldsanalys över trender i transportsystemet.[14] En av de mer omfattande publikationerna på området är Channon et al.[15] som behandlar lagar kring provning, försäkring, produktansvar,[16] cybersäkerhet och dataskydd ur ett internationellt perspektiv. Frågeställningar kring provningsbestämmelser, produktionsbestämmelser och typgodkännande sammanfaller vanligen inom gällande United Nations Economic Commission for Europes (ECE) föreskrifter. Dessa föreskrifter reglerar säkerhetsaspekter inom respektive processer.[17] En reform som behandlas i SoU 2018:16 men som inte

[11] Liveri Dimitra. (2018). Enhancing automotive cybersecurity in Europe. (OECD Workshop on Digital Security and Resilience in Critical Infrastructure and Essential Services |16.02.18, Paris) Från: https://www.oecd.org/going-digital/digital-security-in-critical-infrastructure/digital-security-workshop-february-2018-Liveri.pdf. Senast 15/04/2019; European Automobile Manufacturers Association. (2017). *ACEA Principles of Automobile Cybersecurity.* Från: https://www.acea.be/uploads/publications/ACEA_Principles_of_Automobile_Cybersecurity.pdf. Senast 15/04/2019; Vägen till självkörande fordon - introduktion: Slutbetänkande av Utredningen om självkörande fordon på väg. SOU 2018:16; Matthew Channon, Lucy McCormick, och Kyriaki Noussia (2019). The Law and Autonomous Vehicles. Oxon: Routledge. Kap 5; Trafikverket. (2018). *Trender i transportsystemet: Trafikverkets omvärldsanalys 2018.* Från: https://trafikverket.ineko.se/Files/en-US/51419/Ineko.Product.RelatedFiles/2018_180_trender_i_transportsystemet_trafikverkets_omv%C3%A4rldsanalys_2018.pdf. Senast 16/04/2019.

[12] ENISA (2016) Cyber Security and Resilience of smart cars Good practices and recommendations. doi: 10.2824/87614; European Automobile Manufacturers Association. (2017). *ACEA Principles of Automobile Cybersecurity.* Från: https://www.acea.be/uploads/publications/ACEA_Principles_of_Automobile_Cybersecurity.pdf. Senast 15/04/2019; Vägen till självkörande fordon - introduktion: Slutbetänkande av Utredningen om självkörande fordon på väg. SOU 2018:16

[13] ENISA (2016) Cyber Security and Resilience of smart cars Good practices and recommendations. doi: 10.2824/87614

[14] Trafikverket. (2018). *Trender i transportsystemet: Trafikverkets omvärldsanalys 2018.* Från: https://trafikverket.ineko.se/Files/en-US/51419/Ineko.Product.RelatedFiles/2018_180_trender_i_transportsystemet_trafikverkets_omv%C3%A4rldsanalys_2018.pdf. Senast 16/04/2019.

[15] Matthew Channon, Lucy McCormick, och Kyriaki Noussia (2019). The Law and Autonomous Vehicles. Oxon: Routledge

[16] För frågor kring produktansvar, se även Vägen till självkörande fordon - introduktion: Slutbetänkande av Utredningen om självkörande fordon på väg. SOU 2018:16

[17] Se exemplevis Föreskrifter nr 79 från Förenta nationernas ekonomiska kommission för Europa (FN/ECE) – Enhetliga bestämmelser om godkännande av fordon med avseende på styrutrustning. *EUT L 137, 27.5.2008, s. 25–51*

förekommer i existerande litteratur om cybersäkerhet är kontroll-besiktning.[18] I dagsläget är det oklart vilken betydelse kontrollbesiktningar kan få för cybersäkerhet i fordon, men det är ändå väsentligt att ta upp i denna rapport eftersom lagrummet reglerar fordonens och utrustningens beskaffenhet.

Dessa studier har i regel inte försökt klarlägga hur lagrummens säkerhets-principer och bestämmelser kan komma att tillämpas på smart vägtrafik. De möjliggör inte heller någon analys över hur utvecklingen av teknologi eller lagstiftning samspelar och påverkar varandra. Nedan förtydligas för vilka syften de olika lagrummen utformat säkerhetsprinciper och säkerhetskrav, till vilken mån lagen omfattar smart vägtrafik (fordon respektive transportsystem), samt redogör för de olika säkerhetsprinciper och säkerhetskrav som finns i respektive lagrum.

2.1 Robotteknik

I början på 2017 antog Europaparlamentet en resolution om civilrättsliga bestämmelser för (smart) robotteknik, inklusive smarta transportmedel.[19] Resolutionen är inte bindande för unionens medlemsstater, men den ger rekommendationer till kommissionen om vilka steg den bör ta i sitt regleringsarbete och pekar alltså ut en väg framåt för fortsatt reglering.

Resolutionens fokus på ansvar och skadeståndsansvar är en början på en tilltagande framtida reglering av smart robotteknik. Det finns flera anledningar till varför säkerhet och cybersäkerhet bör behandlas som en del av den framtida civilrättsliga regleringen av robotteknik, inklusive smarta fordon. Dessa inkluderar:

- mänskliga fri- och rättigheter (särskilt dataskydd och privatliv)
- sociala frågor
- folkhälsa
- industrifrågor
- konsumentskydd
- transportsäkerhet.[20]

[18] Vägen till självkörande fordon - introduktion: Slutbetänkande av Utredningen om självkörande fordon på väg. SOU 2018:16

[19] Europaparlamentets resolution av den 16 februari 2017 med rekommendationer till kommissionen om civilrättsliga bestämmelser om robotteknik (2015/2103(INL)), ingress;

[20] Europaparlamentets resolution av den 16 februari 2017 med rekommendationer till kommissionen om civilrättsliga bestämmelser om robotteknik (2015/2103(INL)), ingress; Betänkande (27.1.2017) med rekommendationer till kommissionen om civilrättsliga bestämmelser om robotteknik (2015/2103(INL)), se yttranden;

Ett särskilt mål med att reglera cybersäkerhet i smarta fordon på unionsnivå är att undvika en splittrad ansats bland medlemsstaterna.[21] En enhetlig reglering borde både ge säkrare fordon men också skapa en förutsägbarhet för de industriaktörer som ska utveckla systemen och i gränsöverskridande frågor om körning, försäkring, personuppgiftsbehandling etc.

I och med att resolutionens definition av smart robotteknik omfattar självkörande bilar är även dess säkerhetsrelaterade avsnitt relevanta för den framtida utvecklingen av regler och standarder. Även om resolutionen inte explicit behandlar cybersäkerhet, behandlar den koncept som tillförlitlighet och integritet, bland annat genom standardisering, etisk uppförandekod och licensiering.

Eftersom resolutionen inte är bindande för medlemsstaterna avgörs inte sakfrågor om cybersäkerhetsbestämmelser av resolutionen i sig. Den direkta effekten för cybersäkerhet i autonoma fordon verkställs först genom kommande ändringar och utveckling inom separata men relaterade lagrum som reglerar fordonen utifrån resolutionens inriktning. Det är även troligt att expertgrupper och myndigheter med mandat att utforma föreskrifter, allmänna råd och andra former av vägledningar kommer att inspireras av resolutionens innehåll. På EU-nivå finns redan expertgrupper som arbetar utifrån liknande principer, inte minst kring artificiell intelligens och etik.[22] I och med resolutionen (och en rad andra initiativ) överväger även Europeiska kommissionen att inrätta en ny myndighet för robotteknik och artificiell intelligens. Myndigheten skulle stödja medlemsstaterna med teknisk, etisk och rättslig expertis för att bättre bemöta möjligheter och utmaningar med utvecklingen. Transportsektorns gränsöverskridande karaktär kommer förmodligen göra den sektorn till ett huvudtema för en sådan myndighet.[23] Det är även möjligt att ett sådant initiativ till ny myndighet kan komma att återspeglas på nationell nivå i vissa medlemsstater givet den strategiska betydelsen av teknisk utveckling inom robotteknik och artificiell intelligens för medlemsstaternas ekonomi, säkerhet etc.

[21] Europaparlamentets resolution av den 16 februari 2017 med rekommendationer till kommissionen om civilrättsliga bestämmelser om robotteknik (2015/2103(INL)), autonoma transportmedel

[22] Europeiska kommissionen. (2019). *Ethics guidelines for trustworthy AI.* Från: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. Senast 01/10/2019; Europeiska kommissionen. (2019). *High-Level Expert Group on Artificial Intelligence.* Från: https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence. Senast 01/10/2019.

[23] Europaparlamentets resolution av den 16 februari 2017 med rekommendationer till kommissionen om civilrättsliga bestämmelser om robotteknik (2015/2103(INL)), 2, 16, samt Annex med rekommendationer

2.1.1 Smarta fordon inom smart robotteknik

Resolutionen ger både en övergripande definition av vad en smart robot är och av robotteknikens förhållande till autonoma transportmedel generellt, och självkörande fordon i synnerhet.

En smart robot är ett fysiskt system med ett antal kännetecken enligt resolutionen. Systemet kan inhämta information genom sensorer eller uppkoppling till nätverk. Systemet kan dessutom lära sig av information om sina interaktioner och erfarenheter. Systemet anpassar sitt beteende efter omgivningen och uppnår autonomi genom informations-behandlingen.[24]

Autonoma transporter omfattar automatiserade, uppkopplade och autonoma transportmedel på land, sjö och i luftrummet. Samtidigt som resolutionens säkerhetsrelaterade principer, krav och rekommendationer skulle kunna omfatta transportområdet i stort, identifierarar resolutionen självkörande fordon som ett område med akut behov av reglering.

2.1.2 Cybersäkerhet för smarta fordon och vägnät

Cybersäkerhetsaspekterna i resolutionen inbegriper inte bara de själv-körande fordonen i sig utan också infrastrukturen som fordon kommunicerar med. Det fria flödet av uppgifter och skyddet av nätverk ses som instrumentellt för framgångsrik tillämpning av robotteknik. Resolutionen riktar sig i synnerhet till forskare, konstruktörer och användare men utan att definiera dessa eller förhållandet mellan dessa aktörer.

Resolutionen påkallar särskilt reglering och investeringar som främjar effektiv, tillförlitlig, integritetskyddande och tät kommunikation och informationsdelning för fordonen via informations- och tele-kommunikationsinfrastruktur. Kommissionen och medlemsstaterna bör, enligt resolutionen, harmonisera sina civilrättsliga bestämmelser för robottekniken mot det europeiska dataskyddet, särskilt ”inbyggt integritetsskydd och integritetsskydd som standard, uppgiftsminimering, ändamålsbegränsning samt insynsvänliga kontrollmekanismer”.[25] Dessutom understryks behovet av tillförlitlig tids- och positionerings-information, exempelvis via satellitkommunikation.

[24] Ett ytterligare krav är att system ska ha avsaknad av liv i biologisk bemärkelse. Se Europaparlamentets resolution av den 16 februari 2017 med rekommendationer till kommissionen om civilrättsliga bestämmelser om robotteknik (2015/2103(INL)),stycke 1 i allmänna principer.

[25] Europaparlamentets resolution av den 16 februari 2017 med rekommendationer till kommissionen om civilrättsliga bestämmelser om robotteknik (2015/2103(INL))

Inom forsknings- och innovationsinitiativ uppmanas Europeiska kommissionen och medlemsstaterna att särskilt främja forskning om långsiktiga risker och sociala konsekvenser. Sådan verksamhet kan innefatta forskning om interoperabilitet, inbyggd säkerhet, och inbyggd integritet. Kommissionen ska särskilt stödja sådan forskning som sker inom ramen för öppna standarder och öppna forskningsmiljöer (detta inkluderar öppna plattformar och innovativa licensieringsmodeller).[26]

2.1.3 Standardisering för cybersäkerhet i självkörande fordon

Resolutionen uppmanar dessutom till fortsatt arbete med standardisering för produktsäkerhet och konsumentskydd. Utöver Internationella standardiseringsorganisationen (ISO) nämner resolutionen de europeiska standardiseringsorganen (Comité Européen de Normalisation, Comité Européen de Normalisation Électrotechnique, och European Telecommunications Standards Institute) som särskilt viktiga. Standardiseringen föreslås utvecklas genom specialiserade kommittéer, såsom ISO/TC 299 Robotics. Enligt resolutionen bör den även främja säkerhetsprövning av teknologin genom verkliga scenarion och i verkliga miljöer. Man förutser i resolutionen att det bör vara Europeiska kommissionens jobb att ta fram enhetliga kriterier som medlemsstaterna kan följa för att genomföra sådan säkerhetsprövning.[27]

2.1.4 Etisk uppförandekod för robotingenjörer

Delar av resolutionens säkerhetsprinciper kan utläsas ur en uppförandekod[28] för ingenjörer och forskare. Uppförandekoden riktar sig till forsknings- och utvecklingsverksamhet och innefattar följande säkerhetsrelaterade vägledningar:

Mänskliga rättigheter och integritet – forskare och ingenjörer bör respektera grundläggande rättigheter, inklusive rätten till skydd av personuppgifter samt individens integritet.

[26] Europaparlamentets resolution av den 16 februari 2017 med rekommendationer till kommissionen om civilrättsliga bestämmelser om robotteknik (2015/2103(INL)), Bilaga till resolutionen

[27] Europaparlamentets resolution av den 16 februari 2017 med rekommendationer till kommissionen om civilrättsliga bestämmelser om robotteknik (2015/2103(INL)), standardisering, trygghet och säkerhet

[28] Europaparlamentets resolution av den 16 februari 2017 med rekommendationer till kommissionen om civilrättsliga bestämmelser om robotteknik (2015/2103(INL)), Bilaga till resolutionen

Försiktighetsåtgärder – forskare bör genomföra skyddsåtgärder med hänsyn till eventuell säkerhetspåverkan. En riskbedömning bör ligga till grund för forskningen.

Säkerhet – konstruktörer bör ta hänsyn till människors säkerhet och ska utan dröjsmål lämna uppgifter om hot mot allmänhetens säkerhet.

2.1.5 Behörigheter för konstruktörer och användare

För att (bland annat) främja säker konstruktion och tillämpning av robottekniken (inklusive smarta fordons) bör den enligt resolutionen licensieras.

Säkerhetsaspekterna i licensieringsmodellen för konstruktörer av smarta fordon respektive användare av smarta fordon redovisas i nedanstående tabell (Tabell 1).

Tabell 1: Säkerhetsaspekter i licensieringsmodellerna för konstruktörer och användare av robotteknik.

Konstruktör	Skada, utnyttja, och vilseled inte användare
	Tillämpa tillförlitlig hårdvaru- och mjukvarudesign
	Säkerställ inbyggt integritetsskydd
	Gör automatiserat beslutsfattande spårbart och förutsägbart med transparent programmering
	Analysera osäkerhet kopplat till förutsägbarhet
	Säkerställ spårbarhet i automatiserat beslutsfattande
	Utvärdera risker (och fördelar)
	Garantera säkerheten för människor som interagerar med systemen, samt
	Genomför etisk prövning och erhåll ett positivt utlåtande från en etisk kommitté innan tester i verklig miljö
Användare	Skaffa tillåtelse att använda en robot utan risk för fysisk skada
	Var medveten om systemets perceptiva, kognitiva och handlingsbegräsningar
	Beakta individers integritet
	Inhämta samtycke vid personuppgiftsbehandling
	Modifiera inte system för att använda dem som vapen

2.2 Dataskydd och elektronisk kommunikation

Under början på 2018 trädde den Europeiska unionens allmänna dataskyddsförordning (även kallad GDPR)[29] i kraft. GDPR fastställer ett skydd för individers grundläggande rättigheter vid behandling av deras personuppgifter. Detta gäller även inom smarta vägnät och fordon. För närvarande ligger också ett förslag om en förordning för integritet och elektronisk kommunikation (COM/2016/0590) på EU-nivå.[30] En sådan skulle fastställa bestämmelser om skydd av grundläggande rättigheter för individer och företag vid tillhandahållandet och användningen av elektroniska kommunikationstjänster. Förslaget (COM/2016/0590) skulle ersätta Direktiv 2002/58/EC (ePrivacy-direktivet)[31] och uppdatera lag (2003:389) om elektronisk kommunikation i Sverige. Även om e-Privacy-förslaget kan spåras till 2017 har det under sommaren 2019 försenats i Europeiska unionens råd. Under det finska EU-ordförandeskapet är dock tanken att e–Privacy ska prioriteras.[32]

Det bör även uppmärksammas att systemet för tillsyn och utvecklingen av tillämpbara vägledningar för dataskyddet är omfattande. Därför bör aktörer som behandlar personuppgifter inom transportsektorn, och som vill uppmärksamma bästa praxis, följa utvecklingen inom ett flertal instanser. Den europeiska dataskyddsstyrelsen utfärdar råd, rekommendationer och bästa praxis för tillämpningen av hela det europeiska dataskyddet.[33] Styrelsen är sammansatt av representanter från

[29] 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) (Text av betydelse för EES), EUT L 119, 4.5.2016, s. 1–88

[30] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om respekt för privatlivet och skydd av personuppgifter i samband med elektronisk kommunikation och om upphävande av direktiv 2002/58/EG (förordning om integritet och elektronisk kommunikation) COM/2017/010 final - 2017/03 (COD)

[31] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) EGT L 201, 31.7.2002, s. 37–47

[32] David Thomas. (2019). *ePrivacy Regulation continues to stall, but there's hope?.* Från: https://iapp.org/news/a/eprivacy-regulation-continues-to-stall-but-theres-hope/. Senast 30/09/2019.

[33] 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) (Text av betydelse för EES), EUT L 119, 4.5.2016, s. 1–88, Artikel 70

tillsynsmyndigheterna i respektive medlemsstater och den Europeiska datatillsynsmannen.[34] I Sverige är det Datainspektionen som är tillsynsmyndighet för dataskyddet och som ger vägledning om dataskydd och följer utvecklingen av ny teknik, industripraxis och integritetsfrågor.[35] Det är även Datainspektionen som tar fram föreskrifter och allmänna råd för dataskyddet i Sverige.[36] Personuppgiftsansvariga har även möjlighet att, med andra i sin bransch, påverka tillämpningen av dataskyddet genom att gemensamt utarbeta uppförandekoder för personal inom branschen som ansvarar för verksamhet där uppgifterna behandlas.[37] Uppförandekoderna kan bistå i specifik branschtillämpning av dataskyddet då de ska utformas med hänsyn till den specifika branschen i sig och till behoven hos medelstora och små företag inom branschen. En utarbetad uppförandekod ska godkännas av Datainspektionen.[38]

Denna textdel fokuserar endast på den rättsliga utvecklingen under de senaste tio åren och går således inte in på äldre lagstiftning på området, exempelvis lag (2003:389) om elektronisk kommunikation. För en sammanställning över rättsakterna och vägledningar se Tabell 2.

[34] 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) (Text av betydelse för EES), EUT L 119, 4.5.2016, s. 1–88, Skäl 139

[35] Datainspektionen. (2019). *Datainspektionens uppdrag.* Från https://www.datainspektionen.se/om-oss/vart-uppdrag/. Senast 30/09/2019.

[36] Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning; Datainspektionen. (2019). *Datainspektionens föreskrifter och allmänna råd.* Från: https://www.datainspektionen.se/lagar--regler/datainspektionens-foreskrifter-och-allmanna-rad/. Senast 30/09/2019.

[37] 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) (Text av betydelse för EES), EUT L 119, 4.5.2016, s. 1–88, Artikel 40, Skäl 98-99

[38] 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) (Text av betydelse för EES), EUT L 119, 4.5.2016, s. 1–88, Artikel 40, Skäl 98-99

Tabell 2: Dataskydd och elektronisk kommunikation.

Rättsakter	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) EUT L 119, 4.5.2016
	Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning
Förslag till rättsakter	Förslag till Europaparlamentets och rådets förordning om respekt för privatlivet och skydd av personuppgifter i samband med elektronisk kommunikation och om upphävande av direktiv 2002/58/EG (förordning om integritet och elektronisk kommunikation) COM/2017/010 final - 2017/03 (COD)
	Förslag till Europaparlamentets och rådets direktiv om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning) COM/2016/0590 final - 2016/0288 (COD)
Vägledningar	Article 29 Data Protection Working Party (2017) Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS), 17/EN, WP 252
	Article 29 Data Protection Working Party (2017) Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS), 17/EN, WP 252
	International Working Group on Data Protection in Telecommunications (2018) Connected Vehicles (63rd meeting, 9-10 April 2018, Budapest, Hungary)
	Yttrande från Europeiska datatillsynsmannen om kommissionens meddelande handlingsplan för införande av intelligenta transportsystem i EU och det åtföljande förslaget till Europaparlamentets och rådets direktiv om en ram för införande av intelligenta transportsystem på vägtransport-området och för gränssnitt mot andra transportsätt (2010/C 47/02)

Enligt Enisas vägledning bör bästa praxis för smarta fordon utformas för att skydda personuppgifter.[39] Artikel 29-Gruppen, som var ett rådgivande organ (nu ersatt av Europeiska dataskyddsstyrelsen), publicerade vägledningar för det europeiska dataskyddet och har även utrett dataskyddet i samverkande intelligenta transportsystem (C-ITS) (se del 2.6 av denna rapport om intelligenta transportsystem).[40] Även om Artikel 29-Gruppens utredning endast fokuserade på C-ITS, påpekade de att en högre grad av automation i vägtransport kommer medföra nya utmaningar för dataskyddet. Även vägmyndigheter och operatörer av intelligenta transportsystem som levererar samhällsviktiga tjänster måste tillämpa dataskyddet i sitt arbete med nätverks- och informationssäkerhet.[41] Artikel 29-Gruppen hävdade även att viss kommunikationsdata inom C-ITS omfattas av förslaget om en förordning om integritet och elektronisk kommunikation.[42] Ytterligare utredning av C-ITS och dataskyddet ligger på den Europeiska dataskyddsstyrelsens agenda för 2019-2020.[43] ITS omfattar bland annat system som använder informations- och kommunikationsteknologi för trafikledning och fordon.[44] Samverkande ITS (C-ITS) skulle exempelvis kunna vara fordon som kommunicerar med väginfrastrukturen.[45]

[39] ENISA (2016) Cyber Security and Resilience of smart cars Good practices and recommendations. doi: 10.2824/87614

[40] Article 29 Data Protection Working Party (2017) Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS), 17/EN, WP 252

[41] 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 EUVL L 194, 19.7.2016, s. 1—30

[42] Article 29 Data Protection Working Party (2017) Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS), 17/EN, WP 252, 12

[43] Europeiska datskyddsstyrelsen. (2019). Tenth Plenary session: Election of a new Deputy Chair, response to MEP In ‘t Veld, third annual Privacy Shield Review. Från: https://edpb.europa.eu/news/news/2019/tenth-plenary-session-election-new-deputy-chair-response-mep-t-veld-third-annual_en. Senast 25/06/2019.

