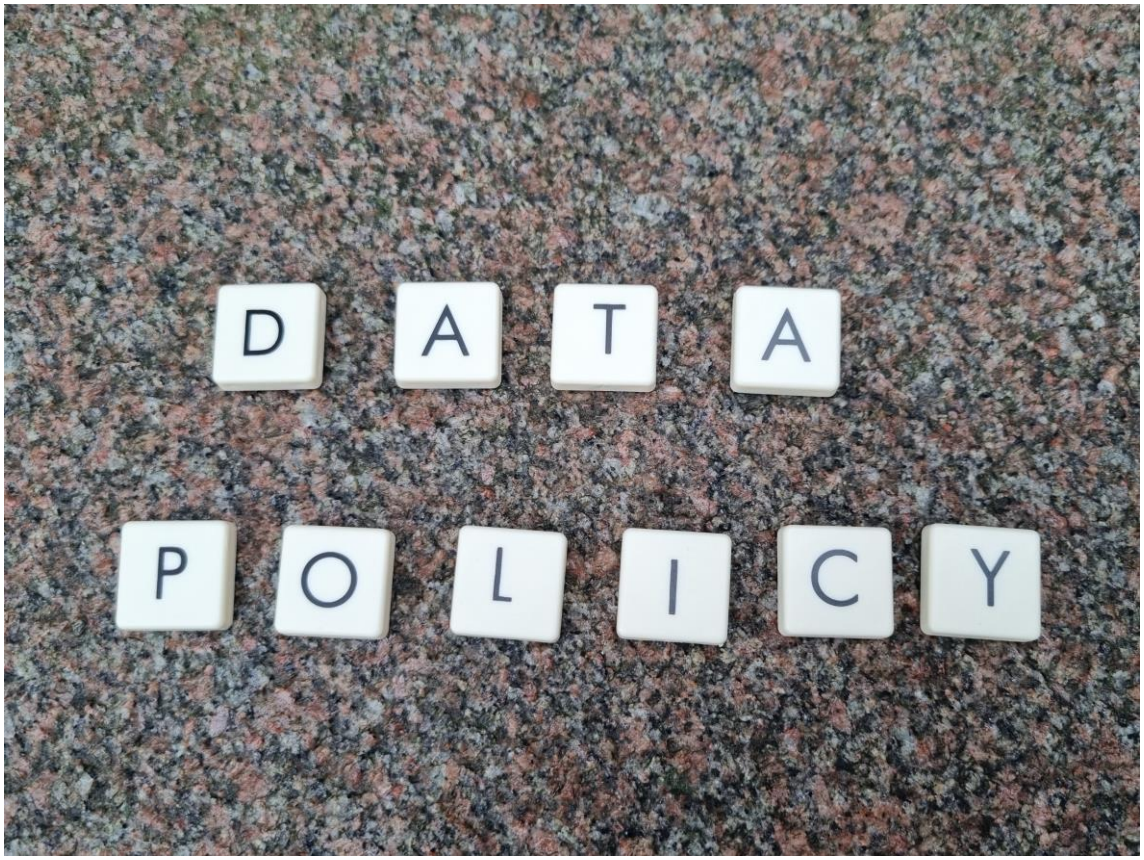
DIGITALA SYSTEM
MOBILITET OCH SYSTEM



Regelverk för datadelning inom citylogistik: nulägesanalys

Kristina Andersson

RISE Rapport 2022:57

FFI Fordonsstrategisk Forskning och Innovation

Regelverk för datadelning inom citylogistik: nulägesanalys

Kristina Andersson

Abstract

Regulations for data sharing in city logistics: current situation analysis

Almost all data sharing regulations have origins from the EU. At EU level, three trends can be identified for data sharing. The first trend is that data sharing more and more is regulated by legislation. Current regulations are being amended and many new regulations are underway within the EU. Data sharing legislations are thus in an expansive phase. There are also many reasons why the EU believes that a certain regulatory framework is needed, such as:

- Information security: Historically, information security has generated a large amount of activity in the field of regulatory framework. This includes, for example, cyber security and preventing data breaches.
- Human health: Human health is also a reason to regulate data sharing. Examples of regulations in this area are the GDPR and sharing of sensitive personal data.
- Consumer protection: There are also regulations aimed at strengthening consumer protection and ensuring that, for example, digital services are safe for consumers to share data in.
- A free and efficient internal market: For the EU, it is important to create an internal market for data sharing. Many regulations are aimed at ensuring that SMEs can compete with large companies. Example of legislation in this area is the Platform Regulation.
- Increased innovation power: For the EU, it is also important to increase innovation capacity in the internal market. One way is to protect innovations through, for example, copyright and trade secrets rules.
- Increased transparency and trust: To create an internal market, people and companies also need to feel safe sharing data. Example of legislation within this area is the proposed Data Governance Act.
- Fundamental rights and freedoms: Finally, the EU is reassessing in many regulatory frameworks in terms of respect of fundamental human rights and freedoms. Examples of regulations in this area are the GDPR and the e-Privacy regulation. The EU is also working on developing a code on this theme. The code shall guide the future work on the develop of new legislation.

The second trend is for the EU to encourage industry organizations to develop voluntary rules on data sharing (code of conduct) to accelerate the creation of an internal market for data sharing. An example of this is the Code of Conduct for sharing agricultural data in agreements. The Free Flow of non-personal data regulation would also like to see industry organizations develop principles for data sharing.

The third trend is that the EU would like to see us all make more data publicly available or that we donate data, both from authorities and individuals (open data and altruism). Examples of this are the Open Data Directive and the forthcoming Data Governance Act. In this lies a conflict of interest between information security and open data that is not easy to solve. The challenge lies in the fact that each individual dataset itself does

not have to reveal anything sensitive. However, if many datasets are added together, aggregated data can reveal too much.

The EU is also interested in data sharing for certain sectors, of which vehicles and mobility is an area that is becoming more and more regulated in terms of data sharing. Here, a lot of new regulations are expected that will have a major impact on the sector, both in terms of vehicle development but also in terms of the development of new business models. The trend is towards vehicle manufacturers being increasingly forced to share data with authorities. When it comes to logistics, the pressure from new legislation about data sharing is not as clear. The existing legislation is more about the safe distribution of goods in a crisis or regarding sharing data from certain goods e.g., tobacco. What problems does the EU address in its mobility and vehicle regulations?

- Human health: Compared to the general regulatory framework, there is a clear emphasis on human health and data sharing in the regulations. It is both about data sharing related to air quality but also road safety.
- Consumer protection: There are also regulations aimed at strengthening consumer protection, e.g., for manufacturers to inform consumers about how much exhaust fumes a particular vehicle emits so that the consumer can make an informed choice based on this aspect between different manufacturers.
- A free functioning efficient internal market: Examples of legislation in this area are the access of independent branded workshops to data from connected vehicles to increase competition.

At EU level, there are several regulatory frameworks in the pipeline that will have a major impact on what we want to explore in our project. In the HITS2024 project, we want to explore and test efficient city logistics based on different vehicle concepts and logistics solutions. At EU level, a forthcoming e-Privacy Regulation is being discussed. The regulation will dictate how data from vehicles is allowed to be transfer to a cloud solution i.e., the connection as such. The e-Privacy Regulation is closely related to the GDPR, but there are also differences between these regulations. The GDPR accepts consent and balancing of interests to collect personal data while the e-Privacy Regulation only accepts consent (at the time of writing). The challenge for the automotive industry, for example, is that an autonomous vehicle can only collect personal data based on balancing interests because it is not doable to work with consent. However, if the e-Privacy Regulation in its current state is approved, the data will not be allowed to leave the vehicle because there is no consent. Another challenge is the upcoming AI Act. The AI Act distinguishes between technologies that already have an international regulatory framework for, e.g., type approval of a truck and technology where only the EU regulates the issue, e.g., machines. But a vehicle consists of many different “parts” and not all parts are type approved. How do you fit different technologies and different legislation together in an autonomous truck? In the logistics area, the upcoming Data Act can be of great importance as it will be about data sharing between companies. Until now, coordination between different data regulations has not always been optimal. The same phenomenon has been regulated in different regulations. There is a risk that different regulations in the future will find it difficult to co-exist with each other. How will, for example, GDPR, e-Privacy regulation and Data Act work together in a vehicle and logistics context? Developments in this area need to be followed.

Key words: logistic, mobility, data sharing, policy, regulation

RISE Research Institutes of Sweden AB

RISE Rapport 2022:57
ISBN: 978-91-89561-97-7
Göteborg 2022

Innehåll

Förord

Den här rapporten är ett resultat av ett arbete som utförts i projektet *Hållbara & Integrerade urbana Transport System - HITS2024*. Projektet pågår under åren 2020–2024 och handlar om morgondagens citylogistik med fokus på bl.a. datadelning mellan olika aktörer. I projektet finns 19 projektparter från myndighet, akademi och företag. Scania CV AB är projektledare.

Svenska staten genom VINNOVA, Energimyndigheten och Trafikverket samt den svenska fordonsindustrin genom AB Volvo, Volvo Personvagnar AB, Scania CV AB och Fordonskomponentgruppen/FKG har avtalat att inom temaområdena Klimat & Miljö samt Säkerhet samverka avseende fordonsstrategisk forskning, utveckling och innovation (”FFI”). Målet med satsningen är att minska vägtransporters miljöpåverkan och energianvändning, minska antalet dödade och skadade i trafiken samt öka svensk fordonsindustris förutsättningar att genom bland annat starka forsknings- och innovationsmiljöer, med ledande kunskaper inom dessa och andra områden, stärka sin konkurrenskraft. Inom ramen för samverkan har i stycket nämnda parter beslutat finansiera projektet HITS2024 (VINNOVA diarienummer 2020–00565). Läs mer om FFI på www.vinnova.se/ffi .

Projektet är vidare indelat i två faser. Den första fasen är mer utforskande för att i den andra fasen bli mer konkret och börja testa olika företeelser i verkligheten. Den här rapporten hör till den första fasen. Arbetet har gjorts i form av en nuläges- och omvärldsanalys för att förstå hur regelverk påverkar de förslag som finns i projektet kring datadelning. Med datadelning och policy avses regelverk som är relevanta för transaktioner i stort. Analysen omfattar tiden fram t.o.m. december 2021.

Jag vill rikta ett stort tack till alla som medverkat under projektets gång och bidragit med sin tid, kompetens och åsikter.

Ståndpunkter och slutsatser är mina egna och överensstämmer inte med nödvändighet med någon annan projektpart eller annan medverkande vid denna rapports tillkomst.

Göteborg i januari 2022

Kristina Andersson

Sammanfattning

Nästan alla regelverk för datadelning kommer numera från EU. På EU-nivå kan tre trender på en generell horisontell nivå urskiljas för datadelning. Den första trenden visar att alltmer datadelning regleras genom lagstiftning. Existerande regelverk görs om och många nya regelverk är på gång inom EU. Regler för datadelning befinner sig således i en expansiv fas. Det finns också många orsaker till varför EU anser att ett visst regelverk behövs. Det kan handla om:

- Informationssäkerhet: Historiskt har informationssäkerhet genererat en stor aktivitet inom regelgivningsområdet. Det handlar t.ex. om cybersäkerhet och att förhindra dataintrång.
- Människors hälsa: Människors hälsa är också en orsak att reglera datadelning. Exempel på regelverk inom detta område är GDPR och känsliga personuppgifter.
- Konsumentskydd: Det finns även regelverk som syftar till att stärka konsumentskyddet och garantera att t.ex. digitala tjänster är säkra för konsumenter att dela data med.
- En fri fungerande effektiv inre marknad: För EU är det viktigt att skapa en inre marknad för datadelning. Många regelverk går ut på att se till så att små och medelstora företag kan konkurrera med stora företag. Exempel på lagstiftning inom detta område är plattformsförordningen.
- Ökad innovationskraft: För EU är det också viktigt att öka innovationsförmågan på den inre marknaden. Ett sätt är att skydda innovationer genom t.ex. regler för upphovsrätt och företagshemligheter.
- Ökad transparens och tillit: För att få till en inre fungerande marknad behöver personer och företag även känna sig trygga med att dela data. Transparens och tillit är något som återkommer i flera regelverk t.ex. GDPR och den kommande dataförvaltningsakten.
- Grundläggande fri- och rättigheter: Slutligen återkommer EU i många regelverk kring behovet av att respektera grundläggande mänskliga fri- och rättigheter. Exempel på regelverk inom detta område är GDPR och e-Privacyförordningen. EU arbetar också med att ta fram en kodex på detta tema. Kodexen ska vara vägledande för det framtida arbetet med att ta fram ny lagstiftning.