[44] 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 Text av betydelse för EES OJ L 207, 6.8.2010, p. 1–13, Artikel 4; Lag (2013:315) om intelligenta transportsystem vid vägtransporter, 3§

[45] Europeiska kommissionen (2016) MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET, RÅDET, EUROPEISKA EKONOMISKA OCH SOCIALA KOMMITTÉN SAMT REGIONKOMMITTÉN: En europeisk strategi för samverkande intelligenta transportsystem, en milstolpe mot samverkande, uppkopplad och automatiserad rörlighet, COM(2016) 766 final, 3

2.2.1 Behandling av personuppgifter och elektronisk kommunikation i smarta fordon och vägnät

Alla uppgifter som kan knytas till en identifierad eller identifierbar individ är en personuppgift. Det spelar ingen roll vilket format uppgiften har (data, metadata, text, tal, bild etc.) för att det ska vara en personuppgift.[46] Det kan exempelvis röra sig om ägarnamn, modell eller nummerplåtar på fordon. Personuppgifter omfattar även digitaliserad data såsom onlineidentifikatorer, exempelvis IP-adresser, cookies och andra digitala spår som kan användas för att skapa profiler av teknikanvändare.[47] All typ av användning av uppgifterna är personuppgiftsbehandling. Detta medför ett rättsligt ansvar, bland annat för uppgifternas säkerhet.

En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra behandlar personuppgifter är antingen personuppgiftsansvariga eller personuppgiftsbiträden. I smarta fordon och vägnät finns flera aktörer som kan anta dessa roller, exempelvis systemtillverkare, fordonstillverkare, komponenttillverkare eller tjänsteleverantörer.[48] Personuppgiftsansvariga är de som bestämmer ändamål och metoder för personuppgiftsbehandling. Personuppgifts-biträden behandlar personuppgifter för den personuppgiftsansvariges räkning. Troligtvis är det generellt sett fordonstillverkare, system-tillverkare och komponenttillverkare som är personuppgiftsansvariga medan tjänsteleverantörer, exempelvis för integrering av applikationer

[46] 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) (Text av betydelse för EES), EUT L 119, 4.5.2016, s. 1–88, Artikel 4;Se även Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om respekt för privatlivet och skydd av personuppgifter i samband med elektronisk kommunikation och om upphävande av direktiv 2002/58/EG (förordning om integritet och elektronisk kommunikation) COM/2017/010 final - 2017/03 (COD), Artikel 4

[47] 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) (Text av betydelse för EES), EUT L 119, 4.5.2016, s. 1–88, Skäl 30

[48] Article 29 Data Protection Working Party (2017) Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS), 17/EN, WP 252, 5; International Working Group on Data Protection in Telecommunications (2018) Connected Vehicles (63rd meeting, 9-10 April 2018, Budapest, Hungary),

eller smart telefoni, tar rollen som personuppgiftsbiträden.[49] Det är den personuppgiftsansvariges skyldighet att tillgodose lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna samt att endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder.[50] Detta ansvar omfattar även tekniska och organisatoriska åtgärder för säkerhet (se nedan).

Förslaget om en förordning för integritet och elektronisk kommunikation (COM/2016/0590) avser särskilt dataskydd och säkerhet för leverantörer av elektroniska kommunikationstjänster och kommunikationsnät behandling av elektronisk kommunikation (exempelvis metadata). Med elektronisk kommunikationstjänst avses ett system för bland annat överföring, koppling eller dirigering av elektronisk kommunikation.[51] Med elektroniska kommunikationstjänster avser man en tjänst via ett elektroniskt kommunikationsnät som antingen omfattar internetanslutning eller signalöverföring och som tillhandahåller maskin till maskin-tjänster.[52]

[49] International Working Group on Data Protection in Telecommunications (2018) Connected Vehicles (63rd meeting, 9-10 April 2018, Budapest, Hungary), 11

[50] 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) (Text av betydelse för EES), EUT L 119, 4.5.2016, s. 1–88, Artiklarna 24-28

[51] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om respekt för privatlivet och skydd av personuppgifter i samband med elektronisk kommunikation och om upphävande av direktiv 2002/58/EG (förordning om integritet och elektronisk kommunikation) COM/2017/010 final - 2017/03 (COD), Artikel 4; Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning) COM/2016/0590 final - 2016/0288 (COD)

[52] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om respekt för privatlivet och skydd av personuppgifter i samband med elektronisk kommunikation och om upphävande av direktiv 2002/58/EG (förordning om integritet och elektronisk kommunikation) COM/2017/010 final - 2017/03 (COD), Artikel 4; Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning) COM/2016/0590 final - 2016/0288 (COD)

2.2.2 Krav på säker databehandling i smarta fordon och nät

Syftet med säkerhetsbestämmelserna i dataskyddet[53] är att förebygga personuppgiftsincidenter. Personuppgiftsincidenter är oavsiktlig, obehörig eller otillåten behandling av personuppgifter,[54] exempelvis oproportionerlig delning av personuppgifter, läsning eller annan åtkomst av tredje part, ändringar och raderingar.[55] Dataskyddet fastställer ett antal krav, varav flera är gemensamma med eller likartade de i e-Privacy-förslaget (COM/2016/0590). Kraven är generella men experter[56] har påvisat att vissa av dem har särskild betydelse för transportsektorn.

Genomför konsekvensbedömning vid personuppgiftsbehandling med ny teknik.[57] GDPR fastställer ett antal typer av behandling med ny teknik där konsekvensbedömning ska genomföras. För transportsektorn innefattar förmodligen de mest relevanta scenariona någon form av systematisk övervakning på allmän plats eller en automatiserad lokalisering.[58] Betydelsen av just automatiserad lokalisering kan förväntas växa i takt

[53] Se även Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning) COM/2016/0590 final - 2016/0288 (COD), Artikel 10(1)

[54] 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) (Text av betydelse för EES), EUT L 119, 4.5.2016, s. 1–88, Artikel 4

[55] 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) (Text av betydelse för EES), EUT L 119, 4.5.2016, s. 1–88, Artiklarna 5, 33

[56] Se exempelvis EDPS. (2016). Artificial Intelligence, Privacy and Data Protection. Från: https://edps.europa.eu/sites/edp/files/publication/16-10-19_marrakesh_ai_paper_en.pdf. Senast 02/07/2019; Article 29 Data Protection Working Party (2017) Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS), 17/EN, WP

[57] 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) (Text av betydelse för EES), EUT L 119, 4.5.2016, s. 1–88, Artikel 35

[58] 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) (Text av betydelse för EES), EUT L 119, 4.5.2016, s. 1–88, Artikel 35

med ökad autonomi i fordonens styrning.[59] Även om konsekvensbedömningen främst är en skyddsåtgärd mot risker för individens rättigheter än för säkerheten i sig, ska konsekvensbedömningen även innehålla åtgärder och rutiner för behandlingens säkerhet. [60]

Genomför förhandssamråd innan behandlingen. Om konsekvensbedömningen påvisar att personuppgiftsbehandlingen medför en hög risk för individens rättigheter, exempelvis svårigheter att hantera risken för personuppgiftsincidenter, ska den personuppgiftsansvarige samråda med Datainspektionen för att få skriftliga råd i frågan.[61]

Personuppgifter ska behandlas med lämplig säkerhet enligt GDPR.[62] Elektroniska kommunikationer ska vara konfidentiella, skyddade och ha möjlighet att tillhandahålla sekretess[63] enligt förslaget för en förordning om integritet och elektronisk kommunikation. Tekniska och organisatoriska åtgärder för säkerheten i dataskyddet såväl som elektroniska kommunikationer ska väljas utifrån samma kriterier,[64] det vill säga:

- vilka typer av personuppgifter som ska skyddas

[59] EDPS. (2016). Artificial Intelligence, Privacy and Data Protection. Från: https://edps.europa.eu/sites/edp/files/publication/16-10-19_marrakesh_ai_paper_en.pdf. Senast 02/07/2019. 12

[60] 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) (Text av betydelse för EES), EUT L 119, 4.5.2016, s. 1–88, Artikel 35

[61] 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) (Text av betydelse för EES), EUT L 119, 4.5.2016, s. 1–88, Artikel 36

[62] 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) (Text av betydelse för EES), EUT L 119, 4.5.2016, s. 1–88, Artiklarna 5, 33

[63] Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning) COM/2016/0590 final - 2016/0288 (COD), Artikel 8

[64] Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning) COM/2016/0590 final - 2016/0288 (COD), Artiklarna 5, 8, 10, Skäl 37

- de risker som behandlingen medför (inklusive risk för data-ändring, dataläckage eller dataförstöring samt risker för individens rättigheter)
- vilka typer av skador som kan uppstå vid incidenter (exempelvis materiell och immateriell skada)
- hur risker uppkommer (exempelvis obehörig eller otillåten åtkomst eller röjande av uppgifterna)
- vad som är den senaste utvecklingen inom säkerhetstekniker
- genomförandekostnaderna för säkerhetsåtgärder i förhållande till riskerna.[65]

Lagarna är generellt sparsamma med att explicit förespråka tekniska säkerhetsåtgärder. Både GDPR och förslaget för en förordning om integritet och elektronisk kommunikation håller kryptering som en möjlig åtgärd (se tabell 3).[66]

En av farhågorna som Artikel 29-Gruppen i sin senare granskning uttryckte med C-ITS är att delar av tjänsterna baseras på fortlöpande ”peer-to-peer” kommunikation mellan enheter (exempelvis fordon) som gör spridningen av uppgifter svår att begränsa och därmed även svår att skydda.[67] Artikel 8 i förslaget (COM/2016/0590) skulle kunna innebära ett generellt förbud mot insamling av sådana data, exempelvis ”peer-to-peer” kommunikation, så länge insamlingen inte är tidsbegränsad och uppfyller säkerhetskraven i Artikel 32 GDPR (ovan).[68] Medan ”public key infrastructure” (PKI) har tillämpats som säkerhetslösning, anser Artikel 29-Gruppen att ytterligare kompletterande säkerhetsåtgärder kommer att krävas, exempelvis:

[65] 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) (Text av betydelse för EES), EUT L 119, 4.5.2016, s. 1–88, Artiklarna 5, 33; Article 29 Data Protection Working Party (2017) Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS), 17/EN, WP 252, 12-13

[66] 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) (Text av betydelse för EES), EUT L 119, 4.5.2016, s. 1–88, Artikel 32; Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning) COM/2016/0590 final - 2016/0288 (COD), Skäl 37

[67] Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS), 17/EN, WP 252, 3, 12

[68] Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS), 17/EN, WP 252, 12

- periodiska kontroller av PKI-certifieringen
- åtgärder för att motverka obehörig ändring av kommunikationer under sändningen (exempelvis genom injicering av falsk data)
- förmåga att urskilja falskt positiva och falskt negativa säkerhetsmeddelanden ur kommunikationerna.[69]

[69] Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS), 17/EN, WP 252, 12-13

Tabell 3: tekniska säkerhetsåtgärder för behandling av personuppgifter och för elektronisk kommunikation.

GDPR (Förordning (EU) 2016/679 – Artikel 32) [70]	Pseudonymisering och kryptering av personuppgifter.
	Förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingsystemen och tjänsterna.
	Förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident.
	Ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.
Förslag COM/2016/0590	Kontroll av säkerhetshot, såsom förekomst av sabotageprogram.[71]
	Använda specifika typer av programvara eller krypteringsteknik.[72]
	Avhjälpa nya oförutsedda säkerhetsrisker och återställa tjänstens normala säkerhetsnivå.[73]
	Säkerheten bedöms mot bakgrund av artikel 32 i förordning (EU) 2016/679.[74]
	Bevara eller återupprätta säkerheten för elektroniska kommunikationsnät och elektroniska kommunikationstjänster, eller för att upptäcka tekniska fel och/eller brister i överföringen av elektronisk kommunikation.[75]

[70] 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) (Text av betydelse för EES), EUT L 119, 4.5.2016, s. 1–88, Artikel 32

[71] Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning) COM/2016/0590 final - 2016/0288 (COD), Skäl 16

[72] Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning) COM/2016/0590 final - 2016/0288 (COD), Skäl 37

I smarta fordon med ökad autonomi kommer förmodligen exakt kartografi och lokalisering vara en avgörande faktor för säker drift.[76] Då automatiserad lokalisering kan utgöra känsliga personuppgifter kommer sannolikt betydelsen av anonymisering som säkerhetsåtgärd även få ökad betydelse för dataskyddet i systemen.[77]

Risker och incidenter ska meddelas. Både GDPR och förslaget (COM/2016/0590) för en förordning om integritet och elektronisk kommunikation kräver i vissa fall att berörda individer får säkerhetsrelaterad information. Enligt förslaget ska användare av programvara för elektronisk kommunikation få information om hur de justerar sekretessinställningar för att tredje part inte ska lagra kommunikationerna.[78] Förslaget kräver att leverantörer av elektroniska kommunikationstjänster informerar sina användare redan när en risk mot säkerheten identifieras, om risken inte kan åtgärdas av leverantören. Användare ska då även få information om hur de kan lindra risken samt eventuella kostnader för åtgärderna.[79] GDPR förutsätter istället att individer vars personuppgifter behandlas ska informeras först vid en personuppgiftsincident. Om en personuppgiftsincident kan innebära någon risk för individens fri- och rättigheter ska incidenten, dess omständigheter, effekter och korrigerande åtgärder rapporteras till

[73] Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning) COM/2016/0590 final - 2016/0288 (COD), Skäl 37

[74] Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning) COM/2016/0590 final - 2016/0288 (COD), Skäl 37

[75] Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning) COM/2016/0590 final - 2016/0288 (COD), Artikel 6

[76] EDPS. (2016). Artificial Intelligence, Privacy and Data Protection. Från: https://edps.europa.eu/sites/edp/files/publication/16-10-19_marrakesh_ai_paper_en.pdf. Senast 02/07/2019. 12

[77] Yttrande från Europeiska datatillsynsmannen om kommissionens meddelande handlingsplan för införande av intelligenta transportssystem i EU och det åtföljande förslaget till Europaparlamentets och rådets direktiv om en ram för införande av intelligenta transportsystem på vägtransportområdet och för gränssnitt mot andra transportsätt (2010/C 47/02), 44-49§§

[78] Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning) COM/2016/0590 final - 2016/0288 (COD), Artikel 10

[79] Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning) COM/2016/0590 final - 2016/0288 (COD), Artikel 17

Datainspektionen som är tillsynsmyndighet i Sverige.[80] Om incidenten medför en hög risk för fri- och rättigheter ska information utgå till den registrerade vars personuppgifter kompromitterats.[81]

2.3 Nätverks och informationssäkerhet i samhällsviktig verksamhet

I maj 2018 antogs ett antal lagar för nätverks- och informationssäkerhet i samhällsviktig verksamhet. Lagarna införde gemensamma regler för nätverks- och informationssäkerhet i samtlig samhällsviktig verksamhet, inklusive inom vägtransport,[82] inom hela den Europeiska unionen. Reglerna gäller för leverantörer av samhällsviktiga tjänster och förekommer i ett antal rättsakter och föreskrifter på europeisk och nationell nivå (se tabell 4).

Utöver att MSB är den svenska övergripande tillsynsmyndigheten, är MSB också incidenthanteringsorganisation (så kallad CERT och CSIRT).[83] MSB får även meddela föreskrifter och allmänna råd för NIS-regleringen i Sverige.[84] Ytterligare föreskrifter för nätverks- och informationssäkerhet kan utarbetas dels på övergripande nivå för

[80] 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) (Text av betydelse för EES), EUT L 119, 4.5.2016, s. 1–88, Artikel 33

[81] 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) (Text av betydelse för EES), EUT L 119, 4.5.2016, s. 1–88, Artikel 34

[82] 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 EUVL L 194, 19.7.2016, s. 1—30; Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster; Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster

[83] 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 Text av betydelse för EES, EUT L 207, 6.8.2010, s. 1–13 Artikel 9; Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, 21, 24-27§; MSB. (2019). *NIS-direktivet.* Från: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/. Senast 26/07/2019; MSB. (2019). *Cert.se.* Available: https://www.cert.se/. Senast 26/07/2019.

[84] Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, 4, 17, 20, 21§§; Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster, 3-4§§

samhällsviktig verksamhet och dels på sektoriell nivå (inom transportsektorn). När MSB utarbetar föreskrifter och allmänna råd brukar dessa gå på remiss för att inhämta relevanta aktörers synpunkter.[85] Transportstyrelsen är tillsynsmyndighet för NIS-efterlevnad på transportsektorn[86] och får därmed utarbeta ytterligare föreskrifter om säkerhetsåtgärder specifika för transportsektorn. Även Transportstyrelsen lägger ut sina föreskrifter på remiss för att kommenteras av relevanta offentliga och privata aktörer.[87]

Tabell 4: Nätverks- och informationssäkerhet i samhällsviktig verksamhet.

Rättsakter	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, EUT L 194, 19.7.2016, s. 1–30 Lag (2018:1174) om informationssäkerhet för samhällsviktiga digitala tjänster Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster, MSBFS 2018:7 Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster, MSBFS 2018:8 Myndigheten för samhällsskydd och beredskaps allmänna råd om informationssäkerhet för leverantörer av samhällsviktiga tjänster, MSBFS 2018:8 Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster, MSBFS 2018:9

På unionsnivå är det Enisa som ska bistå med råd och expertis kring nätverks- och informationssäkerhet samt stödja den europeiska samarbetsgruppen för behöriga myndigheter med sina uppgifter.[88]

[85] MSB. (2019). *Remisser, föreskrifter och allmänna råd.* Från: https://www.msb.se/sv/regler/remisser-foreskrifter-och-allmanna-rad/. Senast 30/09/2019.
[86] Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster, 17§
[87] Transportstyrelsen. (2019). *Remisser.* Från: https://transportstyrelsen.se/sv/Regler/Remisser/. Senast 30/09/2019.
[88] 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 EUVL L 194, 19.7.2016, s. 1—30, Skäl 36, 38

Samarbetsgruppen ska också underlätta informationsutbyte och utbyte av bästa praxis kring nätverks- och informationssäkerhet, samt säkerhetsstandardisering.[89] Samarbetsgruppen består i huvudsak av representanter från Enisa och medlemsstaterna, men företrädare från berörda aktörer kan även delta vid inbjudan.[90] Även icke-europeiska stater och internationella organisationer kan bjudas in.[91]

MSB är Sveriges behöriga myndighet och nationella kontaktpunkt för att delta i gränsöverskridande samarbete i den europeiska samarbetsgruppen och europeiska CSIRT-nätverket.[92] Det europeiska CSIRT-nätverket samlar företrädare från medlemsstaternas CSIRT-enheter för att bland annat diskutera, utforska och utfärda riktlinjer kring incidenter, kategorier av incidenter och relaterade risker, tidig varning, ömsesidigt bistånd och samordning vid gränsöverskridande incidenter.[93]

Behöriga myndigheter som MSB och Transportsstyrelsen bör även, utöver formella mekanismer, upprätthålla informella mekanismer för informationsutbyte mellan myndigheter och leverantörer av samhällsviktiga tjänster (inklusive privat sektor).[94] Även leverantörerna av samhällsviktiga tjänster bör upprätta eller medverka i egna informella samarbetsgrupper för informationsutbyte och utveckling av praxis kring säkerhet.[95] I Sverige samordnar exempelvis MSB informella samarbeten kring säkerhet med aktörer över sektorer. Ett exempel är det privata-offentliga samverkansforumet FIDI-SCADA som fokuserar bland annat på informationsombyte om informationssäkerhet i industriella

[89] 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 EUVL L 194, 19.7.2016, s. 1—30, Artikel 11

[90] 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 EUVL L 194, 19.7.2016, s. 1—30, Artikel 11

[91] 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 EUVL L 194, 19.7.2016, s. 1—30, Artikel 13

[92] 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 Text av betydelse för EES, EUT L 207, 6.8.2010, s. 1–13 Artiklarna 8, 11, 12

[93] 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 EUVL L 194, 19.7.2016, s. 1—30, Artikel 12

[94] 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 EUVL L 194, 19.7.2016, s. 1—30, Skäl 44

[95] 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 EUVL L 194, 19.7.2016, s. 1—30, Skäl 35

informations- och styrsystem.[96] En stor del av ansvaret för säkerhet och val av åtgärder vilar på leverantörerna av samhällsviktiga tjänster själva.[97] Därför kan det vara värdefullt att utforska möjligheterna att utbyta erfarenheter genom informella samarbeten med aktörer som möter liknande typer av utmaningar i tillämpningen av lagstiftning. Dock bör det påpekas att NIS-direktivet inte bara förutser privat-offentlig samverkan i att utforska gemensamma säkerhetskrav utan även medverkan från forskningscentrum i dessa frågor.[98]Just i hänseende till standardisering hänvisar NIS-direktiv till behov av ökat internationellt samarbete för att förbättra säkerhetsstandarder (se del 2.4 i denna rapport).[99]

2.3.1 Leverantörer av samhällsviktig verksamhet inom vägtransport

Leverantörer av samhällsviktiga tjänster är privata eller offentliga organisationer som upprätthåller ekonomiskt och samhälleligt kritisk verksamhet. För att verksamheten ska identifieras som samhällsviktig i lagens mening ska den även vara beroende av nätverks- och informationssystem, och en incident (med negativ inverkan på systemen) medföra en betydande störning för tillhandahållandet av tjänsten. Inom vägtransportområdet kan vägmyndigheter och operatörer av intelligenta transportsystem vara leverantörer av samhällsviktiga tjänster.

Vägmyndigheter har ansvar för planering, kontroll eller förvaltning av nationella vägar[100] såsom Trafikverket samt kommuner som ansvarar för

[96] MSB. (2018). *FIDI-SCADA.* Senast: https://www.msb.se/RibData/Filer/pdf/27924.pdf. Från 30/09/2019.

[97] 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 EUVL L 194, 19.7.2016, s. 1—30, Skäl 44

[98] 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 EUVL L 194, 19.7.2016, s. 1—30, Skäl 5

[99] 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 EUVL L 194, 19.7.2016, s. 1—30, Skäl 43

[100] Se Kommissionens delegerade förordning (EU) 2015/962 av den 18 december 2014 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller tillhandahållande av EU-omfattande realtidstrafikinformationstjänster (Text av betydelse för EES) EUT L 157, 23.6.2015, s. 21–31, Artikel 2

vägarna.[101] I Sverige omfattas TEN-T vägnät och vägnäten i storstodsområdena för Stockholm, Göteborg och Malmö.[102]

Operatörer av intelligenta transportsystem ansvarar för system på vägtransportområdet som tillämpar informations- och kommunikationsteknik. Systemen kan vara del av infrastruktur, fordon och användare, samt användas för trafikledning och mobilitetshantering likväl som gränssnitt mot andra transportslag.[103] I Sverige anses larmcentraler för eCall samt rikstäckande statliga databaser med uppgifter om hastighetsbegränsningar, vägbredd, bärighet eller rekommenderad väg för farligt gods vara operatörer av intelligenta transportsystem.[104]

Hårdvaru- och mjukvarutillverkare är inte leverantörer av samhällsviktiga tjänster även om deras produkter påverkar nätverks-och informationssäkerheten i dessa tjänster. Dessa tillverkare omfattas istället av lagar för produktsäkerhet[105] samt av standardisering för informations- och kommunikationsteknologi etc. (se avsnitt 2.4, 3 samt Bilaga 1 i denna rapport).

2.3.2 Säkerhetskrav för samhällsviktig verksamhet

NIS-lagstiftningen innehåller tre (till fyra) huvudsakliga säkerhetskrav för vägmyndigheter och operatörer av intelligenta transportsystem: anmälan av den samhällsviktiga tjänsten, ändamålsenliga och proportionerliga åtgärder (inklusive ett systematiskt och riskbaserat tillvägagångssätt för säkerhet) och incidentrapportering. Dessa kan förklaras som följer.

[101] Transportstyrelsen (2016) Framställan om ändring i förordning (2016:383) om intelligenta transportsystem vid vägtransporter: Ändring med anledning av förordning (EU) nr 2015/962 om realtidstrafikinformationstjänster (TSG 2016-2881), Sid 19; Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster. MSBFS 2018:7, 3§ 1 Kap

[102] Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster. MSBFS 2018:7, 4§ 4 Kap

[103] 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 Text av betydelse för EES, EUT L 207, 6.8.2010, s. 1–13 Artikel 4; Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster. MSBFS 2018:7, 3§ 1 Kap

[104] Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster. MSBFS 2018:7, 4§ 4 Kap

[105] 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 EUVL L 194, 19.7.2016, s. 1—30, Skäl 50

Anmäl den samhällsviktiga tjänsten till Transportstyrelsen i enlighet med MSB:s föreskrifter.[106]

Vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att förebygga, detektera, och minimera verkningarna av och hantera risker mot tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter samt säkerställa kontinuitet i tjänster som utförs genom nätverk och informationssystem. [107]

Informationssäkerhetsarbetet ska vara systematiskt, riskbaserat, utformat efter organisationens behov, och baseras på SS-EN ISO/IEC 27001:2017 och SS-EN ISO/IEC 27002:2017 eller motsvarande standard.[108] För specialiserat informationssäkerhetsarbete, såsom inom verksamhet med smarta fordon och vägnät, kan det vara önskvärt att tillämpa motsvarande men specialiserade standarder. I så fall bör leverantören analysera och dokumentera likheter och olikheter med SS-EN ISO/IEC 27001:2017 och SS-EN ISO/IEC 27002:2017.[109] Det riskbaserade informationssäkerhetsarbetet innefattar att:

- tydliggöra ansvar, roller, befogenheter och resurser för informationssäkerhetsarbetet[110]
- upprätta en informationssäkerhetspolicy med målsättningar, inriktning och interna regler för informationssäkerhet[111]
- informera om och utbilda personalen i de interna reglerna samt utvärdera och uppdatera utbildningen om brister identifieras[112]

[106] 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 EUVL L 194, 19.7.2016, s. 1—30, Artikel 5; Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, 23§; Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster, MSBFS 2018:7

[107] Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, 12§; Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster MSBFS 2018:8, 5§

[108] Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, 12§; Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster MSBFS 2018:8, 5§

[109] Myndigheten för samhällsskydd och beredskaps allmänna råd om informationssäkerhet för leverantörer av samhällsviktiga tjänster MSBFS 2018:8, 5§

[110] Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster MSBFS 2018:8, 6§

[111] Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster MSBFS 2018:8, 7§

[112] Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster MSBFS 2018:8, 9§

- utföra en årlig, dokumenterad riskanalys som identifierar, analyserar och värderar risker[113]
- klassa information, med grund i riskanalysen, utifrån potentiella konsekvenser för konfidentialitet, riktighet och tillgänglighet[114]
- dokumentera en åtgärdsplan med åtgärder som är lämpliga utifrån riskanalysen och informationsklassningen,[115] (där åtgärderna bör grupperas i skyddsnivåer kopplade till informationsklassningens konsekvensnivåer)[116]
- vidare dokumentera när åtgärder vidtas[117]
- följa upp och utvärdera informationssäkerhetsarbetet.[118]

Det finns även ytterligare krav på vad de tekniska och organisatoriska åtgärderna samt de interna reglerna för informationssäkerhet ska ta hänsyn till. Det ska finnas interna regler om ett antal åtgärder. För det första för systemens drift och förvaltning, arkitektur samt sammankoppling mot andra nätverk och system. Upptäckt och åtgärdande av incidenter och avvikelser i informationshanteringen regleras också internt. Slutligen måste det även finnas regler om hur behovet av kontinuitet fastställs, upprätthålls och övas samt hur arbetet med att minimera effekterna av incidenter ska utvärderas.[119] Sedan finns det även krav på fem tekniska och organisatoriska åtgärder:

[113] Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, 12§; Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster MSBFS 2018:8, 8§

[114] Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, 12§; Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster MSBFS 2018:8, 8§; Myndigheten för samhällsskydd och beredskaps allmänna råd om informationssäkerhet för leverantörer av samhällsviktiga tjänster MSBFS 2018:8, 8§

[115] 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 EUVL L 194, 19.7.2016, s. 1—30, Artikel 14; Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, 2, 13, 12 och 14§§; Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster MSBFS 2018:8, 8§; Myndigheten för samhällsskydd och beredskaps allmänna råd om informationssäkerhet för leverantörer av samhällsviktiga tjänster MSBFS 2018:8, 8§

[116] Myndigheten för samhällsskydd och beredskaps allmänna råd om informationssäkerhet för leverantörer av samhällsviktiga tjänster MSBFS 2018:8, 8§

[117] Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster MSBFS 2018:8, 8§

[118] Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster MSBFS 2018:8, 8§

[119] Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster MSBFS 2018:8, 10-12§§

- säkerheten i system och anläggningar
- incidenthantering
- hantering av driftskontinuitet
- övervakning, revision och testning
- efterlevnad av internationella standarder.[120]

MSB:s allmänna råd innehåller även ytterligare vägledning om hur informationssäkerhet, incidenthantering och kontinuitetshantering bör tillämpas (se tabell 5).

Rapportera incidenter med betydande inverkan utan onödigt dröjsmål[121] till MSB:s CSIRT-enhet.[122] Information om hur incidenter ska rapporteras finns i MSB:s föreskrifter[123] samt på MSB:s webbsida.[124] För transportsektorn ska en incidents inverkan framför allt bedömas som betydande utifrån tre faktorer. Det ska finnas minst 1000 påverkade användare och pågått minst en timme. Alternativt kan varaktighet överstigit två timmar eller så uppgår det påverkade geografiska området till 10 000 kvadratkilometer.[125] Utöver dessa ska leverantören ta hänsyn till ytterligare förhållanden för att bedöma om inverkan är betydande, inklusive:

- inverkan på ekonomisk eller samhällsviktig verksamhet
- inverkan på allmän säkerhet

[120] 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 EUVL L 194, 19.7.2016, s. 1—30, Artikel 16; Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster, 6§

[121] 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 EUVL L 194, 19.7.2016, s. 1—30, Artikel 14; Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, 18§;

[122] Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster, 11-12§§; Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster, MSBFS 2018:9, 2§ 2 Kap

[123] Myndigheten för samhällsskydd och beredskaps allmänna råd om informationssäkerhet för leverantörer av samhällsviktiga tjänster MSBFS 2018:8

[124] MSB. (2019). *NIS-direktivet.* Fråm: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/. Senast 26/07/2019; MSB. (2019). *Cert.se.* Från: https://www.cert.se/. Senast 26/07/2019.

[125] Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster, 9§; Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster, MSBFS 2018:9, 4 Kap

- vilken marknadsandel (eller omfattning av tjänsten) som påverkas av störningen
- alternativa sätt att tillhandahålla tjänsten (exempelvis utan nätverks- och informationssystem).[126]

Tabell 5: Vägledningar om informationssäkerhet, incidenthantering och kontinuitetshantering.

Informationssäkerhet[127]	Beakta den tekniska utvecklingen
	Identifiera och åtgärda tekniska hot och sårbarheter löpande
	Säkerställ korrekt och tillräcklig information över system
	Upprätta separata miljöer mellan produktion och tester
	Analysera behov av certifierade krypto- och it-säkerhetsprodukter
Incidenthantering[128]	Fastställa interna regler för tillförlitlig spårbarhet och händelseloggning i systemen
	Revidera arbetssätt och säkerhetsåtgärder vid incidenter och avvikelser
	Bered tillgång till information om incidenter och avvikelser för den som leder informationssäkerhetsarbetet
Kontinuitetshantering[129]	Ta hänsyn till den samhällsviktiga tjänstens kvalitet, kvantitet och tjänstegarantier vid bedömning av driftskontinuitet
	Fastställ interna regler för accepterad återställandetid, beslut om alternativa respektive normala arbetssätt för tjänsteleverans, samt behov av uthållighet över tid
	Utvärdering av kontinuitetshantering efter upptäckta brister, övningar, utkontraktering eller ändrade rättsliga eller organisatoriska krav

[126] 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 EUVL L 194, 19.7.2016, s. 1—30, Artikel 6, Skäl 26

[127] Myndigheten för samhällsskydd och beredskaps allmänna råd om informationssäkerhet för leverantörer av samhällsviktiga tjänster MSBFS 2018:8, 10§

[128] Myndigheten för samhällsskydd och beredskaps allmänna råd om informationssäkerhet för leverantörer av samhällsviktiga tjänster MSBFS 2018:8, 11§

[129] Myndigheten för samhällsskydd och beredskaps allmänna råd om informationssäkerhet för leverantörer av samhällsviktiga tjänster MSBFS 2018:8, 12§

Behandla personuppgifter på ett sätt som är förenligt med dataskyddet inklusive säkerhetsregler som fastställs genom dataskyddslagarna (se del 2.2 om dataskydd i denna rapport).[130]

2.4 Cybersäkerhetsstandardisering

COM(2017) 477 innefattar ett förslag om en ny europeisk förordning om certifiering av informations- och kommunikationsteknologi (”cybersäkerhetsakten”).[131] En överenskommelse nåddes i december 2018 som ska höja säkerheten och motståndskraften i europeisk informations- och kommunikationsteknologi och produkter.[132] Den centrala delen av förslaget innefattar harmoniserade certifieringsordningar (standardisering, ackreditering och certifiering) som intygar att produkterna är cybersäkerhetscertifierade på ett sätt som kan skapa och bevara tilltro hos kunder och användare.[133] Europeiska kommissionen förutser att tillitsaspekten av cybersäkerhet och certifieringsordningarna kommer vara särskilt viktiga för nya system med hög nivå av digitalisering och höga säkerhetskrav, exempelvis uppkopplade och automatiserade fordon.[134] Det är viktigt att uppmärksamma att, om inte annat föreskrivs, ska europeisk cybersäkerhetscertifiering vara frivillig.[135]

Enisa kommer att ha övergripande ansvar för att stödja unionens politik för cybersäkerhetscertifiering av produkter och tjänster för informations-

[130] 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 EUVL L 194, 19.7.2016, s. 1—30, Artikel 2

[131] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD)

[132] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), Artikel 1

[133] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), 8-10

[134] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), 8-9

[135] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), Artikel 48, sid 12

och kommunikationsteknologi (IKT-produkter och tjänster), inklusive att utarbeta förslag till europeiska system för cybersäkerhetscertifiering.[136] Enisa kommer även utfärda föreskrifter för god praxis i cybersäkerhet för IKT-tillverkare och tjänsteleverantörer.[137] Europeiska cybersäkerhetscertifikat ska utfärdas av ackrediterade[138] organ som bedömer överstämmelse med cybersäkerhetsbestämmelser.[139] I vissa fall kommer de europeiska cybersäkerhetscertifikaten utfärdas av offentliga organ, exempelvis nationella tillsynsmyndigheter eller ett nationellt organ uppfört enligt ISO/IEC 17065:2012.[140] De europeiska nationella tillsynsmyndigheterna ska bland annat:

- övervaka och kontrollera nationella bestämmelser samt utfärdade certifikat och överensstämmelse med cybersäkerhetsakten
- övervaka och kontrollera organ som bedömer överstämmelse med cybersäkerhetsbestämmelser
- övervaka utvecklingen på området för cybersäkerhetscertifiering
- samarbeta och dela information med andra nationella tillsynsmyndigheter samt delta i den europeiska gruppen för cybersäkerhetscertifiering som bland annat ska bistå Europeiska kommissionen och Enisa med råd och yttranden.[141]

[136] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), Artikel 8.

[137] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), Artikel 8.

[138] Se Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 (Text av betydelse för EES) OJ L 218, 13.8.2008, p. 30–47

[139] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), Artikel 48, sid 12

[140] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), Artikel 48

[141] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), Artiklarna 50 och 53

Enligt förslaget ska Enisa dessutom inrätta en ständig intressentgrupp för att, bland annat tillgodose förankring hos privata sektorn och andra berörda aktörer.[142] Den ständiga intressentgruppen ska bestå av erkända experter och branschföreträdare, konsumentgrupper, samt företrädare för behöriga myndigheter, dataskyddsmyndigheter och rättsvårdande myndigheter.[143] Intressentgruppens ska ge råd till Enisa avseende verksamhetsgenomförande och utarbetande av arbetsprogram. Dessa ska bland annat innehålla mål, resultat och resultatindikatorer för verksamheten).[144] Redan i dagsläget inhämtar Enisa, som är ansvarig myndighet för informationssäkerhet, expertis och råd från intressentgrupper.[145] Eftersom förslaget även avser vidareutveckling av standardisering bör det också påpekas att organisationerna som utarbetar standarder tenderar att förlita sig på återkoppling från experter inom berörda områden. Till exempel använder sig Comité Européen de Normalisation (CEN), som är verksamma inom IKT-standardisering, och Comité Européen de Normalisation Électrotechnique (CENELEC), som är verksamma inom elektronikstandardisering, av arbetsgrupper med experter i utkastframtagningsprocessen och tillåter även medverkan från observatörer i detta arbete.[146]

2.4.1 Cybersäkerhetsstandardisering av IKT-produkter och tjänster i smarta fordon och vägnät

Med cybersäkerhet avser förslaget om en cybersäkerhetsakt nödvändig verksamhet för att skydda nät- och informationssystem, deras användare och berörda personer från potentiella omständigheter och händelser som

[142] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), Skäl 44

[143] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), Artikel 20

[144] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), Artikel 20

[145] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), sid 18

[146] CEN CENLEC (2011) Internal Regulations – Part 2: Common Rules for Standardization Work

kan påverka systemen negativt.[147] Standardiseringen inom det så kallade europeiska systemet för cybersäkerhetscertifiering avser Europeiska unionens regler, tekniska krav, standarder och förfaranden som tillämpas på IKT-produkter och tjänster, det vill säga delar av nät- och informationssystem.[148]

De europeiska cybersäkerhetscertifikaten kommer kunna sökas av tillverkare för IKT-produkter och av leverantörer av IKT-tjänster.[149] I och med att det europeiska systemet för cybersäkerhetscertifiering även ska omfatta IKT i samhällsviktig verksamhet omfattar standardiseringen också IKT för vägmyndigheter och operatörer av intelligenta transportsystem (se del 2.3 ovan).[150] Som tidigare påvisats omfattas även IKT-tillverkare och IKT-tjänsteleverantörer som ansvarar för komponenter av uppkopplade och automatiserade fordon[151] av förslaget. Sannolikt kommer sektorsinriktade cybersäkerhetsinitiativ bli särskilt viktiga för tillämpningen av cybersäkerhetsstandarder inom fordon och vägnät.[152] Till vilken mån europeisk cybersäkerhetsstandardisering

[147] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), Artikel 2

[148] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), Artikel 2

[149] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), Artikel 12

[150] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), Artiklarna 2, 8, sid 2 och 90

[151] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), 8-9

[152] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), 88

kommer vara frivilligt eller bindande för verksamhet kopplad till smarta fordon och vägnät är ännu oklart.[153]

2.4.2 Säkerhetskrav inom den europeiska standardiseringen

Medan de specifika säkerhetskraven är tänkta att hämtas ur unionens regler, tekniska krav, standarder och förfaranden i sig,[154] innehåller förslaget om en cybersäkerhetsakt en övergripande ram med förutsättningar för cybersäkerhetscertifieringen. Bland annat inbegriper cybersäkerhetscertifieringen specificering av cybersäkerhetskrav, bedömningskriterier, metoder, och utvärdering, uppgifter som ska lämnas för certifiering, villkor för beviljande och bibehållande för certifiering, övervakning av certifiering, påföljder vid icke-överstämmelse med krav, samt bestämmelser om hur nyligen upptäckta sårbarheter ska rapporteras.[155] Certifieringen ska stödja tillgänglighet, autenticitet, integritet och konfidentialitet hos data, funktioner eller tjänster för nät- och informationssystem.[156] Certifieringen ska innehålla säkerhetsmål som ska gälla vid tillämpliga fall: [157]

- skydda data mot otillåten eller oavsiktlig behandling, ändring, förlust, och förstöring
- säkerställa begränsning av åtkomsträttigheter för personer, program och maskiner till data, tjänster och funktioner

[153] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), Artikel 48

[154] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), Artikel 2

[155] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), Artikel 47

[156] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), Artikel 43, Skäl 55

[157] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), Artikel 45

- registrera utlämning och tid för utlämning av data, tjänster och funktioner
- säkerställa möjligheten att kontrollera åtkomst till data, tjänster och funktioner
- återställa tillgängligheten till data, tjänster och funktioner vid incidenter
- mekanismer för att säker uppdatering av programvara med kända brister.

Det ska även innehålla tre assuransnivåer (ibland kallat säkerhetsgrader utanför lagstiftningen) med syfte att stärka förtroendet för IKT-produkter och tjänster genom öppenhet kring grundläggande kriterier för och utvärderingen av deras säkerhet.[158] Assuransnivåerna avser påstådda eller styrka cybersäkerhetsegenskaperna, tekniska specifikationer, standarder och förfaranden, inklusive tekniska kontroller för att minimera risken för incidenter.[159] Se tabell 6 för beskrivning av assuransnivåerna.

Tabell 6: Assuransnivåer.

Grundläggande	Certifikatet ger begränsad tillförlitlighet om cybersäkerhetsegenskaperna i IKT- produkter och tjänster
Betydande	Certifikatet ger betydande tillförlitlighet om cybersäkerhetsegenskaperna i IKT- produkter och tjänster
Hög	Certifikatet ger hög tillförlitlighet om cybersäkerhetsegenskaperna i IKT- produkter och tjänster

2.5 Säkerhetsskydd

Nyligen genomfördes omfattande säkerhetsskyddsreformer i Sverige (se tabell 8) för att återspegla den snabba utvecklingen av informations-teknologi och samhällets ökande behov av informationssäkerhet, fysisk säkerhet och personalsäkerhet.[160] Den nya säkerhetsskyddslagen (2018:585) och den nya säkerhetsskyddsförordningen (2018:658) trädde i

[158] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), Artikel 46, Skäl 33, 48, 50, 55 och 57, sid 3 fotnot 8

[159] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), Artikel 46

[160] En ny säkerhetsskyddslag SOU 2015:25, 17

kraft i april 2019 och Säkerhetspolisens föreskrifter om säkerhetsskydd[161] publicerades i Polismyndighetens författningssamling i februari 2019. Säkerhetsskyddet avser skydd av säkerhetskänslig verksamhet från brott som kan hota verksamheten, inklusive spionerи och terrorbrott, samt skydd av säkerhetsskyddsklassificerade uppgifter.[162]

Tabell 7: Säkerhetsskyddet.