Den andra trenden är att EU uppmuntrar branschorganisationer att ta fram frivilliga regler för datadelning (code of conduct) för att påskynda skapandet av en inre marknad för datadelning. Ett exempel på detta är branschöverenskommelsen för att dela jordbruksdata i avtal. Även fria flödesförordningen ser gärna att branschorganisationer tar fram principer för datadelning.

Den tredje trenden är att EU gärna ser att vi alla gör mer data allmänt tillgänglig eller att vi donerar data. Detta gäller både myndigheter och enskilda (öppna data och altruism). Exempel på detta är öppna data-direktivet och den kommande dataförvaltningsakten. I detta ligger en målkonflikt mellan informationssäkerhet och öppna data som inte är enkel att lösa. Utmaning ligger i att varje enskilt dataset i sig behöver inte nödvändigtvis avslöja något känsligt. Men om många datasets läggs samman kan data på aggregerad nivå ändå avslöja för mycket.

EU är också intresserade av datadelning för vissa sektorer varav fordon och mobilitet är ett område som blir mer och mer reglerat. Här förväntas en hel del nya regelverk som kommer att få stor påverkan på sektorn, både vad gäller fordonsutveckling, och vad gäller utvecklandet av nya affärsmodeller. Trenden går mot att fordonstillverkare ska tvingas att dela mer och mer data med myndigheter. När det gäller logistik är trycket på ny lagstiftning inte lika tydligt. Den lagstiftning som finns handlar mer om att varudistributionen måste fungera i en krissituation och datadelning för vissa specifika varugrupper t.ex. tobak. Vilka problem adresserar då EU i sina regelverk för mobilitet och fordon?

- Människors hälsa: Jämfört med det generella regelverket finns det en tydlig tyngdpunkt mot människors hälsa och datadelning i regelverken. Det handlar både om datadelning som rör luftkvalitet, och trafiksäkerhet.
- Konsumentskydd: Det finns även regelverk som syftar till att stärka konsumentskyddet, t.ex. att tillverkare ska informera konsumenter om hur mycket avgaser ett visst fordon släpper ut så att konsumenten kan göra ett informerat val utifrån denna aspekt mellan olika tillverkare.
- En fri fungerande effektiv inre marknad: Exempel på lagstiftning inom detta område är oberoende märkesverkstäders tillgång till data från uppkopplade fordon i syfte att öka konkurrensen.

På EU-nivå finns det flera regelverk på gång, som kommer att få stor betydelse för vad vi vill utforska i vårt projekt. I HITS2024 projektet vill vi utforska och testa effektiv citylogistik utifrån olika fordonskoncept och logistiklösningar. På EU-nivå diskuteras bl.a. en kommande e-Privacyförordning. Förordningen kommer att träffa hur data från fordon får överföras till en molnlösning dvs. uppkopplingen som sådan. E-Privacyförordningen är nära släkt med GDPR, men det finns också skillnader mellan dessa regelverk. GDPR accepterar samtycke och intresseavvägning för att samla in personuppgifter medan e-Privacyförordningen endast accepterar samtycke (när detta skrivs). Utmaningen för fordonsindustrin är t.ex. att ett autonomt fordon kan samla in personuppgifter med stöd av intresseavvägning (fordonet kan inte stanna och fråga varje person det kör förbi om samtycke finns). Men om e-Privacyförordningen går igenom, i föreslagen lydelse, kommer inte personuppgifterna att kunna lämna fordonet eftersom det inte finns ett samtycke till detta. En annan utmaning är den kommande AI-förordningen. AI-förordningen skiljer mellan teknik, som det redan finns ett internationellt regelverk för t.ex. typgodkännande av en lastbil och teknik där endast EU reglerar frågan t.ex. maskiner. Konsekvensen av detta blir att AI i ett autonomt fordon kommer att lyda under olika regelverk beroende på om funktionen omfattas av ett typgodkännande eller inte. Inom logistikområdet kan den kommande Data Act få stor betydelse då den kommer att handla om datadelning mellan företag och skydd av databaser. Hittills har samordningen mellan olika regelverk för data inte alltid varit optimal. Samma företeelse har reglerats i olika regelverk. Det finns en risk att olika regelverk i framtiden kommer att ha svårt att fungera tillsammans. Hur kommer t.ex. GDPR, e-Privacyförordningen och Data Act att fungera ihop i ett fordons- och logistiksammanhang? Utvecklingen inom detta område behöver följas.

1 Inledning

Den här rapporten är ett resultat av ett arbete som utförts i projektet *Hållbara & Integrerade urbana Transport System - HITS2024*. HITS2024 pågår under åren 2020–2024 och handlar om morgondagens citylogistik med fokus på bl.a. datadelning mellan olika aktörer i logistikkedjan. Projektet är indelat i två faser. Den första fasen är mer utforskande för att i den andra fasen bli mer konkret och börja testa olika företeelser i verkligheten. Den här rapporten avser den första fasen. Arbetet har gjorts i form av en nuläges- och omvärldsanalys för att förstå hur regelverk påverkar de förslag som finns i projektet kring datadelning. Med datadelning och policy avses regelverk som är relevanta för transaktioner i stort. Analysen omfattar tiden fram t.o.m. december 2021. Exempel på frågor som vi har övervägt i projektet är: Vilka utmaningar finns i framtiden för datadelning inom fordons- och logistiksektorn kopplat till olika aktörer som myndigheter respektive företag? Hur påverkar olika regelförslag angående data fordonsutvecklingen? Hur påverkar datadelning olika hubblösningar och sista milen lösningar? Hur kommer datadelning att påverka framtidens E-handel[1] och Quick e-handel[2]?

Den här rapporten syftar till att ge en kort översikt över de mest relevanta regelverk som reglerar datadelning idag och även ge en summering av förväntad lagstiftning inom området de närmaste åren inom EU och Sverige. Samtidigt är datadelning ett brett område som kopplar till många olika företeelser såsom Artificiell Intelligens (AI), Internet of Things (IoT) och molntjänster, varför det är svårt att ge en heltäckande bild inom området. Vidare finns det många olika kategorier av data som utvecklas i egna spår/silos, vilket också gör det svårt att ge en entydig bild över utvecklingen. Vissa kategorier av data omfattas av ett detaljerat regelverk, t.ex. personuppgifter, medan andra kategorier av data inte ens har ett eget regelverk. Det finns även motstridiga intressen inom området som påverkar utvecklingen. Ska data delas fritt med så många som möjligt (öppna data) eller endast inom min utvalda grupp (exklusivitet)? Om fler delar data med varandra, t.ex. mellan företag och myndighet, kan detta trigga investeringar som driver utvecklingen framåt på båda sidor. Tillgång till stora mängder data kan också vara en viktig konkurrensfördel. Datadelning skapar därmed nya möjligheter för innovation och påverkar också affärsmodellen. En annan utmaning är att datadelning i större skala är en förhållandevis ny företeelse, vilket innebär att det kan vara bra att låta den utvecklas på egen hand och inte reglera för tidigt och därmed riskera att hämma utvecklingen.

Datadelning, dvs. utbyte av data mellan olika aktörer, är en central del i utvecklingen av en dataekonomi. Idag delas data företag till företag (B2B) främst utifrån perspektivet att data kontrolleras av någon och att data har ett värde (civilrättsligt perspektiv). Jämfört med många andra företeelser är datadelning B2B förhållandevis oreglerat. Datadelning mellan olika företag sker primärt genom avtal dvs. att det är upp till ett enskilt företaget att bestämma hur, när, vad, vem och till vilket pris företaget vill dela

[1] Försäljning av varor och tjänster online.
[2] Varorna ska vara hemma hos köparen inom en kort tid t.ex. inom 1 timme.

data med andra företag. Sedan finns det vissa legala inskränkningar i avtalsfriheten utifrån t.ex. personuppgifter (mer om det nedan). En annan sak, som det är viktigt att komma överens om vid datadelning, är formatet på data (standard) som man vill dela med varandra. Den aspekten ligger dock utanför denna rapport.

Datadelning i morgon kan fortsätta på den inslagna vägen (att data primärt delas B2B genom avtal). På EU-nivå förs dock en diskussion om det finns ett behov av förändrat regelverk kring datadelning på en övergripande generell nivå. EU ser att det finns risk för att för mycket data samlas hos ett företag, vilket i sin tur försvårar ett fritt flöde av data. I framtiden kan det komma tvingande lagstiftning på generell nivå som reglera vem som ska ha tillgång till data och när etc. för att förhindra att monopol skapas. Risken med detta är att generell (horisontell) lagstiftning används för att lösa ett problem i en vertikal sektor, men kan få oväntade allvarliga konsekvenser för en annan vertikal sektor t.ex. förhindra en tänkt affärsmodell. Det gäller alltså att förstå vad som händer med regelverket för datadelning på den generella/horisontella nivån eftersom den kan få stor påverkan på en viss enskild sektor vertikalt.

Jag har intervjuat projektparter (främst Scania) och branschorganisationen BilSweden. Deras insikter har sedan legat till grund för att identifiera relevanta regelverk och behov av kunskap i projektet. Därefter har jag genomfört desktop research för att förstå hur regelverk påverkar vårt projekt. I projektet har vi även haft workshops där vi diskuterat och analyserat resultatet.

Dispositionen av rapporten är enligt följande. Först kommer en genomgång av aktuella horisontella nationella regelverk. Därefter kommer en genomgång av de vertikala nationella regelverken, följt av en genomgång av kommande lagstiftning på EU-nivå. Till sist kommer en avslutande analys.

2 Dagens generella regelverk för datadelning ur ett svenskt perspektiv

Förenklat kan regelverk för informationsdelning indelas i kategorier efter vem som delar data med vem. Handlar det t.ex. om myndigheter som delar data eller företag som delar data? Det finns också regelverk som är generella och riktar sig till alla. Generella regler kan även beskrivas som horisontell lagstiftning. Här följer ett urval av de viktigaste generella regelverken som handlar om datadelning utifrån vem regelverket berör mest. Samtidigt innebär inte denna indelning att någon annan aktör kan bortse ifrån regelverket.