Rättsakter och förslag	Säkerhetsskyddslag (2018:585)
	Säkerhetsskyddsförordning (2018:658)
	Offentlighets- och sekretesslagen (2009:400)
	Kompletteringar till den nya säkerhetsskyddslagen SOU 2018:82
	Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2
	Försvarsmaktens föreskrifter om säkerhetsskydd FFS 2019:2[163]

Säkerhetspolisen har särskilt ansvar för säkerhetsskyddet. Detta är ett generellt ansvar som grundar sig i Säkerhetspolisens ansvar för förebyggande och utredande åtgärder mot kontraspionage, kontraterror, säkerhetsskydd och personskydd.[164] Ansvaret innebär också att Säkerhetspolisen, bland annat, ska ge råd för att förebygga brotten, inklusive genom vägledningar och föreskrifter.[165] Transportstyrelsen utövar även viss tillsyn för säkerhetsskyddet i transportsektorn. Bestämmelserna i säkerhetsskyddsförordning (2018:658), som inbegriper tillsyn, och föreskriftsrätt, riktar sig däremot till luftfart och hamnskydd

[161] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2
[162] Säkerhetsskyddslag (2018:585), 2§
[163] Försvarsmaktens föreskrifter gäller inte för transportsektorn men innehåller likväl information om ytterligare lämpliga säkerhetsskyddsåtgärder
[164] En ny säkerhetsskyddslag SOU 2015:25, 184-186; Transportsstyrelsen. (2019). Säkerhetsskyddslagstiftning. Från: https://www.transportstyrelsen.se/sv/Om-transportstyrelsen/vart-uppdrag-och-arbetssatt/sakerhetsskyddslagstiftning/. Senast 25/06/2019.
[165] En ny säkerhetsskyddslag SOU 2015:25, 184-186; Transportsstyrelsen. (2019). Säkerhetsskyddslagstiftning. Från: https://www.transportstyrelsen.se/sv/Om-transportstyrelsen/vart-uppdrag-och-arbetssatt/sakerhetsskyddslagstiftning/. Senast 25/06/2019.

snarare än vägtrafik.[166] Som en del av lagstiftningsprocessen i säkerhetsskyddsreformerna inkom regeringen vid slutet av 2018 med ett tilläggsdirektiv för kompletteringar till nya säkerhetsskyddslagen.[167] Betänkandet om kompletteringar föreslår att en ändamålsenlig tillsyn för säkerhetsskyddet inom transportsektorn även ska omfatta vägtrafik.[168] Betänkandet uppmärksammar att inte hela ansvaret för transportsektorn i dagsläget vilar på Transportsstyrelsen. Istället ligger tillsynsansvaret för verksamhetsutövare inom vägtrafiken på länsstyrelserna. Betänkande föreslår därför att även ansvaret för tillsyn av vägtrafiken bör utövas av Transportstyrelsen.[169]

2.5.1 Säkerhetskänslig verksamhet kopplat till smarta fordon och vägnät

Säkerhetskänslig verksamhet är verksamhet som har betydelse för Sveriges säkerhet eller Sveriges internationella åtaganden.[170] Säkerhetskänslig verksamhet omfattar skyddsobjekt, det vill säga områden, anläggningar, byggnader och objekt som behöver ett förstärkt skydd mot sabotage, terror och spioneri, inklusive vissa elektroniska kommunikationer och transporter.[171] Säkerhetskänslig verksamhet omfattar även uppgifter, system och systemhantering med betydelse för Sveriges säkerhet.[172] Betänkandet om kompletteringar till säkerhetsskyddslagen förslår att skyddsvärden inom transportområdet ska innefatta styrsystem och infrastruktur som behövs för transport, i synnerhet centrala knytpunkter.[173] Eftersom behovet av säkerhetsskydd varierar från fall till fall är det den som bedriver säkerhetskänslig verksamhet som bedömer vilka funktioner inom verksamheten som behöver säkerhetsskydd.[174] Trafikverket påvisar i sin omvärldsanalys från 2018 att tilltagande digitalisering, cyberhot och terrorhot mot

[166] En ny säkerhetsskyddslag SOU 2015:25, 190-191; Säkerhetsskyddsförordning (2018:658), 1§, 7 kap; Transportsstyrelsen. (2019). Säkerhetsskyddslagstiftning. Från: https://www.transportstyrelsen.se/sv/Om-transportstyrelsen/vart-uppdrag-och-arbetssatt/sakerhetsskyddslagstiftning/. Senast 25/06/2019.
[167] Kompletteringar till den nya säkerhetsskyddslagen SOU 2018:82
[168] Kompletteringar till den nya säkerhetsskyddslagen SOU 2018:82, 361.
[169] Kompletteringar till den nya säkerhetsskyddslagen SOU 2018:82, 380
[170] Säkerhetsskyddslag (2018:585), 1§ 1 Kap
[171] En ny säkerhetsskyddslag SOU 2015:25, 22-23; Skyddslag (2010:305), 1 och 2§§ 1 Kap
[172] En ny säkerhetsskyddslag SOU 2015:25, 22-23
[173] Kompletteringar till den nya säkerhetsskyddslagen SOU 2018:82, 380
[174] En ny säkerhetsskyddslag SOU 2015:25, 23

transportsektorn, samt framtida autonomi i transporter, förmodligen kommer öka behovet av säkerhetsskydd inom sektorn.[175]

2.5.2 Säkerhetsskyddsklassificerade kopplat till smarta fordon och vägnät

Uppgifter som relaterar till säkerhetskänslig verksamhet och omfattas av sekretess är säkerhetsskyddsklassificerade uppgifter.[176] Begreppet omfattar alltså uppgifter av betydelse för Sveriges säkerhet eller internationella säkerhetsåtaganden.[177] Följaktligen omfattar säkerhetsskyddsklassificerade uppgifter på transportområdet sådana uppgifter som rör den säkerhetskänsliga verksamheten inom transportsektorn.[178] Uppgifterna är indelade i fyra säkerhetsklasser:

1. kvalificerat hemlig vid en synnerligen allvarlig skada
2. hemlig vid en allvarlig skada
3. konfidentiell vid en inte obetydlig skada
4. begränsat hemlig vid endast ringa skada.[179]

2.5.3 Krav på säkerhetsskydd

Säkerhetsskyddslagen medför ett antal säkerhetskrav. Genomförandet av kraven uppfylls genom ett antal åtgärder.

Genomför säkerhetsskyddsanalys. Den som bedriver säkerhetskänslig verksamhet ska minst vartannat år genomföra en dokumenterad säkerhetsskyddsanslys och därmed identifiera skyddsvärden[180] och utreda behovet av säkerhetsskydd.[181] Verksamhet kan vara skyddsvärd utifrån behov av konfidentialitet, tillgänglighet eller riktighet.[182] Säkerhetsskyddsanalysen ska dokumentera verksamhetens art, förekomsten av säkerhetsskyddsklassificerade uppgifter, övriga omständigheter och planerade säkerhetsskyddsåtgärderna.[183] Säkerhetsskyddsanalys ska även

[175] Trafikverket. (2018). *Trender i transportsystemet: Trafikverkets omvärldsanalys 2018.* Från: https://trafikverket.ineko.se/Files/en-US/51419/Ineko.Product.RelatedFiles/2018_180_trender_i_transportsystemet_trafikverkets_omv%C3%A4rldsanalys_2018.pdf. Senast 16/04/2019.
[176] Säkerhetsskyddslag (2018:585), 2§ 1 Kap; Se även offentlighets- och sekretesslagen (2009:400)
[177] En ny säkerhetsskyddslag SOU 2015:25, 22
[178] Kompletteringar till den nya säkerhetsskyddslagen SOU 2018:82, 380
[179] Säkerhetsskyddslag (2018:585), 5§ 2 Kap
[180] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 1§ 2 Kap
[181] Säkerhetsskyddslag (2018:585), 1§ 2 Kap
[182] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 4§ 2 Kap
[183] Säkerhetsskyddslag (2018:585), 1§ 2 Kap

identifiera övergripande sårbarheter för verksamheten.[184]Enligt Säkerhetspolisens förskrifter ska bedömningen av potentiell antagonistisk handling (exempelvis sabotage, terror och spionerі) mot skyddsvärdena kategoriseras enligt konsekvenskategorier (se tabell 8) och konsekvensnivåer (se tabell 9).[185]

Tabell 8: Konsekvenskategorier.

Konsekvenskategorier	Skada för Sveriges yttre säkerhet
	Skada för Sveriges inre säkerhet
	Skada på nationellt samhällsviktig verksamhet
	Skada för Sveriges ekonomi

Tabell 9: Konsekvensnivåer.

Nivå 5	Synnerligen allvarlig skada för Sveriges säkerhet
Nivå 4	Allvarlig skada för Sveriges säkerhet
Nivå 3	Inte obetydlig skada för Sveriges säkerhet
Nivå 2	Ringa skada för Sveriges säkerhet
Nivå 1	Inte mätbar eller inte relevant konsekvens med bäring på Sveriges säkerhet

Rapportera särskilt säkerhetskänslig verksamhet. Om konsekvenserna av en antagonistisk handling mot verksamheten ligger på nivå 4 (allvarlig skada) eller 5 (synnerligen allvarlig skada) ska verksamheten rapporteras till Säkerhetspolisen.[186] Säkerhetspolisen tillhandahåller verksamhetsutövarna hotbilder att använda i sina bedömningar.[187]

Upprätta en säkerhetsskyddsplan. Verksamhetsutövaren ska fastställa säkerhetsskyddsåtgärder genom en säkerhetsplan inom ramen för sin säkerhetsskyddsanalys. Åtgärderna fastställs utifrån de identifierade hoten och sårbarheterna.[188] Säkerhetsskyddsåtgärderna ska säkerställa informationssäkerhet, fysisk säkerhet, och personalsäkerhet.

[184] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 9§ 2 Kap
[185] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 2-3§§ 2 Kap
[186] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 6§ 2 Kap
[187] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 7§ 2 Kap
[188] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 11§ 2 Kap; Säkerhetsskyddsförordning (2018:658), 1§ 2 Kap; Säkerhetsskyddslag (2018:585), 1§ 2 Kap

Tabell 10: Informationssäkerhetsåtgärder.

Utveckling och framtagning	Se till att de som deltar i utveckling, framtagning och driftsättning besitter kompetens om systemets informationssäkerhet och sårbarheter.[189]
	Granska programvara för säkerhetsbrister och sårbarheter.[190]
Driftsättning	Samråd med Säkerhetspolisen innan driftsättning av informationssystem för att behandla säkerhetsskydds-klassificerade uppgifter.[191]
	Beakta säkerhetsskydds-klassificerade uppgifter innan driftsättning.[192]
	Testa och dokumentera om systemets säkerhetsåtgärder uppfyller säkerhetskrav.[193]
	Kontrollera att säkerhetsåtgärder enligt särskild bedömning har implementerats med avsedda effekter.[194]
	Dokumentera behov av resurser för säkerhetsskydd under systemets livstid.[195]
Hantering	Fastställ rutiner för informationssystemets hantering genom dess livstid.[196]
	Granska säkerheten årligen.[197]
	Anpassa säkerhetsåtgärder kontinuerligt mot hot och sårbarheter.[198]
	Vidta lämpliga åtgärder för att försvåra och hantera obehörig åtkomst, avlyssning och inverkan mot systemet.[199]
	Anteckna förekomsten av och inventera (årligen) säkerhetsskydds-klassificerade handlingar.[200]

Informationssäkerhet innebär att förebygga obehörig röjning, ändring, otillgängliggörande, eller förstöring av säkerhetsskyddsklassificerade uppgifter, samt att förebygga skadlig inverkan på informationssystem i

[189] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 3§ 4 Kap
[190] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 4 och 5§§ 4 Kap
[191] Säkerhetsskyddsförordning (2018:658), 2§ 3 Kap
[192] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 6§ 4 Kap
[193] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 7§ 4 Kap
[194] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 9§ 4 Kap; Säkerhetsskyddsförordning (2018:658), 5§ 3 Kap
[195] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 8§ 4 Kap
[196] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 10§ 4 Kap
[197] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 11§ 4 Kap
[198] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 2§ 4 Kap
[199] Säkerhetsskyddsförordning (2018:658), 4§ 3 Kap
[200] Säkerhetsskyddsförordning (2018:658), 7-8§§ 3 Kap

säkerhetskänslig verksamhet.[201] Säkerhetsskyddet inbegriper flera organisatoriska informationssäkerhetsåtgärder vid utveckling och framtagning, driftsättning och hantering av informationssystem (se tabell 10).

Säkerhetsskyddet för informationssystem innefattar även tillämpningen av ett antal tekniska åtgärder:

- Unika identiteter inom informationssystem som gör åtkomst spårbar till individ, system eller resurs.[202]
- Styrning så att behörigheter avseende system är restriktiva, tidsbegränsade, och så att uppföljning genomförs.[203]
- Autentisera med flera faktorer vid systemåtkomst, med tillämpning av administrativa regler för lösenordshantering och utformning, samt med det högsta säkerhetsskyddet för användning av systemets centrala funktioner för identifiering eller behörighetskontroll.[204]
- Skydd mot röjande signaler om uppgifterna i systemet är av konfidentiell eller högre klassificering.[205]
- Kontrollerad kommunikation mellan informationssystemet, andra informationssystem, nätverk, delsystem eller komponenter.[206]
- Separering av informationssystem som behandlar begränsat hemlig eller konfidentiell information (genom logisk separering) och hemlig eller kvalificerat hemlig information (genom fysisk separering och envägskommunikation vid dataimport och dataexport).[207]
- Kryptografiska funktioner om säkerhetsskyddsklassificerade uppgifter kommuniceras till system utanför verksamhetsutövarens kontroll, och för övrigt analysera behoven av kryptografi.[208]
- Konfigurationer för att avsluta systemfunktioner som inte används för att reducera sårbarheter.[209]

[201] Säkerhetsskyddslag (2018:585), 2§ 2 Kap
[202] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 12§ 4 Kap
[203] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 13§ 4 Kap
[204] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 14-17§§ 4 Kap
[205] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 18§ 4 Kap; Säkerhetsskyddsförordning (2018:658), 4§ 3 Kap
[206] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 19§ 4 Kap
[207] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 20-21§§ 4 Kap
[208] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 22§ 4 Kap; Säkerhetsskyddsförordning (2018:658), 5§ 3 Kap
[209] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 23§ 4 Kap

- Uppdatera programvara för att motverka sårbarheter.[210]
- Dokumentera logiska samband och beroenden mellan komponenter.[211]
- Dokumentera hårdvara, mjukvara och deras beroenden när de används för behandling av kvalificerat hemliga uppgifter.[212]
- Skydda mot skadlig kod.[213]
- Skydda mot och detektera obehörig ändring av uppgifter.[214]
- Detektera och skydda system som behandlar konfidentiell information (eller högre) mot intrång.[215]
- Logga händelser i systemet för att detektera obehörig åtkomst, påverkan och funktionsstörningar samt händelser av betydelse för den säkerhetskänsliga verksamheten.[216]
- Bevara loggar i minst 10 år (25 år vid skydd av kvalificerat hemliga uppgifter) samt skydda loggarna.[217]
- Övervaka system för att upptäcka incidenter i system med hemliga eller kvalificerat hemliga uppgifter.[218]
- Kontrollera årligen att säkerhetskopior av säkerhetsskydds-klassificerade uppgifter kan återskapas.[219]
- Skydda säkerhetsskyddsklassificerade uppgifter som lämnas till utländska aktörer genom internationella säkerhetsskydds-åtaganden, kryptografisk förbindelse eller Utrikesdepartementets kurirförbindelser.[220]

Fysisk säkerhet innebär att vidta åtgärder med funktioner som förebygger, upptäcker, försvårar eller hanterar obehörigt tillträde till och skadlig inverkan mot områden, byggnader och andra anläggningar eller objekt där det förekommer säkerhetsskyddklassificerade uppgifter.[221] Åtgärder för fysisk säkerhet omfattar bevakningspersonal, teknisk övervakning,[222] tillträdesbegränsning såsom fysiska barriärer, skyddsavstånd och

[210] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 24§ 4 Kap
[211] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 25§ 4 Kap
[212] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 26§ 4 Kap
[213] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 27§ 4 Kap
[214] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 28§ 4 Kap
[215] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 29§ 4 Kap
[216] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 30-31§§ 4 Kap
[217] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 34-35§§ 4 Kap
[218] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 36-37§§ 4 Kap
[219] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 38§ 4 Kap
[220] Säkerhetsskyddsförordning (2018:658), 9-10§§ 3 Kap
[221] Säkerhetsskyddslag (2018:585), 3§ 2 Kap; Säkerhetsskyddsförordning (2018:658), 1§ 4 Kap; Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 5 Kap
[222] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 2§ 5 Kap

byggnadsteknisk förstärkning,[223] behörighetskontroll vid tillträde,[224] passersystem med förteckning över och krav på hantering av kort, koder och nycklar,[225] samt ingripande av väktare, vakt och polis vid incident.[226]

Personalsäkerhet avser åtgärder som säkerställer att endast personal som är pålitlig och har tillräcklig kunskap har tillgång till säkerhetsskydds-klassificerade uppgifter och deltar i den säkerhetskänsliga verksamheten.[227] Dessa åtgärder inbegriper registerkontroll och personutredning,[228] säkerhetsprövning för anställning och för att den anställde ska placeras i säkerhetsklass,[229] säkerhetssamtal vid anställning,[230] personalutbildning i säkerhetsskydd,[231] samt avanmälan av anställning eller deltagande i säkerhetsskyddad verksamhet.[232]

Genomför särskild säkerhetsskyddsbedömning vid förändrad hotbild. Om en förändring av hotbilden betydligt kan påverka verksamheten, ska verksamhetsutövaren genomföra en särskild säkerhetsskyddsbedömning. Förändringar av hotbild kan bland annat orsakas av ändringar i säkerhetskänsliga system och upphandling inom säkerhetskänslig verksamhet.[233]

Upphandla med säkerhetsskyddsavtal. Myndigheter, landsting, kommuner och enskilda verksamhetsutövare ska ange säkerhets-skyddskrav i ett säkerhetsskyddsavtal vid upphandling av varor, tjänster eller byggentreprenader om detta involverar säkerhetskänslig verksamhet eller säkerhetsskyddsklassificerade uppgifter (som är konfidentiella eller har högre klassning).[234]

Anmäl säkerhetshotande händelser. Säkerhetshotande händelser såsom röjning av säkerhetsskyddsklassificerade uppgifter, IT-incidenter i

[223] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 3§ 5 Kap
[224] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 5§ 5 Kap
[225] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 6-8§§ 5 Kap
[226] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 4§ 5 Kap
[227] Säkerhetsskyddslag (2018:585), 4§ 2 Kap;
[228] Säkerhetsskyddslag (2018:585), 3 Kap; Säkerhetsskyddsförordning (2018:658), 12-21§§ 5 Kap; Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 7-14§§ 6 Kap
[229] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 1-3§§ 6 Kap; Säkerhetsskyddsförordning (2018:658), 2-11§§ 5 Kap
[230] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 4 och 6§§ 6 Kap
[231] Säkerhetsskyddsförordning (2018:658), 1§ 5 Kap; Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 5§ 6 Kap
[232] Säkerhetsskyddsförordning (2018:658), 22§ 5 Kap
[233] Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 12§ 2 Kap
[234] Säkerhetsskyddslag (2018:585), 6§ 2 Kap; Säkerhetsskyddsförordning (2018:658), 5-8§§ 2 Kap

informationssystem för säkerhetskänslig verksamhet, eller misstanke om annat hot ska skyndsamt meddelas till Säkerhetspolisen.[235]

Tillämpa tystnadsplikt. Personal som tagit del av säkerhetsskydds-klassificerade uppgifter eller deltagit i säkerhetskänslig verksamhet får inte obehörigen röja eller utnyttja uppgifterna.[236]

2.6 Intelligenta transportsystem

Intelligenta transportsystem (ITS) är system för infrastruktur, trafikledning, fordon, användare, mobilitetshantering, samt gränssnitt mot andra transportslag som tillämpar informations-och kommunikations-teknologi.[237] ITS-direktivet (direktiv 2010/40/EU med svensk implementering (Lag 2013:315) syftar bland annat till att bestämmelser kring framställande av specifikationer och åtgärder (inklusive för säkerhet) för ITS och dess gränssnitt mot andra transportslag.[238] Systemens säkerhet är en central del av ITS-regleringen. ITS-tillämpningar som stödjer trafiksäkerhet samt kontinuitet i trafikledning och godstransporter är ett av de prioriterade områdena där sådana bestämmelser ska utarbetas.[239] Tillhandahållandet av en ITS-tjänst innefattar per definition en ITS-tillämpning för att bidra till ökad säkerhet.[240] Den svenska myndighet som kan arbeta fram föreskrifter inom ITS-området är Transportstyrelsen.[241] Artikel 10 av ITS-direktivet lägger dessutom fram bestämmelser om personlig integritet och säkerhet. Samverkande ITS (C-ITS) omfattar system som exempelvis fordon som

[235] Säkerhetsskyddsförordning (2018:658), 10-11§§ 2 Kap
[236] Säkerhetsskyddslag (2018:585), 1-2§§ 5 Kap
[237] 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 Text av betydelse för EES OJ L 207, 6.8.2010, p. 1–13, Artikel 4; Lag (2013:315) om intelligenta transportsystem vid vägtransporter, 3§
[238] 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 Text av betydelse för EES OJ L 207, 6.8.2010, p. 1–13, Artikel 4; Lag (2013:315) om intelligenta transportsystem vid vägtransporter, 2§
[239] 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 Text av betydelse för EES OJ L 207, 6.8.2010, p. 1–13, Artikel 2
[240] 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 Text av betydelse för EES OJ L 207, 6.8.2010, p. 1–13, Artikel 4
[241] Förordning (2016:383) om intelligenta transportsystem vid vägtransporter, 8 §

kan kommunicera med väginfrastrukturen eller direkt med varandra.[242] Inom ramen för kommissionens delegerade förordning (EU) (ej ännu gällande) omfattar samverkande ITS sådana system som använder unionens förvaltningssystem för säkerhetsbehörighetsuppgifter och möjliggör utbyten av säkra och tillförlitliga meddelanden mellan ITS-användare.[243] Syftet bakom den delegerade förordningen är att främja säkerhet[244] och kontinuitet.[245] Under sommaren 2019 invände Europeiska unionens råd mot den delegerade förordningen om samverkande ITS. Orsaken verkar närmast vara kopplad till lagstiftningsprocessen och att lagen inte anses vara neutralt formulerad och därför påverkar vissa system, teknologier och industrier mer än andra.[246] Även om läget för e-Privacy är osäkert för tillfället verkar det alltså inte som invändningarna mot förslaget är kopplade till säkerhetskravet. Det är även viktigt att påpeka att även om NIS-direktivet identifierar operatörer av intelligenta transportsystem som leverantörer av samhällsviktiga tjänster, är säkerhetsbestämmelser inom ITS-lagstiftningen kompletterande till de generella säkerhetskraven i NIS-lagstiftningen.[247] Lagarna som denna analys utgår ifrån redovisas i tabell 11.

[242] Europeiska kommissionen (2016) MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET, RÅDET, EUROPEISKA EKONOMISKA OCH SOCIALA KOMMITTÉN SAMT REGIONKOMMITTÉN: En europeisk strategi för samverkande intelligenta transportsystem, en milstolpe mot samverkande, uppkopplad och automatiserad rörlighet, COM(2016) 766 final, 3

[243] KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/… av den 13.3.2019 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller införande och operativ användning av samverkande intelligenta transportsystem, C(2019) 1789 final, Artikel 2

[244] KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/… av den 13.3.2019 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller införande och operativ användning av samverkande intelligenta transportsystem, C(2019) 1789 final, 1

[245] KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/… av den 13.3.2019 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller införande och operativ användning av samverkande intelligenta transportsystem, C(2019) 1789 final, Artikel 1

[246] 5GAA. (2019). *5GAA welcomes Council objection against C-ITS Delegated Act.* Från: https://5gaa.org/news/5gaa-welcomes-council-objection-against-c-its-delegated-act/. Senast 30/09/2019.

[247] KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/… av den 13.3.2019 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller införande och operativ användning av samverkande intelligenta transportsystem, C(2019) 1789 final, Skäl 6

Tabell 11: Intelligenta transportsystem.

Rättsakter och förslag	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 Text av betydelse för EES
	Kommissionens Delegerade Förordning (EU) …/… av den 13.3.2019 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller införande och operativ användning av samverkande intelligenta transportsystem, C(2019) 1789 final
	Kommissionens beslut 2008/671/EG av den 5 augusti 2008 om harmoniserad användning av radiospektrum i frekvensbandet 5 875–5 905 MHz för säkerhetsrelaterade tillämpningar i intelligenta transportsystem (ITS) (EUT L 220, 15.8.2008, s. 24)
	Kommissionens delegerade förordning (EU) nr 305/2013 av den 26 november 2012 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU avseende harmoniserat tillhandahållande av interoperabelt EU-omfattande eCall Text av betydelse för EES EUT L 91, 3.4.2013, s. 1–4
	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 Text av betydelse för EES EUT L 247, 18.9.2013, s. 6–10
	Kommissionens delegerade förordning (EU) nr 885/2013 av den 15 maj 2013 om komplettering av Europaparlamentets och rådets ITS-direktiv 2010/40/EU vad gäller tillhandahållande av informationstjänster för säkra och skyddade parkeringsplatser för lastbilar och kommersiella fordon Text av betydelse för EES EUT L 247, 18.9.2013, s. 1–5
	Kommissionens delegerade förordning (EU) 2015/962 av den 18 december 2014 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller tillhandahållande av EU-omfattande realtidstrafikinformationstjänster (Text av betydelse för EES) EUT L 157, 23.6.2015, s. 21–31
	Lag (2013:315) om intelligenta transportsystem vid vägtransporter
	Förordning (2016:383) om intelligenta transportsystem vid vägtransporter

2.6.1 ITS-tillämpningar, tjänster och leverantörer

Cybersäkerhetsreglerna inom ITS-rätten avser främst ITS-tillämpningar, ITS-tjänster, och C-ITS-stationer. Det betyder att de omfattar operativa instrument för att applicera ITS (tillämpningarna) och tillhandahållandet

av tillämpningarna (tjänster).[248] De inbegriper även hårdvaru- och programvarukomponenterna för säkra och tillförlitliga meddelanden som möjliggör tillhandahållandet av C-ITS-tjänster (stationer).[249] Ansvaret för säkerheten åligger vanligen privata och offentliga leverantörer av ITS-tjänster,[250] fysiska eller juridiska personer som tillverkar C-ITS-stationer (tillverkare), personer som driftsätter (operatörer), importerar till Europa (importör) eller annan person i leveranskedjan (distributör) för stationerna.[251]

2.6.2 Krav på säkerhet inom ITS och samverkande ITS

Sedan ITS-direktivet från 2010 har säkerhetskraven för ITS till stor del hämtats utifrån andra lagrum, exempelvis för produktsäkerhet och dataskydd. Den rättsliga cybersäkerhetsregleringen skulle ha blivit stärkt i och med delegerade förordningen om samverkande ITS (C(2019) 1789 final) som stoppades i Europeiska unionens råd. Sammantaget innehåller ITS-rätten följande säkerhetskrav:

[248] 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 Text av betydelse för EES OJ L 207, 6.8.2010, p. 1–13, Artikel 4

[249] KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/… av den 13.3.2019 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller införande och operativ användning av samverkande intelligenta transportsystem, C(2019) 1789 final, Artikel 2

[250] 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 Text av betydelse för EES OJ L 207, 6.8.2010, p. 1–13, Artiklarna 4, 10, Bilaga 1

[251] KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/… av den 13.3.2019 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller införande och operativ användning av samverkande intelligenta transportsystem, C(2019) 1789 final, Artikel 2

Inför ITS-tillämpningar och tjänster som uppfyller produkt-säkerhetskrav enligt gällande europeisk rätt för produktansvar, inklusive säkerhetsregler relaterade till CE-märkning.[252]

Behandla personuppgifter i enlighet med dataskyddet vilket även omfattar dataskyddets- och lagen om elektronisk kommunikations säkerhetsrelaterade bestämmelser (se del 2.2 om dataskydd i denna rapport). Det innefattar även användning av uppgiftsminimering samt pseudonymiserings- och anonymiseringstekniker i enlighet med dataskyddet.[253]

Särskilda säkerhetskrav för C-ITS och C-ITS-stationer. Den delegerade förordningen om samverkande ITS (C(2019) 1789 final), som stoppades in Europeiska unionens råd, medför de mest omfattande och

[252] 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 Text av betydelse för EES OJ L 207, 6.8.2010, p. 1–13, Artikel 11; Lag (2013:315) om intelligenta transportsystem vid vägtransporter, 8§; KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/… av den 13.3.2019 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller införande och operativ användning av samverkande intelligenta transportsystem, C(2019) 1789 final, Skäl 14, 25; Kommissionens delegerade förordning (EU) nr 885/2013 av den 15 maj 2013 om komplettering av Europaparlamentets och rådets ITS-direktiv 2010/40/EU vad gäller tillhandahållande av informationstjänster för säkra och skyddade parkeringsplatser för lastbilar och kommersiella fordon Text av betydelse för EES EUT L 247, 18.9.2013, s. 1–5, Skäl 12

[253] 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 Text av betydelse för EES OJ L 207, 6.8.2010, p. 1–13, Artikel 10; KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/… av den 13.3.2019 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller införande och operativ användning av samverkande intelligenta transportsystem, C(2019) 1789 final, Skäl 23; Lag (2013:315) om intelligenta transportsystem vid vägtransporter, 8§; Kommissionens delegerade förordning (EU) nr 305/2013 av den 26 november 2012 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU avseende harmoniserat tillhandahållande av interoperabelt EU-omfattande eCall Text av betydelse för EES EUT L 91, 3.4.2013, s. 1–4, Artikel 6; 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 Text av betydelse för EES EUT L 247, 18.9.2013, s. 6–10, Skäl 5; Kommissionens delegerade förordning (EU) nr 885/2013 av den 15 maj 2013 om komplettering av Europaparlamentets och rådets ITS-direktiv 2010/40/EU vad gäller tillhandahållande av informationstjänster för säkra och skyddade parkeringsplatser för lastbilar och kommersiella fordon Text av betydelse för EES EUT L 247, 18.9.2013, s. 1–5, Skäl 11; Kommissionens delegerade förordning (EU) 2015/962 av den 18 december 2014 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller tillhandahållande av EU-omfattande realtidstrafikinformationstjänster (Text av betydelse för EES) EUT L 157, 23.6.2015, s. 21–31, Skäl 9

omvälvande reglerna för cybersäkerhet inom ITS-rätten. Den delegerade förordningen om samverkande ITS (C-ITS) inbegriper säkerhetskrav och rekommendationer, särskilt för tillverkare, importörer, distributörer och operatörer av C-ITS-stationer. Som bilaga till förordningen om samverkande ITS medföljer även certifierings- och säkerhetspolicy. Säkerhetspolicyn[254] innefattar regler för C-ITS-stationsoperatörers (och tillverkares) strategi för informationssäkerhet, klassificering av information avseende säkerhetsmål, riskbedömning och riskhantering. Certifieringspolicyn[255] som är bindande för betrodda europeiska C-ITS-system, framställer en tillitsmodell för C-ITS-stationer. Tillitsmodellen inbegriper bland annat kryptering med publik nyckel (PKI) och förvaltningen av certifikat, minimikrav för lokala säkerhetsrutiner, tekniska säkerhetsrutiner, operativa rutiner med mera. Det ligger inte inom ramen för denna rapport att gå igenom de detaljerade säkerhetskraven för C-ITS-stationer utifrån dessa (mycket omfattande) policys. De bindande säkerhetskraven utifrån den delegerade förordningen är som följer:

- Tillverkare och importörer av C-ITS-stationer ska skydda konsumenternas säkerhet utifrån de risker som stationerna förorsakar.[256]
- Tillverkare, importörer och distributörer av C-ITS-stationer ska se till att lättbegripliga och tydliga säkerhetsföreskrifter medföljer stationerna.[257]

[254] KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/… av den 13.3.2019 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller införande och operativ användning av samverkande intelligenta transportsystem, C(2019) 1789 final, Annex 4

[255] KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/… av den 13.3.2019 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller införande och operativ användning av samverkande intelligenta transportsystem, C(2019) 1789 final, Annex 3

[256] KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/… av den 13.3.2019 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller införande och operativ användning av samverkande intelligenta transportsystem, C(2019) 1789 final, artiklarna 7 och 9

[257] KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/… av den 13.3.2019 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller införande och operativ användning av samverkande intelligenta transportsystem, C(2019) 1789 final, artiklarna 7, 9 och 10

- Distributörer av C-ITS-stationer ska informera tillverkare och importörer om deras stationer utgör en risk samt underrätta unionens medlemsstater och marknadskontrollsmyndigheter.[258]
- C-ITS-stationsoperatörer ska, innan stationen tas i bruk, bland annat se till at stationen är CE-märkt, innehar tillämplig dokumentation (exempelvis angående certifieringspolicyn), är certifierad enligt säkerhetspolicyn, att den är autentiserad enligt EU:s förvaltningssystem för säkerhetsbehörighetsuppgifter för C-ITS med mera.[259]
- C-ITS-stationsoperatörer ska tillämpa ett system för hantering av informationssäkerhet i enlighet med ISO/IEC 27001 och säkerhetspolicyn samt erhålla certifiering i enlighet med policyn.[260]

Medlemsstaternas marknadskontrollsmyndigheter kan utvärdera C-ITS-stationer enligt tillämpliga säkerhetskrav, ålägga aktörer korrigerande åtgärder om stationen inte uppfyller kraven eller om myndigheten identifierar risker med stationen.[261] EU:s förvaltningssystem för säkerhetsbehörighetsuppgifter för C-ITS ska autentisera alla C-ITS-stationer enligt certifierings-och säkerhetspolicyn.[262] Kommissionen får fatta beslut och tillfälliga åtgärder för att avhjälpa nödsituationer som riskerar C-ITS-nätets korrekta fungerande, cybersäkerhet, integritet och tillgänglighet.[263]

[258] KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/… av den 13.3.2019 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller införande och operativ användning av samverkande intelligenta transportsystem, C(2019) 1789 final, artikel 10

[259] KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/… av den 13.3.2019 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller införande och operativ användning av samverkande intelligenta transportsystem, C(2019) 1789 final, artikel 22

[260] KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/… av den 13.3.2019 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller införande och operativ användning av samverkande intelligenta transportsystem, C(2019) 1789 final, artiklarna 27 och 28

[261] KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/… av den 13.3.2019 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller införande och operativ användning av samverkande intelligenta transportsystem, C(2019) 1789 final, artiklarna 17 och 19

[262] KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/… av den 13.3.2019 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller införande och operativ användning av samverkande intelligenta transportsystem, C(2019) 1789 final, artikel 23

[263] KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/… av den 13.3.2019 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller införande och operativ användning av samverkande intelligenta transportsystem, C(2019) 1789 final, artikel 30

2.7 Produktansvar och produktprövning

En grundläggande princip är att ett fordon, självkörande eller ej, behöver vara godkänd för att föras fram på offentliga vägar. Europeiska unionen har en omfattande reglering av både produktansvar och produktprövning som både syftar till att främja och harmonisera den inre marknaden samt skydda konsumenterna. Det bör noteras att även om automatiska funktioner i fordon är tillåtna, får fordon inte köras på vägarna utan mänsklig tillsyn (kontroll). Ett flertal initiativ har under de senaste åren utforskat möjligheterna till fullständig autonomi, dvs. förarlösa lösningar, inom ramarna för Wienkonventionen om vägtrafik och Genevekonventionen för vägtrafik. Uppdateringen av Wienkonventionen som genomfördes under 2014 avsåg att reglera ”system som påverkar hur fordon körs.” Uppdateringen resulterade dock inte i en tillåtelse för autonoma fordon i internationell trafik, utan i ett fastställande av kravet på en mänsklig förare som bibehåller kontroll över fordonet. I praktiken innebär det att fordon får vara intelligenta och autonoma, men inte utan mänsklig kontroll. De automatiserade systemen bibehåller på så sätt en assisterande funktion, och den mänskliga föraren är även i fortsättningen den sista säkerhetsbarriären. Ett flertal rättsakter reglerar området, dessa har sammanställts i Tabell 12.

G7-deklaration om automatiserad och uppkopplad körning inrymmer både intelligenta och automatiserade fordon, men omfattar inte autonom eller förarlös körning. Inte heller EU:s strategi på det prioriterade ITS-området omfattar autonomi. De rättsliga förutsättningarna för förarlös trafik saknas för närvarande inom EU, vilket innebär både avsaknaden av tillämpliga trafikregler och regleringar för säker teknologi.

Automatisering med inte autonomi är även en princip som gäller för bestämmelserna om produktprövning. Produktprövningen av motorfordon regleras i ramdirektivet 2007/46/. För serieproducerade fordon innebär detta att komponenterna, eller fordonen i sin helhet, ska vara typgodkända. Genom att utfärda ett typgodkännande intygar en medlemsstat att en typ av fordon, system[264], komponent eller teknisk enhet uppfyller vissa administrativa och tekniska krav. Typgodkännande kan vara nationellt (och gäller då enbart i det medlemslandet) eller internationellt. I praktiken innebär detta att motorfordon på den europeiska marknaden innehar EG-typgodkännande, det vill säga uppfyller direktivets administrativa och tekniska krav.[265] I Sverige är

[264] Med system menas ett flertal komponenter eller tekniska enheter som tillsammans bildar ett helhetligt system.

[265] För två- eller trehjuliga motorfordon gäller direktiv 2002/24/EG och direktiv 2003/37/EG reglerar EG-typgodkännanden för jordbruks- och skogsbrukstraktorer

Transportstyrelsen den myndigheten som utfärdar typgodkännande, vilket etableras genom fordonslag (2002:547) och fordonsförordningen (2009:211). Prövningen för typgodkännande genomförs av företag som i sin tur är ackrediterade av SWEDAC. Transportstyrelsen har i sin tur meddelat bland annat föreskrifter om nationellt typgodkännande av fordon (TSFS 2017:77).

Tabell 12: Produktansvar.

Rättsakter	Wienkonventionen om vägtrafik (8 november 1968) UNTS vol. 1042
	Genevekonventionen för vägtrafik (19 september 1949) UNTS vol. 125
	Europaparlamentets och rådets direktiv 2007/46/EG om fastställande av en ram för godkännande av motorfordon och släpvagnar till dessa fordon, samt av system, komponenter och separata tekniska enheter som är avsedda för sådana fordon (av den 5 september 2007)
	Rådets direktiv 85/374/EEG om tillnärmning av medlemsstaternas lagar och andra författningar om skadeståndsansvar för produkter med säkerhetsbrister (av den 25 juli 1985)
	FN/ECE Föreskrift 79
	FN/ECE Föreskrift 13-H
	FN/ECE Föreskrift 6[266]
	FN/ECE Föreskrift 48[267]
	Europaparlamentets och rådets direktiv 2001/95/EG om allmän produktsäkerhet (av den 3 december 2001)
	Europaparlamentets och rådets förordning 78/2009 om typgodkännande av motorfordon med avseende på skydd av fotgängare och andra oskyddade trafikanter
	Europaparlamentets och rådets förordning 79/2009 om typgodkännande av vätgasdrivna motorfordon
	Europaparlamentets och rådets förordning 661/2009
	Fordonslag (2002:547)
	Fordonsförordning (2002:925)
	Transportstyrelsens föreskrifter om nationellt typgodkännande av fordon (TSFS 2017:77)
	Transportstyrelsens föreskrifter och allmänna råd om kontrollbesiktning (2017:54)
	Trafikskadelag (1975:1410)
	Skadeståndslag (1972:207)
	Produktsäkerhetslag (2004:451)

Ramdirektivet 2007/46/EEG innehåller inga tekniska krav utan hänvisar till föreskrifterna utfärdade av Förenta nationernas ekonomiska kommission för Europa (FN/ECE). ECE-föreskrifterna i sin tur tillhandahåller tekniska krav för, i stort sett, samtliga komponenter som kan ingå i ett motorfordon: från dörrgångjärn[268] till hjulskydd.[269] Vid närmare betraktelse blir tydligt att ECE-reglementet inte är oproblematiskt i sitt förhållande till självförande fordon, vilket i synnerhet gäller föreskriften 79[270] som definierar tekniska krav för ett fordons styrutrustning: system med avancerad förarassistans, som inkluderar automatiskt kontrollerad styrfunktion och korrigerande styrfunktion. Här tar utvecklingen inte steget mot att tillåta en fullständig autonomi. Tvärtom, så har det i den senaste uppdateringen av föreskrifterna tillkommit krav på akustisk och visuell varning av föraren om att fordonet påverkas av automatisk funktionalitet så som korrigering av fordonets körriktning vid avvikelser från körfältet, samt på kontroll av förarens beredskap att återta kontroll över fordonet.[271] Detta innebär i praktiken att de reglerade systemen begränsas till att komplettera styrsystemet och hjälper föraren vid körningen. Den assisterande funktionen bekräftas ytterligare med antagandet om att körriktningsvisare styrs av människan, vilket i praktiken förbjuder automatisk signalering. Funktionen som står utanför de restriktiva kraven är den automatiska inbromsningen. På övergripande nivå består dock kravet på optisk och akustisk varning av föraren då automatiserade funktioner aktiveras. Det bör dock påpekas att regleringen är mindre restriktiv vid hastigheter under 10 km/h och därmed tillåter bl.a. att bilen parkerar självständigt utan att föraren behöver befinna sig i bilen.

ECE-föreskrift 79 etablerar även krav på dokumentation som inkluderar en förklaring av systemets funktion(er) och säkerhetskoncept enligt tillverkarens konstruktion. ECE-föreskrift Nr 13-H behandlar bland annat automatiskt styrd bromsning och förskriftens bilaga 8 uppställer

[266] Innehåller i dagsläget inga tydliga krav för automatiserad funktionalitet
[267] Innehåller i dagsläget inga tydliga krav för automatiserad funktionalitet
[268] Rådets direktiv 70/387/EEG av den 27 juli 1970 om tillnärmning av medlemsstaternas lagstiftning om dörrar på motorfordon och släpvagnar till dessa fordon
[269] Rådets direktiv 78/549/EEG av den 12 juni 1978 om tillnärmning av medlemsstaternas lagstiftning om hjulskydd på motorfordon; Europaparlamentets och rådets direktiv 95/28/EG av den 24 oktober 1995 om brinnegenskaperna hos material som används i inredningen till vissa kategorier av motorfordon
[270] Föreskrifter nr 79 från Förenta nationernas ekonomiska kommission för Europa (FN/ECE) – Enhetliga bestämmelser om godkännande av fordon med avseende på styrutrustning Addendum 78: Föreskrifter nr 79 Revision 2
[271] Föreskrifter nr 79 från Förenta nationernas ekonomiska kommission för Europa (FN/ECE) – Enhetliga bestämmelser om godkännande av fordon med avseende på styrutrustning

omfattande krav på dokumentation som ska tillhandahållas för automatiskt styrd bromsning. Till exempel ska det finnas beskrivningar av systemets funktioner, innefattande systemets kontrollfunktioner och mekanismer för kontroll, insignalsvariabler, avkända variabler, och driftsintervaller, utsignalvariabler, och även gränserna för funktionell drift och påverkan på prestanda.[272] Tillverkarens säkerhetskoncept ska även klargöras, det vill säga genom en deklaration som förklarar systemets utformningsstrategi under felfria förhållanden som inte kommer att äventyra säker drift, och en förklaring av mjukvaruarkitekturen, metoder och verktyg som har använts under konstruktion samt en redogörelse för systemlogikens implementation.[273] Funktionaliteten ska även göras transparent och förklaras med ett dokumentationspaket som även innehåller information om:[274]

- systemets utformning och scheman
- komponentförteckning
- enheternas funktioner och signalsammankopplingar med andra enheter
- scheman för mekaniska, pneumatiska och elektriska sammankopplingar
- signalflöde och prioritet
- identifiering av enheterna.

Vidare etableras krav för kontroller och prövningar av prestanda som avses ingå i procedurerna för godkännande i tillverkningen. Önskemålet om att bibehålla transparens och mänsklig kontroll över fordonet är också fastslaget i ECE-föreskrifternas syftesförklaring. Samtidigt som föreskrifterna etablerar krav för att funktionerna ska vara transparenta för föraren, råder osäkerhet vad gäller transparensen för andra trafikanter. Föreskrifterna 6 och 48, till exempel, reglerar ljusanordningar och körriktningsvisare, det vill säga sådana komponenter som tyds av andra trafikanter än föraren, men det är oklart huruvida dessa föreskrifter kan tillämpas för automatiserade varianter av dessa komponenter.

Produktansvaret regleras på EU-nivå genom rådets direktiv 85/374/EEG om tillnärmning av medlemsstaternas lagar och andra författningar om skadeståndsansvar för produkter med säkerhetsbrister[275] och av Europaparlamentets och rådets direktiv 2001/95/EG om allmän

[272] Föreskrift nr Nr 13-H, Bilaga 8
[273] Föreskrift nr Nr 13-H, Bilaga 8
[274] Föreskrift nr Nr 13-H, Bilaga 8
[275] Rådets direktiv 85/374/EEG av den 25 juli 1985 om tillnärmning av medlemsstaternas lagar och andra författningar om skadeståndsansvar för produkter med säkerhetsbrister

produktsäkerhet.[276] Dessa direktiv är dock författade på en generell nivå och innehåller inga närmare specifikationer gällande fordon eller cybersäkerhet. I EU-kommissionens rapport om tillämpningen av rådets direktiv 85/374/EEG[277] uppmärksammas svårigheten i att tillämpa direktivet i den moderna industrins realiteter i koncepten så som ”produkt” och ”säkerhetsbrist”, bland annat med hänvisning till att det är allt fler leverantörer som bidrar till varje produkt. Rapporten påpekar också att cybersäkerhetsfrågor behöver klargöras. För att direktivet även i framtiden ska kunna tillämpas ämnar kommissionen därför att ge ut en vägledning för hur direktivet ska tillämpas, i synnerhet gällande AI och robotteknik. Vägledningen utlovades för mitten av 2019, men har vid tidpunkten för skrivningen av denna rapport ännu inte utgivits.