2.1 Regelverk som alla behöver ta hänsyn till

2.1.1 EU:s allmänna dataskyddsförordning

Dataskyddsförordningen[3] kan vara en utmaning när personuppgifter delas mellan olika aktörer. På engelska heter förordningen General Data Protection Regulation (GDPR). GDPR används därför ofta som ett namn för denna lagstiftning. I dataskyddsförordningen regleras skyddet av enskilda individers grundläggande fri- och rättigheter i samband med behandling av personuppgifter, men också det fria flödet av personuppgifter inom EU. Med personuppgifter avses varje upplysning som direkt eller indirekt kan kopplas till en levande individ. Anonymiserad data anses inte vara en personuppgift. Dataskyddsförordningen skiljer också på personuppgifter som är särskilt känsliga t.ex. en persons hälsotillstånd och uppgifter som inte är särskilt känsliga. Alla typer av befattningar med personuppgifter är att anses som personuppgiftsbehandling oavsett om det är en myndighet eller ett företag som utför behandlingen. Förordningen listar ett antal grundläggande dataskyddsprinciper t.ex. ändamålsbegränsning och lagringsminimering. Den registrerade har också ett antal rättigheter t.ex. rätten att bli glömd och rätt till dataportabilitet. Om ett företag bryter mot dataskyddsförordningen finns det risk för att höga sanktionsavgifter döms ut. I Sverige kompletteras dataskyddsförordningen av lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

2.1.2 Data och kamerabevakningslagen

På ett modernt fordon idag finns flera kameror integrerade. Kamerabevakningslagen (2018:1200) tar sikte på användningen av kameran. Enligt 3 § kamerabevakningslagen är lagen tillämplig om en kamera används på ett sätt som innebär varaktig eller regelbundet upprepad personbevakning utan att manövreras på platsen. Detta skulle kunna vara ett fordon utrustat med en fast kamera, som regelbundet trafikerar och filmar en viss plats. En dashcam omfattas däremot inte av lagstiftningen då den enkelt går att ta med sig (inte en fast installation).

Kamerabevakningslagen träffar främst myndigheter och deras kameraanvändning då en sådan användning många gånger kräver tillstånd från länsstyrelsen. Men företag är skyldig att informera om bevakningen genom att sätta upp skyltar och följa regler om tystnadsplikt. De bilder som kameran samlar in omfattas av dataskyddsförordningen under förutsättning att det rör sig om personuppgifter. Det medför i sin tur att kamerabevakningen måste vara förenlig med de krav som ställs i dataskyddsförordningen.

2.1.3 Skyddslagen och skyddsobjekt

Ett autonomt fordon tar hjälp av sina kameror för att förstå och navigera i sin omgivning. Samtidigt finns det byggnader, anläggningar, områden etc. som inte får filmas (avbildas) s k skyddsobjekt då det finns risk för sabotage, terroristbrott, spioneri

[3] Europaparlamentet 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 upphävandet av direktiv 95/46/EG.

samt grovt rån avseende verksamheten som pågår där. I skyddslagen (2010:305) finns bestämmelser om skyddsobjekt. Den som gör försök med autonoma fordon behöver kontrollera att det inte finns skyddsobjekt längs fordonets väg.

2.1.4 Data och säkerhetsskyddslagstiftning

Det finns samhällsviktiga verksamheter som måste fungera även vid en allvarlig kris eller som det av andra skäl finns starka skäl för ska förbli hemliga. När det gäller krisberedskap är också vissa samhällsfunktioner viktigare än andra. Det handlar om verksamheter som måste finnas på plats för att inte skapa en kris och verksamheter som måste finnas på plats för att hantera en kris om den trots allt skulle inträffa. De samhällsviktiga verksamheterna består i stor utsträckning av olika flöden och processer som på olika sätt utnyttjar infrastrukturer. Avbrott i en verksamhet påverkar dessutom lätt även andra samhällsviktiga verksamheter. Om logistikkedjan av t.ex. läkemedel, drivmedel och livsmedel störs kan det få mycket allvarliga konsekvenser för samhället vilket i sin tur skadar allmänhetens förtroende för samhällets förmåga.

Det finns säkerhetskänsliga verksamheter som omfattas av säkerhetsskyddslagen (2018:585) då de till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd. I sådana verksamheter ska verksamhetsutövaren vidta relativt långtgående åtgärder för att skydda informationen. Säkerhetsskyddslagen reglerar t.ex. hur och när en säkerhetsskyddsanalys ska genomföras samt uppföljning av säkerhetsarbetet. Lagen träffar större knutpunkter inom transportsektorn, men sannolikt även verksamheter som har en särskilt stor överblick över logistiken i landet.

På EU-nivå förhandlas det s k CER-direktivet[4] som kommer att omfatta samhällsviktiga tjänster däribland transporter.

2.1.5 Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS)

Nätverk och informationssystem är viktiga i dagens digitala samhälle och behöver således vara tillförlitliga. För att upprätthålla ekonomisk och samhällelig verksamhet behöver de skyddas. På EU-nivå finns gemensamma bestämmelser i form av det s k NIS-direktivet.[5] Genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster har direktivet genomförts i svensk rätt.

Lagstiftningen går ut på att leverantörer ska vidta rimliga och lämpliga säkerhetsåtgärder för att hantera risker och incidenter i nätverk och informationssystem. Leverantörerna kan finnas både i privat och i offentlig sektor. Lagstiftningen skiljer vidare på leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster. Lagen pekar ut sju sektorer som skyddsvärda inom samhällsviktiga tjänster, däribland transporter. En leverantör av samhällsviktiga tjänster kan t.ex. vara en leverantör av vissa tjänster inom intelligenta transportsystem. En leverantör av digitala tjänster kan vara en juridisk person som tillhandahåller en

[4] Com (2020) 829 final.
[5] Europaparlamentet och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en höggemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

internetbaserad marknadsplats, en internetbaserade sökmotor eller en molntjänst oavsett sektor.

EU-kommissionen har lämnat förslag på ett nytt NIS2-direktiv[6], som ska ersätta det nuvarande direktivet. Förslaget ligger när detta skrivs hos triologen. Triologen innebär en trepartsförhandling. Europaparlamentet, Europeiska unionens råd och Europeiska kommissionen behandlar gemensamt ett lagstiftningsärende.

2.2 Regelverk med tyngdpunkt mot myndigheter

Regeringen antog den 22 juni 2017 en nationell strategi för samhällets informations- och cybersäkerhet (skr. 2016/17:213). Strategin är tänkt att vara en plattform för Sveriges arbete inom detta område samt lyfta fram regeringens prioriteringar och omfattar hela samhället för att bevara ett öppet demokratiskt samhälle. Med informations- och cybersäkerhet avses en uppsättning säkerhetsåtgärder för att bevara konfidentialitet, riktighet och tillgänglighet hos information. Det handlar både om informationen i sig och om de system som används för att hantera information.

2.2.1 Offentlighet och sekretess

För att individer ska kunna tillvarata och utöva sina fri- och rättigheter behövs tillgång till information. Samtidigt finns det uppgifter som är känsliga och behöver skyddas. Offentlighet och sekretess är också intressant ur perspektivet datadelning B2G/G2B. En myndighet har allmänna handlingar som på begäran kan lämnas ut till allmänheten s.k. offentlighetsprincipen (2 kap. 1 § tryckfrihetsförordningen (TF)). Detsamma gäller även för juridiska personer. Rätten att ta del av allmänna handlingar omfattar endast sådana handlingar som inte är sekretessbelagda. Det finns sekretessbestämmelser som är generella och sekretessbestämmelser som gäller för vissa verksamheter. Det finns även mer eller mindre stränga sekretessbestämmelser. I offentlighets- och sekretesslagen (2009:400) (OSL) ges regler för när en allmän handling kan sekretessbeläggas. Det är möjligt att sekretessbelägga en handling om det krävs med hänsyn till exempelvis

- rikets säkerhet,
- intresset av att förebygga eller beivra brott,
- det allmännas ekonomiska intresse, eller
- skydda enskildas personliga eller ekonomiska förhållanden. (2 kap. 2 § TF).

Ett skäl till att göra undantag är alltså skyddet för enskilds personliga eller ekonomiska förhållanden eller det allmännas ekonomiska intresse. Undantag på grund av upphovsrätten kan föras hit (1 kap. 11 § TF). Samtidigt ska allmänna handlingar oavsett upphovsrätten tillhandahållas enligt 2 kap. tryckfrihetsförordningen (26 b § upphovsrättslagen (190:729)). Huvudregeln är alltså att allmänna handlingar som skyddas av upphovsrätten ska tillhandahållas för den som begär det. Men det innebär inte att den som tar emot handlingen har rätt att använda det som är upphovsrättsligt

[6] Com (2020) 823 final.

skyddat utan tillstånd t.ex. kommersiellt. Den som har fått ut handlingen är underkastad de regler som gäller för upphovsrätt. När det gäller informationsfrihet och upphovsrätt finns alltså en motsatsställning.

2.2.2 Public Sector Information och direktivet om öppna data

Sverige har sedan en lång tid tillbaka en tradition med att allmänna handlingar som huvudregel ska vara offentliga. Ute i Europa finns inte samma rättstradition, men på EU-nivå pågår ett arbete med att skapa en ”European Data Economy” som går ut på att ge EU-medborgare en bredare tillgång till data från den offentliga sektorn s k öppna data. EU-kommissionen ser data som en nyckelresurs för innovation, jobbskapande och samhällelig utveckling i allmänhet. Med öppna data avses data i öppna format som kan utnyttjas, vidare utnyttjas och sedan delas fritt av vem som helst för valfritt ändamål. EU-kommissionen beslöt under 2019 om ett nytt öppna data-direktiv.[7] Öppna data-direktivet är ännu inte genomfört i Sverige utan ny lagstiftning förväntas under 2022.

Öppna data i offentligrättslig regi i Sverige brukar nämnas i samma sammanhang som lagen (2010:566) om vidareutnyttjande av handlingar från den offentliga förvaltningen (den s.k. PSI-lagen) som vilar på ett äldre EU-direktivet. PSI står för Public Sector Information. Det är inte alltid enkelt att förena den svenska offentlighetsprincipen och tillgång till allmän handling med tankarna bakom PSI-lagen. Ett sätt att beskriva skillnaden är att offentlighetsprincipen handlar om att tillgängliggöra en allmän handling medan PSI-lagen handlar om att tillhandahålla information dvs. i vilket format (hur) och med vilka avgifter och andra villkor. Det måste alltså först finnas en nationell bestämmelse som ger tillgång till informationen innan den kan vidare utnyttjas. En annan skillnad är att offentlighetsprincipen förutsätter att det finns en begäran från en medborgare som myndigheten svarar på. PSI-lagen handlar i stället om att myndigheter (och andra) ska arbeta aktivt med att tillhandahålla öppna data på egen hand. En utmaning i detta sammanhang är att PSI-lagen inte gäller för handlingar som tredje man innehar rätt till enligt upphovsrättslagen (3 § p 7 PSI-lagen).

2.2.3 Fria flödesförordningen

Fria flödesförordningen[8] går ut på att ge en rättslig säkerhet för företag att behandla sin data var som helst *inom* EU (dataportering). En medlemsstat kan inte kräva i lagstiftning att data ska lokaliseras till det egna landet (t.ex. lagras på servrar eller uppfylla en nationell standard) om det inte är motiverat av allmänt säkerhetsskäl. Förordningens syfte är att säkra principen om fritt flöde av data, *som inte är personuppgifter*, inom EU i syfte att främja en framväxande dataekonomi genom att t.ex. förhindra att data låses in hos en leverantör av databehandlingstjänster/ molntjänster. Samtidigt ska förordningen också underlätta för en myndighet att ta del

[7] Europaparlamentet och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn.
[8] Europaparlamentet och rådets förordning (EU) 2018/1807 av den 14 november 2018 om ram för det fria flödet av andra data än personuppgifter i Europeiska unionen.

av data som lagras i en annan medlemsstat. Förordningen är inte tillämpbar på databehandling som äger rum utanför EU.