I Sverige omsätts direktiven för skadeståndsansvar och produktsäkerhet genom skadeståndslagen (1972:207) och trafikskadelagen (1975:1410) respektive produktsäkerhetslagen (2004:451). Skadeståndslagen är subsidiär till trafikskadelagen när det gäller *skada i följd av trafik med motordrivet fordon som vållats av fordonets förare, i den mån trafikskadeersättning kan utgå för skadan enligt trafikskadelagen*.[278]. Då det är potentiellt möjligt att ett uppkopplat fordon orsakar skada utan att vara i trafik, t.ex. genom att dess uppkoppling utnyttjas för ett DDoS-angrepp, kan skadeståndslagen i framtiden bli mer relevant i fordonssammanhang.

Enligt gällande lag blir en tillverkare (eller importör till EES) skadeståndsskyldig vid brister. Dock inte om säkerhetsbristen inte fanns då produkten sattes i omlopp, och inte heller om det vid lanseringen av produkten inte var möjligt att upptäcka bristen enligt det då rådande vetenskapliga eller tekniska vetandet.[279] Dessa avgränsningar kan vara svårförenliga med hur cybersäkerhetsbrister kan uppträda. Nya angrepps-tekniker utvecklas snabbt och kan vara svåra att fånga upp proaktivt. Till exempel har luftgap, det vill säga fysisk separation mellan en skyddsvärd dator och nätverk, länge ansetts vara en nästan ofelbar säkerhetsåtgärd. Med tiden har det dock utvecklats metoder för att kringgå luftgapet, till

[276] Europaparlamentets och rådets direktiv 2001/95/EG av den 3 december 2001 om allmän produktsäkerhet (Text av betydelse för EES) *Europeiska gemenskapernas officiella tidning nr L 011 , 15/01/2002 s. 0004 - 0017*

[277] REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC) COM/2018/246 final.

[278] Skadeståndslag (1972:207) Kapitel 3 8§

[279] Produktsäkerhetslag (2004:451)

exempel genom analys av elektromagnetiska impulser som uppstår då den skyddade datorn är i drift. Även vid användning av s.k. zero day-sårbarheter, d.v.s. sårbarheter som tills de missutnyttjas har varit i stort sett helt okända för tillverkaren, kan liknande argument framföras. Samtidigt bör tillverkarnas skyldighet att ”bedriva ett förebyggande produktsäkerhetsarbete i syfte att få kännedom om skaderisker hos de varor som de tillhandahåller eller har tillhandahållit”[280] noteras. Det finns en skyldighet att rapportera säkerhetsbristen till lämplig tillsynsmyndighet. Samtidigt kan ägaren till produkten inte tvingas att åtgärda säkerhetsproblemet[281] utan enbart informeras om att det existerar. Vid allvarlig säkerhetsbrist i ett fordon skulle då istället fordonslagen och fordonsförordningen behöva tillämpas för att Transportstyrelsen skulle få möjlighet att ålägga fordonsägaren att åtgärda felet och förvisa fordonet för ombesiktning eller meddela körförbud.[282]

2.7.1 Framtida utveckling

För närvarande föreligger ett antal initiativ som skulle möjliggöra en större automatisering och autonomi i vägtrafiken. En förordning, föreslagen av Europaparlamentet och Europarådet, avser upphäva förordningarna (EG) nr 78/2009 om typgodkännande av motorfordon med avseende på skydd av fotgängare och andra oskyddade trafikanter […], nr 79/2009 om typgodkännande av vätgasdrivna motorfordon, samt nr 661/2009 om typgodkännande av allmän säkerhet hos motorfordon och deras släpvagnar samt av de system, komponenter och separata tekniska enheter som är avsedda för dem.[283] Syftet är att skapa en *reviderad ram som är bättre anpassad till förändringar i rörlighet som följer av samhällstrender […] och den tekniska utvecklingen […]*[284]. Att ett fordon

[280] Produktsäkerhetslagen (2004:451) 20§
[281] Regeringen. *SOU 2018:16. Vägen till självkörande fordon*. Stockholm. 2018.
[282] Regeringen. *SOU 2018:16. Vägen till självkörande fordon*. Stockholm. 2018.
[283] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING 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, om ändring av förordning (EU) 2018/... och om upphävande av förordningarna (EG) nr 78/2009, (EG) nr 79/2009 och (EG) nr 661/2009 COM/2018/286 final – 2018/0145 (COD)
[284] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING 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, om ändring av förordning (EU) 2018/... och om upphävande av förordningarna (EG) nr 78/2009, (EG) nr 79/2009 och (EG) nr 661/2009 COM/2018/286 final – 2018/0145 (COD)

är *automatiserat* innebär enligt förslagets definition att fordonet är konstruerat på ett sådant sätt att det kan *röra sig självständigt under längre perioder utan fortlöpande mänsklig övervakning*. Förslaget kan i och med denna definition, och kraven det ställer, ses som ett större steg mot att skapa rättsliga förutsättningar för automation av fordon. Syftet med förslaget är att vara proaktiv och även *hjälpa förarna att gradvis bli vana vid de nya funktionerna* och *öka allmänhetens förtroende och acceptans vid övergången till automatiserad körning.*[285] Förslaget förelägger regelutveckling till UNECE och föreslår följande krav[286]:

- *Ett system som ska ge en ”markering” till föraren genom gasreglaget att denne är på väg att överskrida gällande hastighet – Intelligent Speed Assistance, ISA.*
- *Varningssystem vid avvikelse ur körfält: system för att varna föraren för att fordonet oavsiktligt kör ut ur sitt körfält.*
- *Avancerat nödbromssystem: system som automatiskt kan detektera en potentiell kollision och aktivera fordonets bromssystem och bromsa fordonet i syfte att undvika eller mildra en kollision.*
- *System för kvarstannande i körfält: system för övervakning av fordonets position i förhållande till körfältets gränser och som kräver ett vridmoment på ratten, eller ett tryck på bromsarna, åtminstone när en avvikelse ur körfältet inträffar eller är på väg att inträffa och en kollision kan vara nära förestående.*

[285] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING 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, om ändring av förordning (EU) 2018/... och om upphävande av förordningarna (EG) nr 78/2009, (EG) nr 79/2009 och (EG) nr 661/2009 COM/2018/286 final – 2018/0145 (COD)

[286] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING 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, om ändring av förordning (EU) 2018/... och om upphävande av förordningarna (EG) nr 78/2009, (EG) nr 79/2009 och (EG) nr 661/2009 COM/2018/286 final – 2018/0145 (COD)

För automatiserade fordon föreslås att de dessutom, genom ytterligare delegerade akter, ska kravställas med hänsyn till[287]:

- system som ersätter förarens kontroll av fordonet, inbegripet styrning, acceleration och bromsning
- system som förser fordonet med realtidsinformation om fordonets och omgivningens status
- system för övervakning av förartillgänglighet
- registreringsapparater för kollisionsdata för automatiserade fordon
- harmoniserade format för utbyte av uppgifter för t.ex. kolonkörning med fordon av flera olika märken.

Förslaget förespråkar att kommissionen ska kunna fastställa ytterligare bestämmelser för *särskilda prövningsförfaranden och tekniska krav för typgodkännande av automatiserade fordon med avseende på dessa krav*. Tansportstyrelsen har tagit ställning till förslaget och har inte anmärkt något gällande cybersäkerhet.[288]

Ett annat förslag som direkt rör cybersäkerheten i fordon och blir aktuellt för automatiserade och autonoma fordon har framförts av FN-arbetsgruppen för automatiserade/autonoma och uppkopplade fordon (GRVA) inom Fordonsregleringsforumet WP.29. Förslaget listar ett antal krav som bör ställas på fordonstillverkaren för att nå en rimlig och jämförbar nivå av cybersäkerhet. Certifieringen av tillverkarens system för hantering av cybersäkerheten, Cyber Security Management System (CSMS), är en av förslagets grundpelare. Sådan certifiering blir enlig förslaget ett grundläggande krav för att kunna få ett typgodkännande. CSMS avser tillverkarens systematiska och riskbaserade arbete för att minska cyberhot och skydda fordon mot cyberangrepp genom organisatoriska processer, ansvarsfördelning och styrning. Certifieringen ska genomföras av organ utsedda av medlemsstaterna och kräver omfattande dokumentation av tillverkarens cybersäkerhetsarbete.

[287] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING 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, om ändring av förordning (EU) 2018/... och om upphävande av förordningarna (EG) nr 78/2009, (EG) nr 79/2009 och (EG) nr 661/2009 COM/2018/286 final – 2018/0145 (COD)

[288] Yttrande över Förslag till Europaparlamentets och rådets förordning 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, om ändring av förordning (EU) 2018/... och om upphävande av förordningarna (EG) nr 78/2009, (EG) nr 79/2009 och (EG) nr 661/2009

Cybersäkerheten ska integreras i fordonets livscykel över tre identifierade faser – utveckling, produktion och efterproduktion. Certifieringen ska enligt förslaget vara giltig i tre år. Typgodkännande utfärdade under certifieringens giltighetstid berörs dock ej av denna tidsbegränsning. Även fordonets koncept och utformning behöver dokumenteras ingående för att kunna typgodkännas. Bland annat information om systemarkitekturen, komponenter (och subkomponenter) relevanta för fordonets cybersäkerhet och hur dessa interagerar emellan varandra och andra komponenter efterfrågas. Utifrån arkitekturen och systemen behöver tillverkaren leverera riskanalyser och beskriva hur dessa risker har hanterats. Även en beskrivning av hur tillverkaren har implementerat cybersäkerhetsprinciperna som omnämns i själva förslaget kan framföras som bevis på efterlevnad.

WP.29 noterar i sitt förslag att nya och oförutsedda sårbarheter och angreppssätt kommer att tillkomma över tid.[289] Därför rekommenderas regelbunden revision av åtgärdsförslagen för att kunna tillgodose den utvecklingen som kommer att ske.

2.8 Försäkring

Rättsvetare och beslutsfattare har hittills arbetat under premissen att gällande försäkringsbestämmelser kan gälla för manuellt styrda såväl som autonoma fordon och de varierande graderna av uppkoppling och automatisering däremellan. I *Vägen till självkörande fordon SoU 2018:16* fastslår utredarna att det ”bedöms [att] trafikförsäkringen kunna tillämpas på alla fordon oavsett automationsnivå” och föreslår därför inga regeländringar.[290] Däremot behöver ansvaret för trafiköverträdelser som sker under automatiserad körning klargöras.[291] Likaledes bedömde Europeiska kommissionens särskilda arbetsgrupp för utredningen av samverkande och uppkopplad automatisk körning preliminärt att gällande europeiska rättsakter[292] kommer vara tillräckliga även för autonoma fordon.[293] En sammanställning över rättsakterna återfinns i tabell 13.

[289] Secretary of the UN Task Force on Cyber Security and Over-the-Air issues, Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA, Informal document GRVA-01-17 1st GRVA session, 25-28 September 2018 Agenda item 6 (b)

[290] Vägen till självkörande fordon - introduktion: Slutbetänkande av Utredningen om självkörande fordon på väg. SOU 2018:16, 34

[291] Regeringen. *SOU 2018:16. Vägen till självkörande fordon*. Stockholm. 2018, sida 45

[292] Nämligen direktiven om ansvar för defekta produkter (85/374/EEG) och om motorförsäkringar (2005/14/EG)

[293] Vägen till självkörande fordon - introduktion: Slutbetänkande av Utredningen om självkörande fordon på väg. SOU 2018:16, sida 241

Tabell 13: Försäkring.

Europeiska rättsakter	EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV 2005/14/EG av den 11 maj 2005 om ändring av rådets direktiv 72/166/EEG, 84/5/EEG, 88/357/EEG och 90/232/EEG samt Europaparlamentets och rådets direktiv 2000/26/EG om ansvarsförsäkring för motorfordon
	Rådets direktiv 85/374/EEG om tillnärmning av medlemsstaternas lagar och andra författningar om skadeståndsansvar för produkter med säkerhetsbrister (av den 25 juli 1985)
	EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV 2000/26/EG av den 16 maj 2000 om tillnärmning av medlemsstaternas lagar om ansvarsförsäkring för motorfordon samt om ändring av rådets direktiv 73/239/EEG och 88/357/EEG (fjärde direktivet om motorfordonsförsäkring)
	Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV om ändring av Europaparlamentets och rådets direktiv 2009/103/EG av den 16 september 2009 om ansvarsförsäkring för motorfordon och kontroll av att försäkringsplikten fullgörs beträffande sådan ansvarighet[294]
Svenska rättsakter	Trafikskadelagen (1975:1410)
	Försäkringsrörelselagen (1982:713)

Det svenska systemet bygger på en obligatorisk försäkring som tecknas av fordonets ägare och följer bilen tills den byter ägare, varpå den nya ägaren behöver teckna en ny försäkring för fordonet. För att detta ska kunna appliceras vid automatiserad körning och i synnerhet när det inte finns någon förare, behöver ansvaret klargöras. Utredarna föreslår att fordonsägaren ska ansvara för fordonets överträdelser även under automatiserad körning, vilket befästes med en sanktionsavgift som ersätter böterna som en förare skulle ha fått vid överträdelse.[295] Det finns samtidigt ingen ytterligare specificering hur detta skulle hanteras för hyrda eller leasade fordon. Förslaget inrymmer även möjligheten att ställa regress- eller skadeståndsanspråk mot tillverkaren av fordonet i t.ex. försäkringsfall eller olyckor.[296]

Utredningen konstaterade att den nuvarande lagstiftningen gällande försäkringsfrågor generellt inte är ett hinder för automatisering. Samtidigt återstår ett antal frågetecken kring ansvar vid autonom körning som

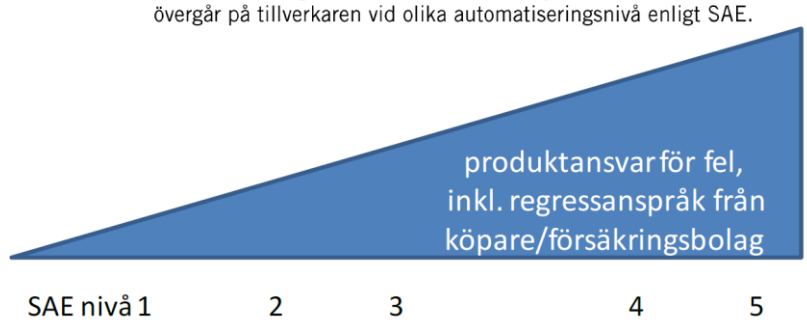
[294] Beredas i skrivande stund
[295] Regeringen. *SOU 2018:16. Vägen till självkörande fordon*. Stockholm. 2018. Sida 45
[296] Regeringen. *SOU 2018:16. Vägen till självkörande fordon*. Stockholm. 2018. Sida l 45

behöver redas ut. Ett av exemplen är ansvaret för skador som uppstår till följd av att det automatiserade fordonet (korrekt) läser felaktig vägskyltning, eller om fordonet inte ”förstår” skyltningen.[297] Översatt till ett cybersäkerhetsproblem kan frågan omformuleras till vem som ansvarar för skador som uppstår då det automatiserade fordonets körning manipuleras genom att vägskyltarnas utformning med uppsåt förändras. Utredningen föreslår att dessa frågor ryms inom skadeståndslagen och trafikförsäkringslagen, men konstaterar samtidigt att sådana fall lätt kan leda till bevissvårigheter och hänvisar till regler för bevislättnad som utvecklas inom ramen för rättspraxis.[298]

Utredningen konstaterar att gällande regler kring produktansvar förblir applicerbara vid skador som orsakas av exempelvis konstruktionsfel. Detta för dock med sig att ansvarsområdet för fordonstillverkaren ökar avsevärt i takt med en ökande automatisering (Figur 1). Samtidigt konstateras att fordonsförsäkringar inte är homogena internationellt, inte heller inom EU. Med tilltagande ansvar för tillverkaren kan det dock uppstå behov att harmonisera den relevanta lagstiftningen och praxisen. I cybersäkerhetssammanhanget kan även en ytterligare typ av försäkring, cybersäkerhetsförsäkring, framträda som ett viktigt alternativ eller nödvändigt tillägg.

Figur 1 **Produktansvar för fel**

En uppskattning av hur ansvaret för det dynamiska körarbetet övergår på tillverkaren vid olika automatiseringsnivå enligt SAE.



Figur 1: Produktansvar för fel. Källa: SOU.

[297] Regeringen. *SOU 2018:16. Vägen till självkörande fordon*. Stockholm. 2018. Sida 512
[298] Regeringen. *SOU 2018:16. Vägen till självkörande fordon*. Stockholm. 2018. Sida 512

Cybersäkerhetsförsäkring (alternativt ”cyberförsäkring”) är en försäkringsgren som fortfarande är under framväxt.[299] I Europa har i synnerhet ikraftträdandet av GDPR och NIS-lagstiftning gett en uppsving till utvecklingen. Försäkringen är tänkt att täcka skador som uppstår till följd av cyberincidenter och IT-brott. Försäkringen – med utgångspunkten i hur systemet ser ut idag – kan tänkas bli aktuell för tillverkarna av autonoma fordon, men även andra alternativ är möjliga, till exempel som sekundära tillägg till ägarens fordonsförsäkring.

2.9 Fordonskontroll

Fordonskontroll avser (bland annat) kontroll av fordon, dess tillhörande system, komponenter och tekniska enheter samt verksamheter inom de besiktningsorgan som genomför kontrollerna.[300] Fordonskontroll regleras utifrån fordonslagen (2002:574) och fordonsförordningen (2009:211) samt utifrån ett antal föreskrifter från Transportstyrelsen.[301] Fordonets tillförlitlighet ur en säkerhetssynpunkt är en väsentlig del av sådana kontroller.[302] Traditionellt sett har tillförlitligheten huvudsakligen inte åsyftat cybersäkerhet. Utredarna för *Vägen till självkörande fordon SoU 2018:16* föreslår ett antal lagändringarna kring fordonskontroll. Ändringarna i SoU 2018:16 avser främst autonoma fordon snarare än endast uppkopplade eller delvis automatiserade fordon. I dagsläget har väldigt få aktörer med besiktningsrelaterad verksamhet som utvecklar metoder och verktyg för bedömning av fordonsbeskaffenhet utifrån cybersäkerhet.[303] Det är dock rimligt att anta att en sådan marknad kan utvecklas om behovet uppstår.

2.9.1 Ansvar för tillverkare och ägare

Det generella ansvaret för fordonskontroller fördelas över tre huvudsakliga aktörer. Besiktningsorganen, ska vara ackrediterade och

[299] Enisa. (2017). *Commonality of risk assessment language in cyber insurance.* Från: https://www.enisa.europa.eu/publications/commonality-of-risk-assessment-language-in-cyber-insurance. Senast 31/10/2019.
[300] Fordonslag (2002:574), 1 kap 1§
[301] Se exempelvis Transportstyrelsens föreskrifter och allmänna råd om registreringsbesiktning, mopedbesiktning och lämplighetsbesiktning (konsoliderad elektronisk utgåva) TSFS 2010:87
[302] Fordonslag (2002:574), 2 Kap 1§
[303] Se exempelvis Tüv Sud. (2019). *POTENTIAL CYBER SECURITY THREATS OF AUTONOMOUS AND CONNECTED VEHICLES.* Från: https://www.tuvsud.com/en/resource-centre/stories/cyber-security-threats-of-connected-vehicles. Senast 04/09/2019.

genomföra besiktningsverksamheten.[304] Tillverkare, eller den som varit direkt engagerad i produktionen av ett fordon, system, komponent eller separat teknisk enhet, ansvarar för typgodkännandeprocessen samt produktsäkerhet.[305] Ägaren, eller den som köpt fordonet eller har nyttjanderätt för fordonet, är ansvarig för fordonets underhåll och att dess nyttjande överensstämmer med fordonsförordningen, såsom besiktning av fordonet.[306]

2.9.2 Cybersäkerhet i fordonskontroller

Svensk lag innehåller redan ett antal bestämmelser som kan tillämpas i syfte att säkerställa cybersäkerheten i fordon. Den publicerade praxisen kring hur dessa skulle tillämpas för att säkerställa cybersäkerhetsaspekter såsom integritet och tillförlitlighet är dock mycket begränsad, vilket föranleder resonemang om hur lagrummet kan behöva utvecklas. Denna analys fokuserar på beskaffenhetsbedömningar av fordon genom registrerings- och lämplighetsbesiktning, samt av kontrollbesiktning.

Som grundläggande förutsättning omfattar bedömningen av den säkerhetsmässiga tillförlitligheten fordon, system, och komponenter, såväl som separata tekniska enheter.[307] Så länge det finns föreskrivna krav för cybersäkerhet kan alltså besiktning och inspektion av sådana krav genomföras.[308] Vid registreringsbesiktning och lämplighetsbesiktning är det den som inställer fordonet vid besiktningen som ska lämna uppgifter och tekniska uppgifter som styrker fordonets beskaffenhet, om uppgifterna inte kan mätas eller på något annat sätt bedömas av besiktningsorganet.[309] Huruvida cybersäkerhet har någon väsentlig roll i underlaget för uppgifterna kommer till stor del bero på

[304] Fordonslag (2002:574)
[305] Fordonslag (2002:574)
[306] Fordonsförordning (2009:211),
[307] Fordonslag (2002:574), 1 Kap 1§; 2 Kap § och 2§§; Fordonsförordning (2009:211), 1 kap 1§
[308] Fordonslag (2002:574), 2 Kap 2§; 2 Kap § och 2§§; Fordonsförordning (2009:211), 2 kap 1§
[309] Transportstyrelsens föreskrifter och allmänna råd om registreringsbesiktning, mopedbesiktning och lämplighetsbesiktning (konsoliderad elektronisk utgåva) TSFS 2010:87, 2 Kap, 3 kap 10-13§§

innehållet i typgodkännande[310] och provningsrapporter.[311] I den mån underlaget baseras på intyg om kravuppfyllnad, exempelvis för tekniska uppgifter, bör det uppmärksammas att Transportstyrelsens föreskrifter tillåter utfärdande av ett antal aktörer som skulle kunna bedöma cybersäkerhetsaspekter i fordonen; nämligen tillverkare, komponenttillverkare, eller en teknisk tjänst på kravområdet.[312]

I dagsläget finns dock ett antal begränsningar för cybersäkerhetskontroller i hur de nuvarande bestämmelserna om beskaffenhet är utformade och tillämpas. Som en övergripande regel är det människor, och inte maskiner (eller datorer), som ansvarar för att fordon har besiktigats enigt gällande bestämmelser.[313] Lagen förutsätter även att lämplighetsbevis som utfärdats vid besiktning ska kunna uppvisas, exempelvis för polis. Dock saknas elektronisk tillämpning av detta i dagsläget.[314] Alltså kan gällande rätt och tillämpning försvåra ansvarsutkrävande vid fullt autonom körning utan närvarande förare. I bedömningen av beskaffenhet föreskriver fordonsförordning (2009:211) att anordningar för manövrering ska vara inrättade för att underlätta förarens åtkomst och förebygga att föraren förväxlar dem.[315] Det är inte tydligt att en sådan formulering är behjälplig vid besiktning av fordon med högre grader av automatiserad manövrering. Beskaffenhetsbedömningen i dess nuvarande utformning fordonsförordning (2009:211) innehåller inga särskilda bedömningar som avser uppkoppling, smarthet, automatisering eller autonomi. Kontroll-besiktningar genomförs för att granska fordonet så att beskaffenheten inte försämrats till en otillåten grad. Denna typ av besiktning genomförs främst ur ett miljö- och trafiksäkerhetssynpunkt snarare än generell lämplighet.[316] Å ena sidan, skulle detta kunna tolkas som att cybersäkerhet inte ska vara en av de säkerhetsaspekter som granskas i

[310] Se exempelvis 13§ angående intyg om överstämmelse med typgodkännande och 14§ om typgodkännande intyg i Transportstyrelsens föreskrifter och allmänna råd om registreringsbesiktning, mopedbesiktning och lämplighetsbesiktning (konsoliderad elektronisk utgåva) TSFS 2010:87

[311] Se 15§ angående provningsrapporter i Transportstyrelsens föreskrifter och allmänna råd om registreringsbesiktning, mopedbesiktning och lämplighetsbesiktning (konsoliderad elektronisk utgåva) TSFS 2010:87

[312] Vägen till självkörande fordon - introduktion: Slutbetänkande av Utredningen om självkörande fordon på väg. SOU 2018:16, 16§, 27-29§§

[313] Vägen till självkörande fordon - introduktion: Slutbetänkande av Utredningen om självkörande fordon på väg. SOU 2018:16; Fordonsförordning (2009:211), 8 Kap 8§

[314] Vägen till självkörande fordon - introduktion: Slutbetänkande av Utredningen om självkörande fordon på väg. SOU 2018:16; Fordonsförordning (2009:211), 5 Kap 7§, 8 Kap 8§

[315] Fordonsförordning (2009:211), 2 Kap 6§

[316] Fordonslag (2002:574), 2 Kap 9§

bedömningen av beskaffenhet. Å andra sidan skulle detta kunna tolkas som att besiktningen endast bör granska cybersäkerhetsbeskaffenhet i den mån den kan ha negativ inverkan på trafiksäkerhet eller miljö. I gällande föreskrifter är beskaffenhetsbedömningarna i kontrollerna generellt inte heller utformade för cybersäkerhet. Lämplighetsbevis, vid lämplighetsbesiktning, omfattar snarare information om exempelvis fabrikat, tjänstevikt, maxlast och axlar.[317] Kontrollprogrammet, vid kontrollbesiktning, omfattar generellt mekaniska funktioner (fysiska) av fordonet såsom stomme, hjulsystem, kaross, och i begränsad omfattning elektronik såsom att hastighetsmätare fungerar eller avläsning av felkoder.[318]

För närvarande ska besiktningsorganet vara ackrediterat[319] enligt Europaparlamentets och rådets förordning (EG) nr 765/2008 samt lagen (2011:791) om ackreditering och teknisk kontroll för att genomföra beskaffenhetsbedömningar (och övrig besiktningsverksamhet). Ackrediteringen är indelad i tre kategorier beroende på fordonstyper som ska besiktigas av organet.[320] Inom EU finns det nu ett förslag om en ny europeisk förordning om certifiering av informations- och kommunikationsteknologi (”cybersäkerhetsakten”) (se del 2.4 av denna rapport).[321] Denna skulle harmoniseras mot förordning (EG) nr 765/2008. I dagsläget kräver Transportstyrelsens föreskrifter att besiktningsorganet ska förfoga över de standarder och fordonsspecifika uppgifter samt utforma nödvändiga rutiner för att genomföra besiktningar.[322] Skulle en ny standardiserings-, certifierings- och ackrediteringsregim bidra till

[317] Transportstyrelsens föreskrifter och allmänna råd om registreringsbesiktning, mopedbesiktning och lämplighetsbesiktning (konsoliderad elektronisk utgåva) TSFS 2010:87, Bilaga 2

[318] Transportstyrelsens föreskrifter och allmänna råd om kontrollbesiktning (konsoliderad elektronisk utgåva) TSFS 2010:84

[319] Fordonslag (2002:574), 4 Kap

[320] Fordonslag (2002:574), 4 Kap 2a§

[321] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD)

[322] Transportstyrelsens föreskrifter och allmänna råd om registreringsbesiktning, mopedbesiktning och lämplighetsbesiktning (konsoliderad elektronisk utgåva) TSFS 2010:87, 1 Kap 5§; Transportstyrelsens föreskrifter och allmänna råd om kontrollbesiktning (konsoliderad elektronisk utgåva) TSFS 2010:84, 2 Kap 4§

utvecklingen av cybersäkerhetsstandardisering för fordon och fordons-besiktning skulle de förmodligen vara frivilliga,[323] om inte annat specificeras i svenska nationella bestämmelser.

En utökad kontrollform för att besiktiga cybersäkerhetsaspekter i smarta fordon skulle förmodligen också kräva nya kompetenser och utrustning hos besiktningsorganen. De grundläggande kompetenserna för en certifierad besiktningstekniker är relativt teknikneutrala.[324] De innehåller kompetenser som att kunna tillämpa gällande föreskrifter, använda tillgängliga IT-lösningar, mätinstrument och andra verktyg, att kunna följa tillämpliga kontrollmetoder etc. Däremot verkar inte denna teoretiska kompetens omfatta IT-säkerhet i dagsläget. Således behövs vidare analys av vilken kunskap cybersäkerhetsbesiktning skulle kräva, vilka instrument och verktyg som teknikerna skulle behöva använda och vad som rimligtvis skulle kunna mätas inom ramen för fordonskontroll. Till exempel, skulle en sådan fordonskontroll främst syfta till att verifiera att typgodkänd programvara och säkerhetsuppdateringar brukades i fordonet, eller skulle prövningen behöva vara mer omfattande?

Flera av ändringarna i SoU 2018:16 skulle inte avsevärt påverka cyber-säkersäkerheten i fordonen i sig, men påverkar indirekt cybersäkerheten. Exempels föreslår man att ändring i lagen (2001:558) om vägtrafikregister för att möjliggöra behandlingen av personuppgifter genom vägtrafikregistret för ” den som är lagringsskyldig enligt 3 kap. 9 § lagen (2019:000) om automatiserad fordonstrafik”.[325] I detta fall blir det istället genom dataskyddslagstiftning som säkerhetsbestämmelser blir gällande för behandlingen. Typgodkännande och Transportstyrelsens föreskrifter kommer fortsatt spela en betydande roll i bedömningen av fordons beskaffenhet.[326] Det bör alltså poängteras att ändringar som avser bedömningarna om beskaffenhet fortsatt är avhängiga hur framtida säkerhetsbestämmelser utvecklas inom UNECE och nationellt. Man föreslår exempelvis ändring i fordonsförordningen (2009:211) avseende bemyndiganden så att ”automatiserade fordon, som inte ska ha en

[323] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD), Artikel 48, sid 12

[324] Transportstyrelsens föreskrifter och allmänna råd om krav på utbildning och kompetens för besiktningstekniker samt polisman och bilinspektör (konsoliderad elektronisk utgåva) TSFS 2017:53, Bilaga: Kompetensprofil

[325] Vägen till självkörande fordon - introduktion: Slutbetänkande av Utredningen om självkörande fordon på väg. SOU 2018:16, 113-114.

[326] Fordonslag (2002:574), 2Kap; Vägen till självkörande fordon - introduktion: Slutbetänkande av Utredningen om självkörande fordon på väg. SOU 2018:16, 162, 366-367

registreringsskylt (alt. motorredskap klass II) får tas i bruk eller användas endast om de är märkta enligt Transportstyrelsens föreskrifter”.[327] I detta fall blir det innehållet i Transportstyrelsen föreskrifter som blir tongivande för cybersäkerheten.

Ett fåtal av förslagen i SoU 2018:16 skulle direkt kunna påverka relationen mellan fordonsbesiktning och cybersäkerhet. Bestämmelser kring besiktningsbehov efter ändring av fordon har huvudsakligen avsett fysiska ändringar av fordonet. Vid smarta och autonoma fordon kan ändringar i programvara ha en inverkan, exempelvis på tillverkarens garantiåtaganden, som föranleder registreringsbesiktning.[328] Detta skulle även kunna gälla programuppdateringar som påverkar fordonens säkerhet. Transportstyrelsen kan även vidta åtgärdsföreläggande ombesiktning för fordonstyper i fall då tillverkaren upptäcker att varan utgör en allvarlig fara för liv och hälsa utifrån bestämmelser i produktsäkerhetslagen.[329]

[327] Vägen till självkörande fordon - introduktion: Slutbetänkande av Utredningen om självkörande fordon på väg. SOU 2018:16, 161
[328] Vägen till självkörande fordon - introduktion: Slutbetänkande av Utredningen om självkörande fordon på väg. SOU 2018:16, 371
[329] Vägen till självkörande fordon - introduktion: Slutbetänkande av Utredningen om självkörande fordon på väg. SOU 2018:16; Produktsäkerhetslag (2004:451) 23 och 36§§

3 Standarder och vägledningar i smart vägtrafik

Flera standardiseringsinstitut utvecklar standarder som är relevant för cybersäkerheten i smarta fordon och vägnät. Likaledes har flera vägledningar utvecklats, både via överstatliga och nationella organisationer på domänområdet. Medan denna del av rapporten reflekterar över vilka organisationer som främst framarbetat dessa, och utifrån vilka perspektiv, återger rapporten även en lista av identifierade standarder i Bilaga 1, en kort genomgång av innehållet i den senaste standarden som utarbetas av Internationella standardiserings-organisationen i Bilaga 2, samt en lista av identifierade vägledningar i Bilaga 3. Anledningen till att det bifogas en genomgång av Internationella standardiseringsorganisationens nya standard på området är för att ge en inblick i det pågående arbetet samt att denna standard även harmoniseras mot UNECE-reglering om produktansvar och därför har en märkbar relevans för framtida tillämpning av cybersäkerhet inom produkt-ansvarsregleringen.

Inom intelligenta transportsystem (ITS), där europeisk lagstiftning och ansvariga nationella myndigheter är utsedda, är standardiseringen etablerad. I och med utvecklingen av kompletterande reglering för samverkande intelligenta transportsystem (C-ITS) pågår även ett omfattande standardiseringsarbete för dessa. Flera av standarderna behandlar även säkerhetsaspekter av ITS- och C-ITS-system då de bakomliggande regleringsinitiativen syftar till vägsäkerhet inbegripet IT-säkerhet.[330] Verksamhet med smarta fordon och vägnät i Sverige berörs främst utav standardiseringen inom:

[330] Se exempelvis COMMISSION DELEGATED REGULATION (EU) /... of XXX supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems. Ref. Ares(2019)153204 - 11/01/2019; COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility. COM/2016/0766 final

- Internationella standardiseringsorganisationen (ISO) som är en internationell icke-statlig organisation som tar fram industristandarder.
- Europeiska standardiseringskommittén (CEN) som arbetar fram standarder för bland annat konsumentprodukter, energi, säkerhet, IKT, maskiner, med mera.
- Europeiska kommittén för elektronisk standardisering (CENELEC) som fokuserar på elektroteknik.
- European Telecommunications Standards Institute (ETSI) som är en organisation för standardisering av telekommunikation.
- Society of Automotive Engineers (SAE) som utvecklar standardisering för transportindustrin, ofta ur ett globalt perspektiv och ihop med ISO.

FN:s ekonomiska kommission för Europa (UNECE), som är en regional kommission för utvecklingen av reglering och vägledning inom transportsektorn, har tagit sig an frågor om intelligenta transportsystem (ITS).[331] WP.29, som är ett regleringsforum för transport inom UNECE, har även arbetat fram vägledningar för dataskydd och cybersäkerhet vid automatiserad körning.[332] I Europa har Europeiska unionens byrå för nät- och informationssäkerhet (ENISA) utvecklat vägledningar för cybersäkerhet både i smarta vägnät[333] och smarta fordon.[334] Likaledes finns det även flera nationella vägledningar exempelvis i Storbritannien[335] och USA.[336]

[331] UNECE. (2019). *Intelligent Transport Systems.* Från: http://www.unece.org/trans/theme_its.html. Senast 24/04/2019; UNECE (2012) Intelligent Transport Systems (ITS) for sustainable mobility. ISBN 9788897212034

[332] Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA. Informal document GRVA-01-17 1st GRVA session, 25-28 September 2018 Agenda item 6 (b); Proposal for draft guidelines on cyber security and data protection. United Nations ECE/TRANS/WP.29/2017/46

[333] ENISA (2015) Cyber Security and Resilience of Intelligent Public Transport: Good practices and recommendations. ISBN: 978-92-9204-146-5

[334] ENISA (2016) Cyber Security and Resilience of smart cars: Good practices and recommendations. ISBN: 978-92-9204-184-7

[335] Se exempelvis Government of the United Kingdom. (2017). *Guidance: Principles of cyber security for connected and automated vehicles.* Från: https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles. Senast 24/04/2019;

[336] Se exempelvis NHTSA (2016) Cybersecurity Best Practices for Modern Vehicles. Report No. DOT HS 812 333

4 Framtida behov och utvecklingsmöjligheter

I samband med denna studie genomfördes en workshop om cybersäkerhetsbestämmelser för smarta fordon och vägnät. Workshopen samlade offentliga och privata aktörer (mestadels inom transportsektorn), och särskilt personal med erfarenhet av att arbeta med rättstillämpningen praktiskt eller personal i en beslutsfattarroll. Deltagarna på denna workshop inkluderade relevanta myndigheter tillsammans med forskare, fordonstillverkare och andra intressenter. Myndighetspersonalen som medverkat kom ifrån Myndigheten för samhällsskydd och beredskap, Polisen, Post- och telestyrelsen, Trafikverket, SWEDAC, Transportstyrelsen, TRAFA samt Totalförsvarets forskningsinstitut. Workshopen hade tre syften:

- höja medvetenheten om cybersäkerhetsbestämmelserna genom ömsesidigt kunskaps- och erfarenhetsutbyte
- utforska möjligheterna till informellt samarbete om smarta fordon och vägnät
- informationsinhämtning om erfarenheterna av rättstillämpning,

Informationsinhämtningen utforskade hur tillämpningen av regleringen kan underlättas och vilka behov av kompletterande bestämmelser och stöd som finns på nationell nivå. Således bidrog workshopen till att besvara fråga fyra och fem i rapporten.

Workshopdeltagarna bekräftade att cybersäkerhetsregleringen i sin helhet är fragmenterad. Det finns inte någon särskild aktör, arkitektur, något tekniskt system, eller tekniska komponenter inom transportsektorn som påverkas av samtliga lagrum. Deltagarna föreslog att effekterna av fragmentering kan minimeras om myndigheter med olika mandat samverkar i tillsyn för att ta fram mer synkroniserade, enhetliga och övergripande granskningar.

Dataskyddet omfattar de bestämmelser som påverkar flest aktörer och flest typer av teknik inom transportsektorn. Detta beror på att definitionerna för personuppgifter och behandling är omfattande. Data som föraridentitet, ägarnamn, registreringsskylt, fordonstyp, fordonsfärg, lokaliseringsuppgifter (med mera) kan vara direkta eller indirekta personuppgifter. Tilltagande uppkoppling, automatisering och autonomi kommer förmodligen innebära att behandlingen ökar i framtiden. Alltså blir ökat medvetande om dataskyddet och tidig utredning av dess tillämpning på nya teknologier särskilt viktig.

Den praktiska tillämpningen av subjektiva principer och krav som ”lämpliga åtgärder” eller ”proportionalitet” är en utmaning som sträcker sig över flera lagrum. Där upplever aktörerna inom transportsektorn att det behövs stöd från behöriga myndigheter som erbjuder olika former av samråd (se tabell 14). De myndigheter som utformar föreskrifter, utformar allmänna råd eller vägledningar för lagrummen bör, enligt deltagarna, även använda mandatet till att arbeta fram tydligare nationella bestämmelser eller tydligare rekommendationer om tillämpningen av sådana bestämmelser.

Tabell 14: Behöriga myndigheter samt stöd- och samverkansformer för rättstillämpning.

Lagrum	**Behörig myndighet**	**Stöd- och samverkansformer**
Dataskydd	Europeiska unionens säkerhetsbyrå	Vägledningar
	Datainspektionen	• Föreskrifter • Allmänna råd • Vägledningar • Godkännande av uppförandekoder
Nätverks- och informationssäkerhet inom samhällsviktig verksamhet	Europeiska unionens säkerhetsbyrå	• Vägledningar
	Myndigheten för samhällsskydd och beredskap	• Föreskrifter • Allmänna råd • Vägledningar • Informella samverksanforum • Deltagande i europeisk samverkan
	Transportstyrelsen	• Föreskrifter • Allmänna råd
Standardisering av cybersäkerhet *(förslag)*[337]	Europeiska unionens säkerhetsbyrå	• Inrättar en ständig intressentgrupp för rådgivning
Säkerhetsskydd	Säkerhetspolisen	• Föreskrifter • Allmänna råd
	Transportstyrelsen *(förslag)*[338]	• Föreskrifter • Allmänna råd
Smarta transportsystem	Transportstyrelsen	• Föreskrifter • Allmänna råd
Produktansvar och produktprövning	Transportstyrelsen	• Föreskrifter • Allmänna råd
Fordonskontroll	Transportstyrelsen	• Föreskrifter • Allmänna råd
Försäkring	Finansinspektionen	• Föreskrifter • Allmänna råd

[337] Ej ännu antaget i lag
[338] Ej ännu antaget i lag

De deltagande myndigheterna bekräftade att det finns flera sätt som aktörer inom transportsektorn kan få stöd från behöriga myndigheter som ansvarar för olika delar av rättstillämpningen (se tabell 14). Dels finns det formella samrådsmekanismer, och formella processer för utveckling av föreskrifter och allmänna råd där berörda aktörer inom transportsektorn kan bistå med remissvar för att bistå myndigheterna i att ta fram mer förankrade lösningar (se tabell 14). För vissa av lagrummen, särskilt de som utvecklats på EU-nivå finns även överstatliga samverkansforum, vägledande organ och arbetsgrupper, exempelvis inom NIS-regleringen, dataskyddet och arbetet med smart robotteknik där de svenska behöriga myndigheternas och experters deltagande skulle stärkas av att de får ökad tillgång till berörda aktörers erfarenheter om strukturella utmaningar i rättstillämpningen.[339]Dessutom finns det även informella tematiska (privat-offentliga) samarbeten där erfarenhetsutbyten tillsammans med behöriga myndigheter kan struktureras. MSB driver ett antal sådana samverkansforum, exempelvis Forum för informationsdelning kring säkerhet i industriella informations- och styrsystem (FIDI-SCADA) där berörda aktörer kan dela information, omvärldsanalys och samarbeta om informationssäkerhet i industriella informationssystem.[340] Ett sådant samverkansforum skulle även kunna struktureras för cybersäkerhet på transportsektorn. Slutligen finns även möjlighet att utveckla forskningskonsortium, forskningsprojekt och övningar där privat-offentlig samverkan och erfarenhetsutbyten kan möjliggöras.

[339] Se exempelvis Europeiska kommissionen. (2019). *NIS Cooperation Group.* Från: https://ec.europa.eu/digital-single-market/en/nis-cooperation-group. Senast 29/10/2019; Europeiska kommissionen. (2019). *High-Level Expert Group on Artificial Intelligence.* Från: https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence. Senast 29/10/2019.

[340] MSB. (2018). *FIDI-SCADA: Forum för informationsdelning kring säkerhet i industriella informations- och styrsystem.* Från: https://www.msb.se/RibData/Filer/pdf/27924.pdf. Senast 29/10/2019.

5 Slutsatser

Tilltagande digitalisering av vägtrafiken kommer troligtvis att ha en stor inverkan på vårt samhälle. Med denna utveckling har även farhågor om tekniska sårbarheter i transportsektorn fått ökad betydelse. Detta sätter i sin tur frågan om cybersäkerheten och dess reglering i fokus. Denna studie har kartlagt ett flertal lagrum och bestämmelser som är relevanta för cybersäkerheten i uppkopplade, automatiserade fordon, inklusive:

- civilrätten för smart robotteknik
- dataskyddsbestämmelser
- nätverks- och informationssäkerhet i samhällsviktig verksamhet (NIS)
- säkerhetsskyddsbestämmelser
- förslag om IKT-standardiseringsbestämmelser
- bestämmelser om intelligenta transportsystem (ITS)
- produktansvars- och produktprövningsbestämmelser
- fordonskontrollsbestämmelser
- försäkringsbestämmelser.