Den fria flödesförordningen begränsar inte företags avtalsfrihet vad gäller beslut om var deras data ska behandlas inom EU. I denna del är det i stället tänkt att branscher ska t.ex. utarbeta en uppförandekod för fritt flöde av data inom EU. Ett EU-initiativ inom detta område är Switching Cloud Providers and Porting Data (SWIPO), som arbetar med att ta fram självreglerande uppförandekoder.

2.2.4 EU:s cybersäkerhetsakt

EU:s cybersäkerhetsakt[9] syftar till att uppnå en hög nivå i fråga om cybersäkerhet, cyberresiliens, och förtroende inom unionen och säkerställa en väl fungerande inre marknad. I förordningen regleras framför allt tre områden.

1) En permanent organisation införs - Europeiska byrån för nät- och informationssäkerhet –
2) som på begäran ska bistå medlemsstater operativt vid gränsöverskridande IT-incidenter samt
3) ska utveckla och förvalta ett EU-ramverk för certifiering av it-säkerhetsprodukter och tjänster.

Genom förordningen ska också medlemsstater etablera tillsynsmyndigheter för cybersäkerhetscertifiering. Sverige har sett över den nationella lagstiftningen och anpassat den till förordningen. Resultatet har blivit en kompletterande lagstiftning – lagen (2021:553) med kompletterande bestämmelser till cybersäkerhetsakten där det t.ex. finns bestämmelser om tillsyn och sanktionsavgift. Försvarets materielverk är nationell tillsynsmyndighet. EU arbetar vidare inom detta område och i framtiden kan lagstiftning komma för t.ex. standard för cybersäkerhet kopplat till Internet of Things.

På sikt kan regelverket få betydelse för företag då regelverket kan resultera i nya standarder för hur datadelning kan ske på ett säkert sätt.

2.3 Regelverk som riktar sig mer mot företag

I princip råder avtalsfrihet när det gäller datadelning B2B dvs. ett företag bestämmer själv vem som ska ha tillgång till företagets data och på vilka villkor. Eftersom det inte finns någon specifik reglering som skyddar data i sig blir avtalet mellan inblandade parter viktigt för att reglera olika frågor. Konsekvensen av detta blir att data praktisk delas på många olika sätt. Det finns dock vissa sektorsundantag som har tvingande krav på datadelning (se nedan). Dataskyddsförordningens krav på dataportabilitet på den registrerades begäran för personuppgifter kan också ses som ett exempel på tvingande datadelning mellan företag. Datadelning mellan företag är ett förhållandevis nytt område och området har ännu inte fått ett stort genomslag. EU-kommissionen

[9] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

uppskattade 2017 att 6 % av företagen arbetar med datadelning i sin verksamhet.[10] Samtidigt ser EU-kommissionen att det finns en risk för att stora mängder data samlas hos ett fåtal aktörer och arbetar för att öka konkurrensen och tillgången till data.

Under 2018 gav EU-kommissionen ut riktlinjer för datadelning mellan företag såvitt avser data som inte utgör personuppgifter och som ingår i Internet of Things och för produkter och tjänster som bygger på maskingenererad data som skapats genom sådana föremål.[11] Enligt EU-kommissionen bör följande fem principer beaktas i avtal om datadelning mellan företag.

- Öppenhet
- Skapande av gemensamma värden
- Respekt för varandras kommersiella intressen
- Säkerställa att konkurrensen inte snedvrids
- Minimerad inlåsning av data

I samma riktlinjer uttalade också EU-kommissionen ett antal principer om datadelning mellan företag och myndigheter. I texten lyfts fram som ett exempel datadelning mellan fordonstillverkare – myndighet i syfte att öka trafiksäkerheten och bidra till bättre trafikledning. Enligt EU-kommissionen ska följande nyckelprinciper reglera datadelning företag – myndighet.

- Proportionalitet i användningen av data från den privata sektorn
- Ändamålsbegränsning
- Inte vålla skada
- Villkor för utnyttjande av data
- Minska begränsningarna hos data från den privata sektorn
- Öppenhet och samhällsdeltagande

2.3.1 Elektronisk kommunikation

Enligt lagen (2003:389) om elektronisk kommunikation är den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst skyldig att vidta tekniska och organisatoriska åtgärder för att skydda uppgifter som behandlas i samband med tillhandahållandet av tjänsten. Där finns också bestämmelser om att leverantören ska säkerställa rimliga krav på driftsäkerhet samt rapportera incidenter till Post- och telestyrelsen.

På EU-nivå finns ett nytt EU-direktiv om inrättande av en europeisk kodex för elektronisk kommunikation.[12] Regeringen har föreslagit att en ny lag ska ersätta lagen om elektronisk kommunikation under 2022, men när detta skrivs har riksdagen inte fattat något beslut i frågan.

[10] EU-commission, Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability (2017).
[11] Communication from the Commission to the European Parliament, the Council and Social Committee and the Committee of the Regions – Towards a common European Data Space, COM (2018) 232.
[12] Europaparlamentet och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation.

2.3.2 Data och plattformar

Plattformsförordningen[13] har till syfte att främja rättvisa villkor och transparens för *företagsanvändare* av online baserade förmedlingstjänster. Med online baserade förmedlingstjänster s k plattformar menas bl.a. digitala marknadsplatser där konsumenter kan köpa varor eller tjänster från olika bolag, men också sökmotorer omfattas av förordningen. Plattformsförordningen ställer t.ex. krav på att företag som äger plattformar ska utforma sina användarvillkor på ett enkelt och begripligt sätt, förvarna sina företagsanvändare om ändringar av användarvillkor och motivera sina beslut att avbryta eller avsluta sina tjänster. För företag som äger sökmotorer gäller bl.a. att de ska ge enkel och begriplig information om de parametrar som bestämmer rangordningen på sökmotorn.

Plattformsförordningen har inga bestämmelser som i sig direkt reglerar datadelning. En möjlig framtida utveckling är att sådana regler införs.

2.3.3 Direktiv om tillhandahållande av digitalt innehåll och digitala tjänster

EU vill skydda konsumenter när de köper digitala tjänster på internet och ser därför att nya konsumentköpregler införs. EU har tagit fram ett direktiv för detta ändamål.[14] Direktivet träffar avtal där en näringsidkare ska tillhandahålla eller utveckla ett digitalt innehåll eller en digital tjänst till en konsument. Enligt direktivet ska nya bestämmelser vara införda senast den 1 januari 2022. Förslaget är att direktivet införs i svensk rätt genom en ny lag – lagen om konsumentskydd vid köp och vissa andra avtal som ska ersätta den nuvarande konsumentköplagen.[15] Den nya lagen föreslås bli tvingande till fördel för konsumenterna. Lagförslaget innehåller bl.a. regler om när det ska anses föreligga fel, påföljder vid fel, hur betalning ska gå till och hur uppdateringar ska tillgängliggöras. Riksdagen har när detta skrivs inte fattat något beslut i frågan.

2.3.4 Data och upphovsrätt

Viktigt att komma ihåg, som en utgångspunkt, är att data dvs. information i allmänhet inte är skyddat på något särskilt sätt utan kan användas fritt. Upphovsrätt kan därmed endast ge ett begränsat skydd för viss data. Förenklat kan man säga att det finns två huvudspår. Det första spåret handlar om skydd för kod (jfr text i en roman). Det andra spåret handlar om skydd för databaser (jfr text i ett uppslagsverk). Sedan tillkommer dimensionen att viss data har gjorts öppen dvs. uttryckligen inte omfattas av upphovsrätt, medan kommersiell data omfattas av upphovsrätt. Vidare är data och upphovsrätt en utmaning vid datadelning och avtalsskrivning med mängder av restriktioner/begränsningar för vad som får göras med data. Data delas ofta via licenser. I detta sammanhang är det viktigt att hålla reda på om den som innehar data

[13] Europaparlamentet och rådets förordning (EU) 2019/1150 av den 20 juni 2019 om främjande av rättvisa villkor och transparens för företagsanvändare av online baserade förmedlingstjänster.
[14] Europaparlamentet och rådets direktiv (EU) 2019/770 av den 20 maj 2019 om vissa aspekter på avtal om tillhandahållande av digitalt innehåll och digitala tjänster.
[15] Se vidare SOU 2020:51.

har besittningsrätt (kontrollerar data rent fysiskt) och/eller har ”äganderätt” (har rätt att bestämma över hur data används).

Data i sig är heller inte nödvändigtvis värdefullt. Det är användandet i en viss kontext som ger exempelvis en möjlighet att dra slutsatser eller omsätta till en prestation. En viss mängd data, eller data samlad på ett visst sätt, kan också innebära att det går att se mönster, göra jämförelser och analysera t.ex. vissa händelser eller verksamheter. Här finns ofta det affärsmässiga perspektivet, eftersom analysen kan ge underlag för att effektivisera eller hitta nytt utrymme för en ny affär eller till och med affärsmodell. I detta sammanhang kan det vara värt att nämna att en AI kan inte få upphovsrätt till sitt skapande utan endast människor omfattas av upphovsrätten.

Utgångspunkten är att litterära och konstnärliga verk skyddas av upphovsrätt. Rättigheten är tvåfaldig, dels en rätt att dra ekonomisk nytta av uttrycket, dels en rätt att bli erkänd som uttryckets skapare (upphovsman). Den första delen ger innehavaren rätt att trycka, visa, framföra eller sälja verket till allmänheten. Den andra delen innebär en rätt att bli omnämnd som upphovsman eller en möjlighet att skydda verket mot kränkande användning. Upphovsrätt gäller per automatik enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk (URL). Det behövs inte någon myndighets tillstånd eller någon ansökan eller registrering. Spridning av verket ger rätt till ekonomisk ersättning och ideellt erkännande. Den ekonomiska rätt som följer av upphovsskydd kan alltså generera intäkter till verkets skapare. Det är uttrycket som skyddas, och inte den underliggande idéen. Rättigheterna uppstår när verket skapas och varar normalt sett i 70 år efter upphovsmannens död. Verket får sedan fritt spridas och återges. Skydd enligt upphovsrättslagen kräver att uttrycket når s.k. verkshöjd, vilket betyder att verket måste framstå som att det har ett visst mått av självständighet och originalitet.

Hur kommer det sig att staten upprätthåller vissa ensamrätter för enskilda? Anledningen är att det anses vara ett incitament för att investera i vad som kan bli uppfinningar eller konstnärliga verk. Ny kunskap kan bli offentlig och spridd utan att förlora i värde för den som har ensamrätt till utnyttjandet av t.ex. ett verk eller uttryck. Kontakter - och kontrakt - mellan den som tänker eller omsätter till en konstruktion (upphovsmakare) och den som producerar eller omsätter till en kund blir lättare. Det betyder att tillgången kan vidarebefordras på ett sätt så att den går att sälja, att den kommer ut på en marknad, och därmed komma konsumenter och samhälle till nytta. En balans är dock absolut nödvändig. Ett för starkt immaterialrättsligt skydd minskar möjligheterna att vidareutveckla och bygga på befintlig kunskap. Det riskerar då att i stället hindra innovation och hämma konkurrensen.

Av intresse för det här projektet är hur databaser skyddas av URL i 49 § (det så kallade katalogskyddet). Den som har sammanställt uppgifterna har rätt att ändra och bearbeta insamlade data, framställa exemplar av arbetet och göra det tillgängligt för allmänheten t.ex. genom spridning. Denna rätt är överlåtbar genom avtal och licenser. Men det innebär också att skaparen enligt upphovsrätten kan förbjuda spridning av databasen. Upphovsrätten är också sådan att all användning som mottagaren gör med data måste vara reglerat i avtalet. Om avtalet inte reglerar en viss användning av data är det inte tillåtet för mottagaren att göra det. Det föreligger inte alltså någon automatisk rätt för en mottagare av data att göra vad man vill med den bara för att man har tillgång till data.

2.3.5 Data och företagshemligheter

Upphovsrätt är ett sätt att skydda egendom. Men egendom kan även skyddas med hjälp av lagen (2018:558) om företagshemligheter (LFH). Det ena skyddet utesluter inte det andra utan snarare kompletterar de varandra. Enligt 2 § lag om företagshemligheter avses med företagshemligheter bl.a. information om affärs- eller driftsförhållande i en näringsidkares rörelse. Skyddet gäller för information som varken som helhet eller i den form dess beståndsdelar ordnats och satts samman (t.ex. en databas över varor) är allmänt känd hos eller lättillgängligt för den som normalt har tillgång till information av aktuellt slag. Informationen kan vara dokumenterad, till exempel i form av ritningar eller modeller, eller helt enkelt vara sådant som bara ett fåtal personer i företaget känner till. Det är viktigt att i avtal reglera att de personer som har kännedom om företagshemligheterna inte tar informationen med sig, om de slutar eller byter jobb, oavsett om de har tillgång till företagshemligheterna i muntlig eller skriftlig form. För att få skydd enligt den lagen måste företaget aktivt försöka hålla informationen hemlig och göra det tydligt för omgivningen, t.ex. genom att låsa in ett recept i kassavalvet eller ha olika behörigheter för tillgång i system som arkiv, bokföring, intranät etc. Ett annat krav är att ett röjande av informationen ska medföra skada i konkurrenshänseende för innehavaren. Företagshemligheter kan lagligen bara delas om innehavaren samtycker till detta.

2.3.6 Data och konkurrensrätt

Konkurrensrätten har också betydelse för datadelning. Om företagshemligheter handlar om sådan data som företaget inte vill dela med andra, handlar konkurrensrätten i detta fall om data som företaget vill dela med andra, men inte ska dela t.ex. information om priser, affärsvillkor, marknader, produktion, teknisk utveckling och investeringar. Konkurrensrätten kan också utgöra en drivkraft för förändring av regelverket för datadelning. Om ett fåtal aktörer har tillgång till stora datamängder och missbrukar denna ställning kan resultatet bli skadlig konkurrens (monopol) som t.ex. EU försöker bryta upp genom nya regelverk. Exempelvis innehåller artikel 101 och 102 i fördraget om Europeiska unionens funktionssätt bestämmelser som syftar till att motverka kartellbildningar och missbruk av dominerande ställning på den inre marknaden.

Konkurrenslagen (2008:579) (KL) har till syfte att undanröja och motverka hinder för en effektiv konkurrens i fråga om produktion av och handel med varor, tjänster och andra nyttigheter (1 kap. 1 § KL). Lagen gäller för fysiska och juridiska personer som bedriver verksamhet av ekonomisk eller kommersiell natur (dock inte verksamhet som avser myndighetsutövning). Konkurrensrätten träffar således någon som har för stor andel av datamängden på marknaden och använder övertaget till att snedvrida konkurrensen (monopol).

Konkurrenslagen skiljer på vertikala och horisontella samarbeten. Konkurrenslagen har förenklat lättare för att acceptera vertikala samarbeten mellan företag och svårare för att acceptera horisontella samarbeten oavsett om företagen är konkurrenter eller inte.

Enligt konkurrenslagen kan samarbeten om datadelning godtas om de uppfyller samtliga fyra kriterier som anges i 2 kap. 2 § KL. De som samarbetar har bevisbördan

för att samarbetet kan godtas. Det första kriteriet går ut på att det måste uppstå en effektivitetsvinst genom samarbetet. Det andra kriteriet går ut på att samarbetet måste vara till nytta för konsumenterna som helhet. Enligt det tredje kriteriet krävs vidare att avtalet etc. inte medför konkurrensbegränsningar som inte är nödvändiga för att uppnå de positiva effekterna i de två första kriterierna. Enligt det sista kriteriet får samarbetet inte sätta konkurrensen ur spel.

3 Dagens sektorsspecifika regelverk för datadelning ur ett svenskt perspektiv

Utöver de generella reglerna för datadelning kan datadelning inom en viss sektor vara reglerad. I dessa fall brukar man tala om vertikal lagstiftning. En sådan reglering träffar vissa förhållanden där det ansett vara särskilt påkallat med lagstiftning. Exempel på områden med sektorsspecifik lagstiftning är fordon, elektricitet och intelligenta transportsystem.

3.1 Datadelning för spårbarhet avseende vissa varor

EU har också regler kring hur data ska delas i logistikkedjan för vissa varugrupper för att skapa spårbarhet mellan vara och transport. Generellt kan man säga att det finns två olika sätt att dela data på. För livsmedel (som är en äldre lagstiftning) delas data i en kedja med många länkar efter varandra. En aktör inom livsmedelsbranschen delar data med den aktör som är före och efter i logistikkedjan. EU har i senare lagstiftning för tobak och läkemedel i stället valt modellen att det finns en central aktör som samlar in data från alla andra (jfr ett hjul med ekrar). Det kan inte uteslutas att fler varugrupper i framtiden får ett eget regelverk kring datadelning.

3.1.1 Livsmedel

Den mat som vi äter måste vara säker, den får inte vara skadlig för hälsan eller på annat sätt vara olämplig som människoföda. Under 1980- och 1990-talet inträffade framför allt två händelser som bidrog till att myndigheter insåg att livsmedel måste kunna spåras. I Storbritannien handlade det om att kunna spåra smittat kött (Galna ko-sjukan) och i Belgien handlade det om att spåra dioxin. Dioxin hade blandats in i djurfoder, som via djuren sedan spreds till människor. För att upprätthålla konsumenternas förtroende för livsmedel behövde myndigheter och företag snabbt kunna spåra och sedan dra tillbaka farliga livsmedel från marknaden för att minska skadeverkningar samt informera konsumenter om vad som hänt. För att kunna göra detta krävdes ett regelverk för spårbarhet. Spårbarhetskravet innebär att alla livsmedel måste kunna spåras och följas genom alla stadier i produktions-, bearbetnings- och

distributionskedjan.[16] De som transporterar livsmedel behöver alltså kunna redogöra för hur livsmedlet har transporterats.

Centralt för livsmedelslagstiftningen är Europaparlamentet och rådets förordning (EG) 178/2002 om allmänna principer och krav för livsmedelslagstiftning, om inrättande av Europeiska myndigheten för livsmedelssäkerhet och om förfaranden i frågor som gäller livsmedelssäkerhet. Kompletterande bestämmelser finns i livsmedelslagen (2006:804). Förordningen utgår ifrån ett antal principer som ska upprätthållas bl.a. att livsmedel ska vara säkra (art. 14). Livsmedelssäkerhet handlar bl.a. att livsmedel inte får skada vår hälsa eller vara olämpliga som livsmedel. Livsmedel som inte är säkra ska inte släppas ut på marknaden. En förutsättning för att kunna vidta åtgärder, så att livsmedelssäkerhet uppnås, är att möjliggöra spårbarhet genom hela livsmedelskedjan (art. 3 p. 15).

Den viktigaste regeln om spårbarhet finns i art. 18 i förordningen och gäller alla livsmedelsföretagare i hela produktions-, bearbetnings-, och distributionskedjan t.ex. transportörer. Spårbarheten gäller ett steg bakåt respektive ett steg framåt i distributionskedjan (extern spårbarhet) och gäller varors fysiska flöde (inte ekonomiska transaktioner). Spårbarhetskravet gäller inte för intern spårbarhet dvs. hur livsmedel transporteras inom ett företag. Av art. 18 framgår att livsmedelsföretag måste ha ett system för spårbarhet (kvitton, fakturor, leveranssedlar, följesedlar, etc.), men anger inte i detalj hur det ska utformas så länge det uppfyller reglernas avsikt och ändamål. Livsmedelsföretag måste också spara information för att möjliggöra spårning. Till regelverket kommer olika branschstandarder som ställer högre krav på spårbarhet än vad förordningen gör.[17] Vissa livsmedel har ännu högre krav på spårbarhet t.ex. fisk där det går att se vem som fångat fisken och var. Kravet på spårbarhet har i sin tur drivet fram ”smarta” avtal för fisk dvs. sensorer mäter hur fiskfiléerna mår under transporten och om de transporterats optimalt genom hela fraktkedjan får transportörerna bättre betalt.

Fördelen med att ha en sektorslagstiftning som så att säga tvingar fram datadelning mellan olika aktörer i branschen är att lagstiftningen senare kan byggas på med frivilliga initiativ. Samarbetet är redan i gång. Se nedan exemplet *EU code of conduct on agricultural data sharing by contract agreement*. Skillnaden mellan det tvingande regelverket och den frivilliga överenskommelsen är att i den frivilliga överenskommelsen kan andra datasets som t.ex. data från energiförbrukning från jordbruksmaskiner tas med också dvs. data som primärt inte har med livsmedelssäkerhet att göra.

3.1.2 Läkemedel och medicintekniska produkter

Andra branscher, som också har höga krav på spårbara transporter av varor, är läkemedel och medicintekniska produkter. Läkemedel och medicinteknik måste vara säkra för människor att använda. Utmaningar för läkemedelsdistribution t.ex. kan vara att varorna är stöldbegärliga, att de byts ut mot förfalskningar eller att varan måste

[16] Art. 1 p. 3 i Europaparlamentets och rådets förordning (EG) nr 178/2002 av den 28 januari 2002 om allmänna principer och krav för livsmedelslagstiftning, om inrättande av Europeiska myndigheten för livsmedelssäkerhet och om förfarande i frågor som gäller livsmedelssäkerhet.
[17] Exempelvis Svensk Dagligvaruhandel – Säker mat i din butik och Fiskbranschens Vägledning.

transporteras vid en viss temperatur för att bibehålla en viss kvalitet. Det finns också ett gemensamt ansvar i form av att incidenter kan inträffa i hela kedjan och att en svag länk får hela kedjan att brista. Spårbarhet blir då något som alla i distributionskedjan är intresserade av att arbeta med (gemensamt ansvar). Fördelarna branscherna uppnår med detta är bl.a. säkra distributionskanaler.

När det gäller medicinteknik har alla aktörer i kedjan mellan tillverkare och slutanvändare någon form av ansvar för att produkternas säkerhet kan garanteras. Inom medicinteknik är det distributören som har huvudansvaret för att produkter bl.a. fraktas och förvaras på rätt sätt enligt tillverkarens instruktion (art. 14 p. 3 Europaparlamentets och rådets förordning (EU) 2017/745 av den 5 april 2017 om medicintekniska produkter). Om transport och lagring inte uppfyller kraven ska distributören tillsammans med andra vidta korrigerande åtgärder för att få produkten att överensstämma med kraven, dra tillbaka produkten eller återkalla den.

3.1.3 Tobak

Även tobak ska märkas och spåras enligt 3 kap. 7–11 §§ lagen (2018:2088) om tobak och liknande produkter.[18] Spårbarhet för tobak finns främst till för att motverka illegal handel med tobaksvaror inom EU, men även för att garantera att tobaken är äkta. Spårbarhetssystemet bygger på identitetsmärkning och identifieringskod. Alla aktörer som ingår i leveranskedjan av tobak har en unik identifieringskod, likaså anläggningar t.ex. en terminal. Alla styckförpackningar har också en unik identitetsmärkning. När styckförpackningar hanteras och transporteras av någon i leveranskedjan ska denne registrera händelsen och skicka informationen till en central databas. Det kan t.ex. handla om att rapportera leveransens destination, avreseplats och mottagare. Tillverkare av tobaksvaror ska tillhandahålla den utrustning som behövs till andra i leveranskedjan. Datalagringen ska ske hos en oberoende tredje part som ska godkännas av Europeiska kommissionen (för att möjliggöra spårbarhet av tobaksvaror inom hela unionen genom t.ex. tekniska standarder). Myndigheter ska vidare ha full tillgång till databasen för att säkerställa oberoende och öppenhet för systemet med spårbarhet.