Cybersäkerhetsregleringen för transportsektorn i sin helhet utgörs av en fragmenterad och komplex lagstiftning. Olika lagrum fyller olika syften, med krav som ofta riktas till olika typer av aktörer och verksamhet. Vissa lagrum har mer övergripande effekt på säkerhetskraven för smarta fordon och vägnät än andra. Dataskyddets breda harmonisering, som exempelvis integreringen av dataskydd i tillämpning av NIS, civilrätt för robotteknik, och ITS innebär däremot att individens integritet är centralt för cybersäkerheten i stort på transportsektorn. Utvecklingen av civilrätt för robotteknik, cybersäkerhetsstandardisering, bestämmelser för ITS, och produktansvar innebär även att bestämmelser om cybersäkerhet, konsumentskydd och transportsäkerhet konvergerar inom transportsektorn.

Vissa lagrum är även mer utvecklade än andra i sin formulering av cybersäkerhetskrav. Dataskyddet, NIS, säkerhetsskyddet och civilrätten för robotteknik är de lagrum som i dagsläget formaliserat flest krav kring organisatoriska och tekniska åtgärder för digitaliserad och teknikberoende verksamhet. Lagstiftarna har generellt sett fokuserat på konkreta organisatoriska åtgärder då tekniska åtgärder ofta behöver anpassas efter verksamhet och teknologiutveckling. Arbetet att konkretisera tekniska krav har till stor del utförts av myndigheter med specialiserad föreskriftsrätt och specialiserade vägledande mandat (såsom Myndigheten för samhällsskydd och beredskap, Säkerhetspolisen och Artikel 29-Gruppen). Inom lagrummen finns en del återkommande åtgärder.

Anmälan och samråd. Flera av lagrummen kräver någon form av anmälan eller samråd med behöriga myndigheter innan den skyddsvärda verksamheten med tekniken påbörjas. Exempelvis ska vägmyndigheter och ITS-operatörer anmäla sin verksamhet till MSB och särskilt säkerhetskänslig verksamhet ska rapporteras till Säkerhetspolisen. Samråd sker ofta innan vissa typer av teknologi driftsätts för att hantera vissa risker, exempelvis behandling av säkerhetsskyddsklassificerade uppgifter eller personuppgiftsbehandling med hög risk för individens rättigheter.

Bedöm risker. Det förekommer ofta krav på verksamhetsansvariga att identifiera, analysera och dokumentera risker och deras konsekvenser för att utforma lämpliga skyddsåtgärder. Till exempel förutser resolutionen om civilrätt för robotteknik att analyser av osäkerhet och oförutsägbarhet, samt etisk prövning, kommer vara nödvändigt för autonoma fordon. Även NIS-lagstiftningen, säkerhetsskyddet och dataskyddet kräver olika former av riskanalyser.

Åtgärda säkerheten. Lämpliga tekniska och organisatoriska åtgärder ska ofta väljas på basis av en riskbedömning. I vissa fall förutsätts att detta sker i förutbyggande syfte (innan påbörjad verksamheten eller i ett tidigt skede), exempelvis genom inbyggd integritet såsom inom dataskyddet och civilrätten för robotteknik. I andra fall uppdateras åtgärderna i takt med återkommande riskanalyser såsom för NIS och säkerhetsskyddet.

Rapportera incidenter. Det finns flera potentiellt överlappande typer av incidenter som ska rapporteras till behöriga myndigheter, exempelvis robottekniska hot mot allmän säkerhet, betydande störningar i samhällsviktig verksamhet, säkerhetshotande händelser i säkerhetsskyddslagens bemärkelse, och personuppgiftsincidenter.

För att ytterligare effektivisera den nationella tillämpningen av dessa bestämmelser kommer det behövas ökad samverkan mellan behöriga myndigheter, industrin och forskarkåren. Arbetet med att utforma, disseminera, och träna på nya föreskrifter och vägledningar måste fortsatt konkretisera organisatoriska och tekniska krav såväl som övergripande rättsliga principer. Det är även viktigt att industrin är delaktig i utformningen av bestämmelserna genom remissvar, genom att söka de samrådsmöjligheter som finns och informera myndigheterna om utmaningarna i tillämpningsarbetet. Slutligen är det även viktigt att informella samarbeten såsom samverkansforum och forskningskonsortier utformas och används för att utbyta erfarenheter om rättstillämpningen.

Källförteckning

ACEA Principles of Automobile Cybersecurity. Från: https://www.acea.be/uploads/publications/ACEA_Principles_of_Automobile_Cybersecurity.pdf. Senast 15/04/2019; ENISA (2016) Cyber Security and Resilience of smart cars Good practices and recommendations. doi: 10.2824/87614.

Article 29 Data Protection Working Party (2017) Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS), 17/EN, WP 252

CEN CENLEC (2011) Internal Regulations – Part 2: Common Rules for Standardization Work

COMMISSION DELEGATED REGULATION (EU) /... of XXX supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems.

Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA. Informal document GRVA-01-17 1st GRVA session, 25-28 September 2018 Agenda item 6 (b); Proposal for draft guidelines on cyber security and data protection. United Nations ECE/TRANS/WP.29/2017/46.

David Thomas. (2019). *ePrivacy Regulation continues to stall, but there's hope?* Från: https://iapp.org/news/a/eprivacy-regulation-continues-to-stall-but-theres-hope/. Senast 30/09/2019.

Datainspektionen. (2019). *Datainspektionens uppdrag.* Från https://www.datainspektionen.se/om-oss/vart-uppdrag/. Senast 30/09/2019.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) EGT L 201, 31.7.2002, s. 37–47.

EDPS. (2016). Artificial Intelligence, Privacy and Data Protection. Från: https://edps.europa.eu/sites/edp/files/publication/16-10-19_marrakesh_ai_paper_en.pdf. Senast: 02/07/2019.

ENISA. (2005-2019). *Smart transport.* Från: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/smart-transport. Senast: 15/04/2019.

Enisa (2016) Cyber Security and Resilience of smart cars Good practices and recommendations. doi: 10.2824/87614.

Enisa. (2017). *Commonality of risk assessment language in cyber insurance.* Från: https://www.enisa.europa.eu/publications/commonality-of-risk-assessment-language-in-cyber-insurance. Senast: 31/10/2019.

European Automobile Manufacturers Association. (2017). *ACEA Principles of Automobile Cybersecurity.* Från: https://www.acea.be/uploads/publications/ACEA_Principles_of_Automobile_Cybersecurity.pdf. Senast: 15/04/2019.

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 Text av betydelse för EES. EUT L 207, 6.8.2010, s. 1–13; ENISA. (2005-2019). *Smart transport.* Från: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/smart-transport. Senast:15/04/2019.

Europaparlamentets resolution av den 16 februari 2017 med rekommendationer till kommissionen om civilrättsliga bestämmelser om robotteknik (2015/2103(INL))

Europeiska kommissionen. (2019). *Ethics guidelines for trustworthy AI.* Från: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. Senast 01/10/2019; Europeiska kommissionen. (2019). *High-Level Expert Group on Artificial Intelligence.* Från: https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence. Senast 01/10/2019.

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) (Text av betydelse för EES), EUT L 119, 4.5.2016.

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 EUVL L 194, 19.7.2016.

Europeiska dataskyddsstyrelsen. (2019). Tenth Plenary session: Election of a new Deputy Chair, response to MEP In ‘t Veld, third annual Privacy Shield Review. Från: https://edpb.europa.eu/news/news/2019/tenth-plenary-session-election-new-deputy-chair-response-mep-t-veld-third-annual_en. Senast: 25/06/2019.

Europeiska kommissionen (2016) MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET, RÅDET,

EUROPEISKA EKONOMISKA OCH SOCIALA KOMMITTÉN SAMT REGIONKOMMITTÉN: En europeisk strategi för samverkande intelligenta transportsystem, en milstolpe mot samverkande, uppkopplad och automatiserad rörlighet, COM(2016) 766 final, 3.

Europeiska kommissionen. (2019). *NIS Cooperation Group.* Från: https://ec.europa.eu/digital-single-market/en/nis-cooperation-group. Senast: 29/10/2019.

Europeiska kommissionen. (2019). *High-Level Expert Group on Artificial Intelligence.* Från: https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence. Senast: 29/10/2019.

Fordonslag (2002:574), 1 kap 1§.

Föreskrift nr 79 från Förenta nationernas ekonomiska kommission för Europa (FN/ECE) – Enhetliga bestämmelser om godkännande av fordon med avseende på styrutrustning. *EUT L 137, 27.5.2008.*

Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om respekt för privatlivet och skydd av personuppgifter i samband med elektronisk kommunikation och om upphävande av direktiv 2002/58/EG (förordning om integritet och elektronisk kommunikation) COM/2017/010 final - 2017/03 (COD).

Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning) COM/2016/0590 final - 2016/0288 (COD).

Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) COM/2017/0477 final/2 - 2017/0225 (COD).

Government of the United Kingdom. (2017). Guidance: Principles of cyber security for connected and automated vehicles. Från: https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles. Senast 24/04/2019.

Government of the United Kingdom. (2017). The key principles of vehicle cyber security for connected and automated vehicles. Från: https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles. Senast 24/04/2019.

Kommissionens delegerade förordning (EU) 2015/962 av den 18 december 2014 om komplettering av Europaparlamentets och rådets

direktiv 2010/40/EU vad gäller tillhandahållande av EU-omfattande realtidstrafikinformationstjänster (Text av betydelse för EES) EUT L 157, 23.6.2015.

KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/… av den 13.3.2019 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller införande och operativ användning av samverkande intelligenta transportsystem, C(2019) 1789 final.

Europaparlamentets och rådets direktiv 2002/24/EG av den 18 mars 2002 om typgodkännande av två- och trehjuliga motorfordon och om upphävande av rådets direktiv 92/61/EEG OJ L 124, 9.5.2002.

Europaparlamentets och rådets direktiv 2003/37/EG av den 26 maj 2003 om typgodkännande av jordbruks- eller skogsbrukstraktorer, av släpvagnar och utbytbara dragna maskiner till sådana traktorer samt av system, komponenter och separata tekniska enheter till dessa fordon och om upphävande av direktiv 74/150/EEG. OJ L 171, 9.7.2003.

Rådets direktiv 70/387/EEG av den 27 juli 1970 om tillnärmning av medlemsstaternas lagstiftning om dörrar på motorfordon och släpvagnar till dessa fordon.

Rådets direktiv 78/549/EEG av den 12 juni 1978 om tillnärmning av medlemsstaternas lagstiftning om hjulskydd på motorfordon.

Rådets direktiv 85/374/EEG av den 25 juli 1985 om tillnärmning av medlemsstaternas lagar och andra författningar om skadeståndsansvar för produkter med säkerhetsbrister.

Europaparlamentets och rådets direktiv 95/28/EG av den 24 oktober 1995 om brinnegenskaperna hos material som används i inredningen till vissa kategorier av motorfordon.

Europaparlamentets och rådets direktiv 2001/95/EG av den 3 december 2001 om allmän produktsäkerhet. Europeiska gemenskapernas officiella tidning nr L 011, 15/01/2002.

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC). COM/2018/246 final.

Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING 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, om ändring av förordning (EU) 2018/... och om upphävande av förordningarna (EG) nr 78/2009, (EG) nr 79/2009 och (EG) nr 661/2009 COM/2018/286 final - 2018/0145 (COD).

Yttrande över Förslag till Europaparlamentets och rådets förordning 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, om ändring av förordning (EU) 2018/... och om upphävande av förordningarna (EG) nr 78/2009, (EG) nr 79/2009 och (EG) nr 661/2009.

Secretary of the UN Task Force on Cyber Security and Over-the-Air issues, Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA, Informal document GRVA-01-17 1st GRVA session, 25-28 September 2018 Agenda item 6 (b).

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

Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

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

Datainspektionen. (2019). *Datainspektionens föreskrifter och allmänna råd.* Från: https://www.datainspektionen.se/lagar--regler/datainspektionens-foreskrifter-och-allmanna-rad/. Senast 30/09/2019.

Liveri Dimitra. (2018). Enhancing automotive cybersecurity in Europe. (OECD Workshop on Digital Security and Resilience in Critical Infrastructure and Essential Services |16.02.18, Paris) Från: https://www.oecd.org/going-digital/digital-security-in-critical-infrastructure/digital-security-workshop-february-2018-Liveri.pdf. Senast: 15/04/2019.

Mark Schaub. (2018). *Cybersecurity: Achilles' Heel for Self-driving Cars?* Från: https://www.lexology.com/library/detail.aspx?g=516d38b3-df85-4293-871a-bb461c572769. Senast 15/04/2019; European Automobile Manufacturers Association. (2017).

Matthew Channon, Lucy McCormick, och Kyriaki Noussia (2019). The Law and Autonomous Vehicles. Oxon: Routledge. Kap 5; Trafikverket. (2018). *Trender i transportsystemet: Trafikverkets omvärldsanalys 2018.* Från: https://trafikverket.ineko.se/Files/en-

US/51419/Ineko.Product.RelatedFiles/2018_180_trender_i_transportsystemet_trafikverkets_omv%C3%A4rldsanalys_2018.pdf. Senast: 16/04/2019.

Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster MSBFS 2018:8,

MSB. (2018). *FIDI-SCADA: Forum för informationsdelning kring säkerhet i industriella informations- och styrsystem.* Från: https://www.msb.se/RibData/Filer/pdf/27924.pdf. Senast: 29/10/2019.

MSB. (2018). Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster. MSBFS 2018:7,

MSB. (2019). *NIS-direktivet.* Från: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/. Senast: 26/07/2019;

MSB. (2019). *Cert.se.* Från: https://www.cert.se/. Senast 26/07/2019.

NHTSA (2016) Cybersecurity Best Practices for Modern Vehicles. Report No. DOT HS 812 333.

NHTSA (2016) AUTOMATED DRIVING SYSTEMS 2.0: A VISION FOR SAFETY.

Alliance of Automobile Manufacturers and the Association of Global Automakers. (2016). *Framework for Automotive Cybersecurity Best Practices.* Från: https://www.globalautomakers.org/OldSiteContentAssets/press-release/Automakers-Develop-Framework-for-Automotive-Cybersecurity-Best-Practices-assets/framework-autocyberbestpractices-14jan20161-pdf. Senast 24/02/2019.

Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS), 17/EN, WP 252.

Regeringen. *SOU 2018:16. Vägen till självkörande fordon – introduktion. Del 1. Slutbetänkande av utredningen om självkörande fordon på väg.* Stockholm. 2018.

Säkerhetsskyddslag SOU 2015:25.

Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2.

Säkerhetsskyddslag (2018:585).

Säkerhetsskyddsförordning (2018:658).

Trafikverket. (2018). *Trender i transportsystemet: Trafikverkets omvärldsanalys 2018.* Från: https://trafikverket.ineko.se/Files/en-US/51419/Ineko.Product.RelatedFiles/2018_180_trender_i_transportsystemet_trafikverkets_omv%C3%A4rldsanalys_2018.pdf. Senast: 16/04/2019.

Transportstyrelsen (2016) Framställan om ändring i förordning (2016:383) om intelligenta transportsystem vid vägtransporter: Ändring med anledning av förordning (EU) nr 2015/962 om realtidstrafikinformationstjänster (TSG 2016-2881).

Transportstyrelsens föreskrifter och allmänna råd om registreringsbesiktning, mopedbesiktning och lämplighetsbesiktning (konsoliderad elektronisk utgåva) TSFS 2010:87

Tuv Sud. (2019). *POTENTIAL CYBER SECURITY THREATS OF AUTONOMOUS AND CONNECTED VEHICLES.* Från: https://www.tuvsud.com/en/resource-centre/stories/cyber-security-threats-of-connected-vehicles. Senast 04/09/2019.

Transportstyrelsens föreskrifter och allmänna råd om krav på utbildning och kompetens för besiktningstekniker samt polisman och bilinspektör (konsoliderad elektronisk utgåva) TSFS 2017:53, Bilaga: Kompetensprofil.

Produktsäkerhetslag (2004:451).

UNECE. (2019). *Intelligent Transport Systems.* Från: http://www.unece.org/trans/theme_its.html. Senast: 24/04/2019.

UNECE (2012) Intelligent Transport Systems (ITS) for sustainable mobility. ISBN 9788897212034

Yttrande från Europeiska datatillsynsmannen om kommissionens meddelande handlingsplan för införande av intelligenta transportsystem i EU och det åtföljande förslaget till Europaparlamentets och rådets direktiv om en ram för införande av intelligenta transportsystem på vägtransportområdet och för gränssnitt mot andra transportsätt (2010/C 47/02),

5GAA. (2019). *5GAA welcomes Council objection against C-ITS Delegated Act.* Från: https://5gaa.org/news/5gaa-welcomes-council-objection-against-c-its-delegated-act/. Senast 30/09/2019.

Bilaga 1 - Standarder

ISO/SAE

21434 Road Vehicles -- Cybersecurity engineering

SAE International

J3061 - Cybersecurity guidebook for cyber-physical vehicle systems

J3101 - Requirements for hardware protected security for ground vehicle applications

ISO (International Organization for Standardization)

17427-4:2015 Intelligent transport systems — Cooperative ITS — Part 4: Minimum system requirements and behaviour for core systems

17427-7:2015 Intelligent transport systems — Cooperative ITS — Part 7: Privacy aspects

17427-1:2018 Intelligent transport systems — Cooperative ITS — Part 1: Roles and responsibilities in the context of co-operative ITS architecture(s)

21185:2019 Intelligent transport systems — Communication profiles for secure connections between trusted devices

ISO/DIS

17427-1 Intelligent transport systems -- Cooperative ITS -- Part 1: Roles and responsibilities in the context of co-operative ITS architecture(s)

ETSI (The European Telecommunications Standards Institute)

102 893: "Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)"

102 940 V1.3.1 (2018-04) Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management

102 942 V1.1.1 (2012-06) Intelligent Transport Systems (ITS); Security; Access Control

103 097 V1.3.1. Intelligent Transport Systems (ITS) Security; Security Header and certificate formats.

103 301 V1.1.1: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services.

302 637-2 V1.3.2 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service

302 637-3 V1.2.2 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service

302 665 V1.1.1 Intelligent Transport Systems (ITS); Communications Architecture

Bilaga 2: ISO/SAE 21434

ISO/SAE 21434

Det pågår för närvarande ett arbete med utveckling av en ISO/SAE-standard 21434 Road Vehicles - Cybersecurity engineering. Detta arbete sker i en arbetsgrupp mellan ISO och amerikanska SAE. Standarden (framtida ISO/SAE 21434) beskriver ett systematiskt arbetssätt inom cybersäkerhet för alla som arbetar med utveckling av fordon och tjänster för uppkopplade fordon. Standarden kommer att vara frivillig att tillämpa, men förhoppningen är att den ska bli så pass bra och få en så bred acceptans globalt att berörda parter väljer att använda den. ISO/SAE standarden kan komma att komplettera det framtida UNECE-reglementet för automotive cybersecurity. Tidplanen är att ISO 21434 ska gå ut på publik remiss senast oktober 2019. Publicering ska ske före oktober 2020.

Syfte

Följande text är hämtad från "ISO SAE 21434 dokument for commenting vers04 (ISO/TC 22/SC 32/WG 11 N 510)". Standarden behandlar konstruktion av E/E-system inom vägfordon. Standarden innehåller ordförråd, processer, krav och vägledande principer.

Tanken med standarden är främst att tillhandahålla ett ramverk för cybersäkerhet för att på så sätt främja cybersäkerhetskultur, hantera cybersäkerhetsrisker och definiera cybersäkerhetsprocesser och organisatoriska mål

Omfattning

Dokumentet specificerar cybersäkerhetskrav gällandes konstruktion, produktion, drift, underhåll och avveckling för elektriska och elektroniska system för vägfordon, deras komponenter och gränssnitt.

I standarden så specificeras ett ramverk som innehåller krav på cybersäkerhetsprocesser och ett gemensamt språk för att kommunicera och hantera cybersäkerhetsrisker.

Standarden kan appliceras på serieproduktionsvägsfordon E / E-system, deras komponenter och gränssnitt men beskriver inte tekniklösningar. Standarden är även begränsad till insidan av fordonet.

Följande klausuler är de nuvarande rubrikerna som behandlas i denna standard.

Klausul 5 och 6 (Management of cybersecurity) inkluderar den organisatoriska cybersäkerhetsstrategin, policy och mål.

Klausul 7 (riskbedömningsmetoder) avgör riskens omfattning.

Klausul 8 (konceptfas) definierar målen för cybersäkerhet. Därefter definieras cybersäkerhetskonceptet för att uppnå cybersäkerhet-målen.

Klausul 9 (Produktutveckling) definierar specifikationen för cybersäkerhetskrav, den arkitektoniska designen och implementerar och verifierar cybersäkerhetskrav som är specifika för produkten.

Klausul 10 till 13 (faser efter utveckling) anger krav för att säkerställa att produkten uppfyller cybersäkerhetskraven från utvecklingen. Den specificerar också aktiviteter för organisationen för att upprätthålla cybersäkerhet tills slutet av stöd eller avveckling, beroende på vad som inträffar först.

Klausul 14 (Stödprocesser) inkluderar organisationsprocesser som hjälper till med konstruktion, utveckling och leverantörshantering.

Bilaga 3: Vägledningar

Centre for Connected and Autonomous Vehicles . (2017). *Automated Driving Systems 2.0: A Vision for Safety.* Från: https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles. Last Senast 28/10/2019.

Economic Commission for Europe. (2017). *Proposal for draft guidelines on cyber security and data protection.* Från: https://www.unece.org/fileadmin/DAM/trans/doc/2017/wp29/ECE-TRANS-WP29-2017-046e.docx . Senast 28/10/2019.

ENISA. (2016). *Cyber Security and Resilience of smart cars.* Från: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars. Senast 28/10/2019.

European Commission. (2017). *Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS).* Från: https://ec.europa.eu/transport/sites/transport/files/c-its_security_policy_release_1.pdf. Senast 28/10/2019.

NHTSA. (2017). *Automated Driving Systems 2.0: A Vision for Safety.* Från: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf. Senast 28/10/2019.

NHTSA. (2016). *Cybersecurity Best Practices for Modern Vehicles.* Från: https://www.nhtsa.gov/crash-avoidance/automotive-cybersecurity. Last Senast 28/10/2019.

The Secretary of the UN Task Force on Cyber Security and Over-the-Air issues. (2018). *Draft Recommendation on Cyber Security of the Task Force on Cyber.* Från: https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29grva/GRVA-01-17.pdf. Senast 28/10/2019.

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se