3.2 Datadelning och fordon

Moderna fordon genererar stora mängder data. EU arbetar på olika sätt med data från fordon. Sedan länge har det funnits ett intresse att samla in utsläppsdata från fordonen för att säkerställa att fordonen följer miljökraven. På senare tid har även effektivare trafiksystem och uppkopplade fordon kommit i fokus.

Generaldirektoratet Mobility and Transport har antagit en strategi *EU:s Sustainable and Smart Mobility Strategy*, där det ingår en bilaga med en åtgärdslista bestående av 82 punkter.[19] Av intresse för denna rapport är främst två punkter.

- *Punkt 52. Review the current EU type approval legislation to facilitate car data-based services including interaction with energy system 2021*

[18] Lagstiftningen bygger delvis på genomförande av art. 15 och 16 i tobaksproduktdirektivets (2014/40/EU) regler om spårbarhet och säkerhetsmärkning.
[19] European Commission, Mobility and Transport, Sustainable and smart mobility strategy.

- *Punkt 53. Propose a new regulatory framework to open up access to car data to mobility services 2021*

Lagstiftning kan förväntas inom dessa områden inom kort.

3.2.1 Digital smart färdskrivare

Enligt lag ska tunga lastbilar och bussar (med vissa undantag) ha en färdskrivare installerad ombord.[20] Färdskrivaren registrerar bl.a. hastighet, tid, positionspunkter, kör- och vilotider samt vem som kör fordonet. Den nuvarande generationerna av digitala färdskrivare är uppkopplade och skickar data till transportföretagets server. Kontrollmyndigheter t.ex. Polismyndigheten kan begära att få tillgång till data från färdskrivare. Regelverket för kör- och vilotider har ändrats under 2020, vilket innebär att nya fordon i framtiden ska ha s.k. smarta färdskrivare installerade.[21] Ännu smartare färdskrivare ska installeras fr.o.m. 2023 (andra generationen). De ska bl.a. visa GPS-data. I framtiden är det meningen att kontrollmyndigheter ska kunna fjärravläsa färdskrivaren. När detta skrivs är ännu inte de tekniska specifikationerna publicerade för andra generationen. Eventuellt finns det en risk för att fordons elarkitektur påverkas av de nya reglerna.

3.2.2 Euro 5, 6 och 7

Alla nya fordon ska klassas efter mängden avgasutsläpp. Traditionellt har kontrollmyndigheters behov av att kunna kontrollera avgasutsläpp drivit på datadelning inom fordonsindustrin t.ex. tillkom ODB-porten ursprungligen för att kunna läsa av utsläppsdata. EU har idag utsläppsklasserna Euro 5 och 6.[22] Utsläppsklasserna regleras i Sverige genom avgasreningslagen (2011:318). Kraven på avgasutsläpp bygger på avgasprovning enligt europeiska provmetoder.[23] I detta ligger att tillverkaren är skyldig att tillhandahålla information och dokumentation dvs. datadelning om fordonets avgasutsläpp inför ett typgodkännande men även efteråt till en tillsynsmyndighet. I framtiden förväntas utökad datadelning mellan fordonstillverkare och myndigheter inom detta område i takt med att utsläppskraven

[20] Europaparlamentet och rådets förordning (EU) nr 15/2014 av den 4 februari 2014 om färdskrivare vid vägtransporter, om upphävande av rådets förordning (EG) nr 3821/85 om färdskrivare vid vägtransporter och om ändring av Europaparlamentets och rådets förordning (EG) nr 561/200 om harmonisering av viss sociallagstiftning på vägtransportområdet

[21] Ändringsförordning (EU) 2020/1054, gäller sedan augusti 2020.

[22] Europaparlamentet och rådets förordning (EG) 715/2007 av den 20 juni 2007 om typgodkännande för lätta personbilar och lätta nyttofordon (Euro 5 och 6) och om tillgång till information om reparation och underhåll av fordon. Se även Europaparlamentet och rådets förordning (EU) 2018/858 av den 30 maj 2018 om godkännande av och marknadskontroll över motorfordon och släpfordon till dessa fordon samt av system, komponenter och separata tekniska enheter som är avsvedda för sådana fordon.

[23] Europaparlamentets och rådets förordning (EG) nr 715/2007 av den 20 juni 2007 om typgodkännande av motorfordon med avseende på utsläpp från lätta personbilar och lätta nyttofordon (Euro 5 och Euro 6) och om tillgång till information om reparation och underhåll av fordon, och Europaparlamentets och rådets förordning (EG) nr 595/2009 av den 18 juni 2009 om typgodkännande av motorfordon och motorer vad gäller utsläpp från tunga fordon (Euro 6) och om tillgång till information om reparation och underhåll av fordon samt om ändring av förordning (EG) nr 715/2007 och direktiv 2007/46/EG och om upphävande av direktiven 80/1269/EEG, 2005/55/EG och 2005/78/EG.

skärps, som kan bli betungande för fordonstillverkare. EU:s nya klimatlag kan på sikt driva fram en ny Euro 7.

I detta sammanhang kan det vara intressant att nämna förordningen 2019/631 om fastställande av normer för koldioxidutsläpp för nya personbilar och för nya lätta nyttofordon[24]. EU har föreskrivet bindande gränsvärden för fordonstillverkare. Enligt förordningen ska tillverkare följa upp och rapportera hur väl personbilars och lätta nyttofordon faktiska koldioxidutsläpp och bränsle- eller energiförbrukning vid körning motsvarar gränsvärdena. Fordonstillverkare ska samla in data från fordonen t.ex. i samband med ett verkstadsbesök och rapportera till myndighet eller i samband med periodisk besiktning.

Ett liknande initiativ är regeringens förslag angående ny lagstiftning om tillgång till information om bränsleförbrukning och koldioxidutsläpp. Syftet med lagen är att tillgodose konsumenters informationsbehov. Förslaget syftar till ett tydligare genomförande av Europaparlamentet och rådets direktiv 1999/94/EG av den 13 december 1999 om tillgång till konsumentinformation om bränsleekonomi och koldioxidutsläpp vid marknadsföring av nya personbilar. Lagstiftningen förväntas träda i kraft under 2022.

3.2.3 Dela data från fordon med 3:e part verkstäder

Det finns verkstäder som är märkesoberoende och verkstäder som är märkesberoende. Traditionellt finns det en osäkerhet från fordonstillverkare att ge märkesoberoende verkstäder tillgång till uppkopplad fordon eftersom det är förenat med säkerhetsrisker t.ex. risk för att en obehörig person kommer åt information om stöldskydd. Samtidigt finns det en misstro från oberoende verkstäder att de inte får tillgång till all data från fordonen, som verkstaden behöver och att det begränsar konkurrensen. Enligt förordning 715/2007[25] och förordning 595/2009[26] ska fordonstillverkare ge tillgång till information om icke-säkerhets- och säkerhetsrelaterad reparation och underhåll till märkesoberoende verkstäder. Säkerhetsrelaterad information kräver mjukvara för att kunna arbeta med fordonet. EU har därför infört regler för märkesoberoende verkstäder. Om de är godkända av SERMI (Forum for Access to Security-Related Vehicle Repair and Maintenance Information) får de arbeta med fordonet uppkopplat. Om de inte är godkända av SERMI får verkstaden endast utföra arbeten som innebär att teknikern inte behöver koppla upp fordonet. SERMI är vidare en behörighetsackreditering på mekanikernivå. Teknikern ska kunna koppla upp sig mot en central europeisk server för att komma åt säkerhetsrelaterad information. Arbetet med att införa SERMI pågår i Sverige.

[24] Europaparlamentet och rådets förordning (EU) 2019/631 av den 17 april 2019 om fastställande av normer för koldioxidutsläpp för nya personbilar och för nya lätta nyttofordon och om upphävande av förordningarna (EG) nr 443/2009 och (EU) nr 510/2011.
[25] Europaparlamentets och rådets förordning (EG) nr 715/2007 av den 20 juni 2007 om typgodkännande av motorfordon med avseende på utsläpp från lätta personbilar och lätta nyttofordon (Euro 5 och Euro 6) och om tillgång till information om reparation och underhåll av fordon.
[26] Europaparlamentet och rådets förordning (EG) 595/2009 av den 18 juni 2009 om typgodkännande av motorfordon och motorer vad gäller utsläpp från tunga fordon (Euro 6) och om tillgång till information om reparation och underhåll av fordon förordning.

3.2.4 Intelligenta transportsystem

Inom intelligenta transportsystem (ITS) blir tillgång till data allt viktigare för t.ex. beslutsfattande, öka trafiksäkerheten och optimera trafikflöden. EU arbetar med fyra olika byggstenar för fordon på väg inom detta område. Dessa är:

- Koordinerade/harmoniserade nationella access punkter (en portal för datautbyte)
- Trans-European Transport Network (TENtec) (är EU-kommissionens informationssystem för t.ex. kartdata för att binda ihop alla trafikslag)
- Trafiksäkerhetsdata
- Data från fordon

Dessa fyra byggklossar är tänkta att leda vidare till en Mobility Data Space (se nedan).

I ITS-direktivet[27] anges att varje medlemsstat ska ha en s k nationell access punkt för datadelning av mobilitetsdata och att varje medlemsstat ska erbjuda en plattform där trafikdata ska göras tillgängligt.[28] Det finns flertalet delegerade akter kopplat till ITS-direktivet som anger hur detta ska förverkligas. De viktigaste är:

Akt A – *Multimodal resinformationstjänster*.[29] Enligt ITS-direktivet måste trafikföretag tillgängliggöra sin kollektivtrafikdata i rätt format. Inom detta område förväntas förslag på ny lagstiftning under 2022 för att underlätta biljettköp för resor som inbegriper olika transportslag (multimodal digital mobility services).

Akt B – *Realtidsdata trafikinformation/Real-Time Traffic Information Service* som handlar om data relaterat till t.ex. trängsel.[30] Just nu genomför EU-kommissionen en översyn av RTTI och ny lagstiftning förväntas under 2022. Utifrån vad som är känt ska RTTI i framtiden omfatta både det statliga och kommunala vägnätet. EU-kommissionen vill även ta in nya typer av data i RTTI och utveckla nya tjänster. EU-kommissionen anger t.ex. i sitt förslag att data genererat från fordon ska ingå i RTTI. Att utvidga RTTI till att omfatta större delen av vägnätet väcker också frågor om hur t.ex. kommunikationen mellan fordon och myndighet ska gå till. Även andra frågor som hur GDPR och e-Privacyförordningen kommer att vara förenligt med RTTI behöver besvaras. När detta skrivs har EU-kommissionens förslag varit öppet för allmänheten att lämna synpunkter på och EU-kommissionen arbetar nu om förslaget utifrån inkomna synpunkter.

[27] Europaparlamentet 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.
[28] Den svenska accesspunkten finns på Welcome - Trafficdata.se
[29] Kommissionens delegerade förordning (EU) 2017/1926 av den 31 maj 2017 om komplettering av Europaparlamentet och rådets direktiv 2010/40/EU vad gäller tillhandahållande av EU-omfattande multimodala reseinformationstjänster.
[30] Kommissionens delegerade förordning (EU) 2015/962 av den 18 december 2014 om komplettering av Europaparlamentet och rådets direktiv 2010/40/EU vad gäller tillhandahållande av EU-omfattande realtidstrafikinformationstjänster.

Akt C – *Vägsäkerhetsrelaterad trafikinformation/Safety-relevant traffic information*.[31] I akten anges bl.a. att viss universell trafikinformationstjänst ska hantera information om t.ex. oskyddad olycksplats, tillfällig hal vägbana och tillfälligt vägarbete och sprida informationen till berörda. Informationen kan komma både från det offentliga och det privata.

EU-kommissionen arbetar med att uppdatera ITS-direktivet utifrån nya riktlinjer och prioriteringar.

Det finns ett antal initiativ inom ITS-området för att skapa öppna plattformar för delning av data i realtid relaterat till trafik. Ett exempel är ett tyskt initiativ Mobility Data Space som kombinerar data från företag och myndigheter. Liknande svenska plattformar är Ericssons Innovation Cloud och Trafiklab (kollektivtrafik data). Utmaningen ligger i att få de olika plattformarna att dela data med varandra. EU vill att en gemensam European Mobility Space utvecklas, som i sin tur kopplar till EU-kommissionens data strategi (se nedan). Inom detta område kan lagstiftning förväntas i framtiden.

4 EU:s arbete med datadelning utanför regelverk

EU arbetar inte bara med tvingande regelgivning för att kontrollera datadelning utan har även andra mer frivilliga verktyg i verktygslådan. I detta sammanhang brukar man tala om ”nudging”. Nudging handlar om att få människor att bete sig på ett visst önskat sätt på frivillig väg, genom olika åtgärder, som gör det enklare för människor att välja rätt.

4.1 Självreglerande datadelning

EU-kommissionen ser gärna att sektorer själva organisera frivilliga regler för datadelning (code of condact). Ett exempel på en sådan frivillig reglering finns inom jordbruket från 2018 *EU code of conduct on agricultural data sharing by contract agreement*. Värd för överenskommelsen är Copa-Cogeca (lantbrukarorganisation på europanivå). Överenskommelsen reglerar inte vilken standard som ska användas vid datadelning utan vilka principer för datadelning som ska tillämpas i avtal om datadelning. Hur ska t.ex. data delas med 3:e part på ett transparent, rättvist och säkert sätt med utgångspunkt i lantbrukarens behov? Målet är att med hjälp av överenskommelsen skapa en marknad för jordbruksdata.

Ett annat exempel är kopplat till fria flödesförordningen där EU gärna ser att branschorganisationer fyller ut regelverket med egna överenskommelser. Ett EU-initiativ inom detta område är Switching Cloud Providers and Porting Data (SWIPO), som arbetar med att ta fram självreglerande uppförandekoder.

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

4.2 Rekommenderad datadelning

Ett annat exempel på hur EU arbetar med datadelning utanför ett tvingande regelverk är rekommendationen om öppen tillgång och bevarande av forskningsdata från offentligt finansierad forskning.[32] Målet är att forskningsdata ska finnas tillgänglig i European Open Science Cloud till 2026 där forskningsdata ska vara lätt att lagra, hitta, dela och återanvända inom EU i en säker och tillförlitlig miljö. I detta arbete är medlemsstaterna viktiga aktörer för att säkerställa att målet nås.

5 Datadelning i morgon – en policyfråga på EU-nivå

5.1 Inledning

Allt börjar med EU:s långtidsbudget (Multiannual Financial Framework) som sätter gränserna för vad EU ska prioritera och finansiera t.ex. olika program och fonder. I december 2020 antogs budgeten *En återhämtningsplan för Europa / Next Generation EU* i syfte att hjälpa medlemsländerna att hantera de ekonomiska och sociala konsekvenserna av coronapandemin för åren 2021–2027.[33] Budgeten ska också säkerställa att medlemsländerna genomför den gröna och digitala omställningen så att de blir mer hållbara och motståndskraftiga i syfte att bekämpa klimatförändringar. Som ett resultat av EU:s långtidsbudget kan det inom de närmaste åren förväntas projekt, reformer och investeringar inom dessa områden. En del av dessa projekt etc. kan komma att rikta sig mot fordonsindustrin.

Olika strategier är också viktiga för att förstå hur EU arbetar. Strategier tas fram gemensamt av Europaparlamentet, Europeiska rådet, Europeiska unionens råd och EU-kommissionen. Det är EU-kommissionens uppgift att sedan omsätta strategierna till konkreta åtgärder. EU-kommissionen har i linje med långtidsbudgeten antagit sex prioriterade delområden för åren 2019–2024.

- En europeisk grön giv
- En ekonomi för människor
- Ett Europa rustat för den digitala tidsåldern
- Ett starkare Europa i världen
- Främjande av vår europeiska livsstil
- En ny satsning på demokrati i Europa

Av intresse för den här rapporten är främst två delområden:

EU:s gröna giv (A European green deal): EU strävar efter att bli klimatneutralt till år 2050. EU:s gröna giv omfattar en handlingsplan för hur detta ska gå till bl.a. vilka investeringar som behövs. Det kommer att finnas en hel del forskningsmedel inom

[32] Kommissionens rekommendation (EU) 2018/790 av den 25 april 2018 om tillgång till och bevarande av vetenskaplig information.
[33] European Commission, (2020) Recovery Plan for Europe – Next Generation EU

detta område att söka. EU:s gröna giv arbetar också med en ny förordning om klimatet i syfte att göra målsättningen bindande för bl.a. medlemsstater. Klimatförordningen kommer att få stor påverkan på fordonsindustrin och kommer att vara en stark drivkraft för omställning av industrin. Ett exempel är en framtida ”Euro 7”, som antagligen kommer att innebära strängare krav på utsläpp från fordon som drivs med bensin eller diesel år 2030. Ett annat exempel kan vara regelverk kring tvingande krav på en hållbar batterivärdekedja för fordon. Båda exemplen kan få stor påverkan på fordonsindustrins affärsmodeller.

Ett Europa rustat för den digitala tidsåldern (Shaping Europe´s digital future): Inom detta område arbetar EU-kommissionen framför allt med tre grundpelare för att säkerställa att den digitala omställningen fungerar för alla människor och företag.

- Teknik som fungerar för människor (en teknik som fungerar i människors vardag och respekterar individers rättigheter).
- En rättvis och konkurrenskraftig ekonomi (små och stora företag ska kunna konkurrera på samma villkor).
- Ett öppet och demokratiskt och hållbart samhälle grundat på europeiska värderingar.[34]

Inom detta område finns det ett flertal förslag på regelverk som är aktuella för denna rapport t.ex. om AI, digitala marknader och uppkoppling. Mer om det nedan.

Under ”Ett Europa rustat för den digitala tidsåldern” finns ytterligare en strategi nämligen *En EU-strategi för data* från 2020 (A European Strategy for data) för åren 2020–2025. Målet är att skapa en inre fungerande och säker marknad för fritt flytande data inom EU till 2030. I denna del ser EU-kommissionen att det i dagsläget finns en bristande tillgång till data, att maktinflytande över data är ojämnt fördelat, att datakvaliteten och interoperabiliteten är bristande samt att respekten för enskildas rättigheter är bristande. I stället vill EU-kommissionen att data ska användas bättre t.ex. i beslutsfattande (jfr big data) och för att höja medborgares livskvalitet.

EU-kommissionen arbetar också med ett gemensamt europeiskt dataområde (*European data space)* som ska möjliggöra uppskalning av datadelning på EU:s inre marknad t.ex. genom data pooler (arbetet hör hemma under en EU-strategi för data).[35] Tillgång till stora mängder data anses vara en konkurrensfördel. Detta ska ske genom ett gemensamt regelverk där individers rättigheter respekteras och med tillförlitlig datadelning grundat i europeiska värderingar. Offentlig data ska vara en hörnsten i utvecklandet av dessa områden, men data ska även komma från privat sektor. Kommissionen ser att det kommer att finnas olika Data Space för olika sektorer t.ex. mobilitet. I detta sammanhang kan det vara värt att nämna samarbetsprojektet GAIA-X som syftar till att åstadkomma en gemensam europeisk molninfrastruktur för olika sektorer t.ex. mobilitet.[36] Ett av målen är att minska beroendet av företag utanför EU

[34] Den som vill veta mer om vad som avses med europeiska värderingar kan t.ex. läsa *Meddelande från Kommissionen till Europaparlamentet, Rådet och Sociala kommittén samt Regionkommittén – EU:s handlingsplan för demokrati* COM(2020)790 final.
[35] Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions (COM/2018/232).
[36] www.gaiax.se

som hanterar vår datainfrastruktur. EU-kommissionen vill ha kvar data inom EU och vill inte gärna lagra data utanför EU.

Under ”Ett Europa rustat för den digitala tidsåldern” finns även en annan strategi för cybersäkerhet för åren 2020–2025. Under denna strategi ligger bl.a. förslaget till ett nytt NIS2-direktiv.

Av intresse för denna rapport är även den äldre strategin *Digital Singel Market* från 2015 för att förverkliga kommissionens huvudsakliga lagstiftningsförslag inom detta område. Målet är att skapa *en* digital marknad för EU:s samtliga medlemsländer genom att förbättra tillgången till digitala varor och tjänster för konsumenter och företag i hela unionen, att skapa de rätta förutsättningarna för att digitala nät och tjänster ska blomstra samt att maximera den digitala ekonomins tillväxtpotential. Det finns ett stort fokus på telekom-industrin inom denna strategi. Strategin lever kvar i sådant som EU-kommissionen fick bakläxa på t.ex. förslag på e-Privacy förordning (se nedan).

Parallellt med de olika strategierna för data har EU-kommissionen lanserat en strategi för *Artificiell Intelligens för Europa* från 2018. Strategin bygger på tre punkter.

- Stärka EU:s tekniska och industriella kapacitet
- Förbereda för socioekonomiska förändringar och
- Säkerställa en lämplig etisk och rättslig ram.

Under 2021 började också EU-kommissionen att arbeta med ett policyprogram kallat ”En färdväg för det digitala decenniet”. Programmet ska säkerställa att EU uppnår sina syften och mål när det gäller den digitala omställningen av vårt samhälle och vår ekonomi i linje med EU:s värderingar. Färdvägen är ett sätt att få struktur på styrningen av den digitala utvecklingen. Tanken är att arbetet också ska leda fram till en deklaration om de digitala rättigheter och principer som ska ligga till grund för det digitala samhället och det digitala medborgarskapet och som ska vägleda beslutsfattare.

Europeiska rådet uppmanade under 2021 EU-kommissionen att bli mer konkreta i sina digitala ambitioner fram till 2030. EU-kommissionen har därför under 2021 presenterat en s k digital kompass som ska visa på konkreta milstolpar och hur de uppställda ambitionerna ska nås i syfte att följa upp så att medlemsländer inte halkar efter i utvecklingen. Den digitala kompassen hör ihop med ”En färdväg för det digitala decenniet”. I den digitala kompassen pekas fyra nyckelområden ut. Dessa är:

- Kompetens (skills) – medborgare ska ha en grundläggande digital kompetens och fler IT-specialister ska utbildas.
- Infrastruktur (infrastructure) – den digitala infrastrukturen ska vara hållbar med avseende på konnektivitet, mikroelektronik och möjligheten att behandla stora mängder data. Det innebär t.ex. att halvledare ska produceras inom EU och att inom EU ska det finnas egen molninfrastruktur.
- Digitalisering av näringsliv (business) – företag ska uppmuntras till att införa digitala tekniker och produkter. Industriell kapacitet som datautrymmen, öppna standarder och test- och experimentanläggningar ska stödjas.
- Digitalisering av offentlig sektor (government) – alla medborgare ska ha full möjlighet att delta digitalt i det demokratiska livet och ta del av det offentligas

tjänster digitalt på ett säkert sätt. Offentliga aktörer ska uppmanas att interagera, utbyta och använda information t.ex. inom e-hälsa.

EU-kommissionen har också aviserat att man vill satsa på stora multinationella teknologiska projekt för att nå målen i den digitala kompassen.

5.2 Förordning om dataförvaltningsakt/ Data governance act

EU-kommissionen vill göra det enklare för olika sektorer och länder att dela data med varandra. Målsättningen med förslaget är att öka tillgången på data som sedan ska kunna användas för att driva program inom AI, medicin, grön omställning, smart tillverkning etc. för att ge EU konkurrensfördelar inom en datadriven ekonomi. I november 2020 lade EU-kommissionen därför fram ett förslag till ny förordning om dataförvaltning (Data governance act).[37] Förslaget är en utkomst av *European Strategy for Data*. Förslaget hör hemma under samma paraply som GDPR, direktivet om integritet och elektronisk kommunikation (se vidare förslaget om e-Privacyförordning) samt öppna datadirektivet. Förslaget syftar till att underlätta *användning* och *vidareutnyttjande* av data inom EU (mellan myndigheter) dvs. fokus på aktivitet och inte på vilken sorts data det är frågan om. Målet är att till 2030 etablera en inre marknad för data. Förslaget riktar sig mot s k dataförmedlare och omfattar både personuppgifter och icke-personuppgifter och kopplar till ett gemensamt europeiskt dataområde. Förslaget vilar på fyra delar.

- För det första ska förslaget underlätta datadelning från offentlig sektor. Idéen är att tillgängliggöra data från offentlig sektor för vidareutnyttjande som andra har rättighet till dvs. företagshemligheter, immateriella rättigheter och personuppgifter. I denna del handlar det om att skydda delandet av denna typ av data.
- För det andra ska förslaget öppna upp för skapandet av neutrala dataförmedlingstjänster och nya affärsmodeller i syfte att skapa en säker miljö för datadelning mot ersättning. Det kan handla om plattformar för säker datadelning.
- För det tredje ska förslaget öppna upp för säker datadelning av personuppgifter mellan personer och företag via en neutral mellanhand. Mellanhanden ska vara en registrerad leverantörer som förmedlar data från personer till företag. Genom att anlita en sådan leverantör ska personer få full kontroll över vilken data som delas med vilket företag i enlighet med GDPR och därför känna sig trygga med att dela data.
- För det fjärde vill EU-kommissionen uppmuntra dataaltruism. Det innebär att personer och företag frivilligt gör data tillgängligt för det allmännas bästa. Tanken är att den skänkta data ska samlas in av organisationer med en viss uppförandekod. Dessa organisationer ska i sin tur finnas registrerade i ett särskilt register. Syfte med registreringen är att skapa tillit för datadelningen med organisationerna.

[37] Förslag till Europaparlamentets och rådets förordning om dataförvaltning (COM/2020/0304).

När detta skrivs ligger förslaget hos triologen. Om förslaget går igenom kan det finnas en förordning som är tillämpbar under 2023.

5.3 Rättsakten om digitala marknader/ Digital markets act

EU-kommissionen lade i december 2020 fram en rättsakt om digitala marknader som är en förlängning av plattformsförordningen.[38] Förslaget hör hemma under *A European Strategy for Data*. Förslaget utgår ifrån att det finns s k grindvakter – stora internetplattformar som sitter mellan slutanvändare och företagsanvändare – och syftar till att reglera deras verksamhet. Målet är att komma till rätta med ekonomiska obalanser och otillbörliga affärsmetoder från grindvaktens sida. I förslaget definieras vad som menas med en s k grindvakt, t.ex. en stark ekonomisk ställning, stor inverkan på den inre marknaden och verksam i flera medlemsländer. I förslaget regleras också förhållandet mellan grindvakten och företagsanvändare som är beroende av plattformen i syfte att underlätta konkurrens mellan företag. Grindvakten får t.ex. inte ge sina egna varor en mer gynnsam behandling på plattformen. Grindvakten behöver också ta ansvar för vad som säljs på plattformen, t.ex. illegala varor och sätta stopp för det. Grindvakten får heller inte göra vad den vill med uppgifter som kommer från slutanvändare. Om grindvakten inte följer reglerna riskerar denne böter eller vite.

Förslaget ligger när detta skrivs hos triologen. Om förslaget går igenom kan det finnas en förordning som är tillämpbar under 2023.

5.4 Rättsakten om en inre marknad för digitala tjänster/Digital services act

EU-kommissionen lade i december 2020 fram en rättsakt om digitala tjänster.[39] Förslaget hör hemma under *A European Strategy for Data* och bygger vidare på det äldre e-handelsdirektivet 2000/31/EG. Förslaget tar sikte på leverantörer, oavsett hemvist, som levererar en digital tjänst på EU:s inre marknad, t.ex. förmedling. Målet är bl.a. att göra plattformarnas inre verksamhet mer transparent. Stora plattformar kommer t.ex. att behöva ange hur de driver intresse mot en viss företeelse t.ex. genom att ge rekommendationer. Konsumenter ska också skyddas mot olämpligt innehåll från 3:e part. Exempelvis ska användare kunna flagga för olämpligt innehåll och grindvakter ska hjälpa till att spåra de som säljer illegala varor/tjänster via plattformen. Beroende på storlek på aktör och tjänst de erbjuder kommer olika regler att gälla för verksamheten. Målet är att ge ett bättre skydd åt konsumenter och deras rättigheter, öka transparensen samt stärka konkurrenskraften inom EU. Regelverket ska också uppmuntra aktörer till att ta frivilligt ansvar för olagligt innehåll.

[38] Förslag till Europaparlamentets och rådets förordning om öppna och rättvisande marknader inom den digitala sektorn (COM/2020/842).
[39] Förslag till Europaparlamentets och rådets förordning om en inre marknad för digitala tjänster (rättsakten om digitala tjänster) och om ändring av direktiv 200/31/EG (COM/2020/825).

Förslaget ligger när detta skrivs hos triologen. Om förslaget går igenom kan det finnas en förordning som är tillämpbar under 2023.

5.5 AI-förordningen/AI act

EU-kommissionen lanserade en vitbok för AI i februari 2020.[40] Vitboken innehåller EU-kommissionens beskrivningar av de åtgärder som EU-kommissionen anser behöver vidtas för att främja utvecklingen. Vitboken består av två delar. Del ett fokuserar på hur ett ekosystem av excellens för utveckling av AI inom EU. Del två handlar om vilka regelverk som behövs för att skapa förtroende för AI. Vilka risker finns det med AI som behöver hanteras och hur möter befintligt regelverk dessa risker?

Europaparlamentet har också antagit resolutioner angående AI. En resolution är ett icke-bindande beslut. I oktober 2020 antog Europaparlamentet två resolutioner. Den första resolutionen syftar till att ge kommissionen rekommendationer för en ram avseende etiska aspekter av AI.[41] Den andra resolutionen syftar till att ge rekommendationer till kommissionen för hur skadestånd och AI ska fungera tillsammans.[42] I oktober 2021 kom en tredje resolution som handlar om hur AI får användas i brottsbekämpande verksamheter.[43]

I april 2021 lade EU-kommissionen fram ett förslag till ny AI-förordning.[44] Förslaget hör hemma under strategin *Ett Europa rustat för den digitala* tidsåldern och innefattar branschöverskridande regler. Förslaget är uppdelat i olika områden. En del siktar på att förhindra oacceptabel användning av AI t.ex. för att manipulera eller diskriminera människor. En annan del riktar sig mot AI som anses vara högriskområden, t.ex. autonoma fordon och hur risker ska hanteras t.ex. genom certifiering och marknadsövervakning. För högrisk AI föreslås det också föreligga ett strikt ansvar hos tillverkaren för eventuella skador. Förordningen gör också skillnad på produkter som EU kan bestämma över själv och produkter som ligger utanför EU:s kompetens, t.ex. internationella konventioner. Exempelvis ligger maskiner under EU:s kompetensområde genom maskindirektivet medan typgodkända ”delar” av fordon ligger under UNECE genom typgodkännandekonventionen. De produkter EU kan bestämma över själv ingår i förslaget om en ny AI-förordning. På sikt tänker emellertid EU att alla produkter ska ingå i förordningen.

Förslaget ligger när detta skrivs hos triologen. Om förslaget går igenom kan det finnas en förordning som är tillämpbar under 2023.

---

[40] European Commission, White paper On Artificial Intelligence – A European approach to excellence and trust (COM/2020/65).
[41] Europaparlamentets resolution av den 20 oktober 2020 med rekommendationer till kommissionen om en ram för etiska aspekter av artificiell intelligens, robotteknik och tillhörande teknik.
[42] Europaparlamentets resolution av den 20 oktober 2020 med rekommendationer till kommissionen om en skadeståndsordning för artificiell intelligens.
[43] Europaparlamentets resolution av den 6 oktober 2021 om artificiell intelligens inom straffrätten och polisens och rättsväsendets användning av artificiell intelligens i brottsärenden
[44] Förslag till Europaparlamentets och rådets förordning om harmoniserade regler för artificiell intelligens (rättsakten om artificiell intelligens) och om ändring av vissa unionslagstiftningsakter.

5.6 E-Privacyförordningen/E-Privacy act

Under 2017 tog EU-kommissionen fram ett förslag till ny e-Privacyförordning som var tänkt att komplettera GDPR och riktar sig mot integritet och elektronisk kommunikation.[45] Förslaget är en vidareutveckling av det äldre e-Privacydirektivet 2002/58/EG. Förslaget möttes emellertid av omfattande kritik och har omarbetats ett antal gånger. När detta skrivs kommer enligt uppgift inte intresseavvägning, som rättslig grund, gå att använda utan endast samtycke kommer att utgöra den rättsliga grunden för behandling av personuppgifter. Det finns en oro för hur den slutliga förordningen kommer att utformas. Hur ska t.ex. samtycke inhämtas i relation till fordon? Ingår uppkopplade fordon eller undantas de? Det finns en risk för att med samtycke kommer den insamlade datamängden att bli mindre. Antagligen vill de som ligger längst ut, de s k randfallen, inte dela data. Men det är i randfallen som säkrare fordon kan utvecklas (förstå orsaken till olyckor). Hur ska vidare t.ex. en fordonstillverkare kunna arbeta med att utveckla mer hållbara fordon för att nå klimatmål om de ej har tillgång till data?

När detta skrivs ligger förslaget hos triologen. Om förslaget går igenom kan det finnas en förordning som är tillämpbar under 2023.

5.7 En förordning om europeisk digital identitet

EU-kommissionen arbetar med att ge EU-medborgare och företag en digital identitet som t.ex. ska kunna användas på nätet för identifiering och ge kontroll över data. I detta sammanhang talas också om ett digitalt medborgarskap. Medborgare ska också kunna ha en digital plånbok (digital wallet) för att lagra olika typer av data. Ett förslag till förordning om digital identitet lades fram i juni 2021 och bygger vidare på förordningen om elektronisk identifiering (EU) 910/2014.[46] I framtiden kan det bli så att det kommer att finnas en liknande lagstiftning rörande digital identitet för saker (IoT).

När detta skrivs ligger förslaget hos triologen. Om förslaget går igenom kan det finnas en förordning som är tillämpbar under 2023.

5.8 Data act

Enligt datastrategin ska EU-kommissionen utreda behovet av lagstiftningsåtgärder som rör förbindelser mellan dataekonomins olika aktörer. När detta skrivs har EU-kommissionen inte presenterat något förslag på lagstiftning ännu utan det förväntas ske under 2022. Bakgrunden till Data Act är att EU-kommissionen vill uppmuntra till så mycket datadelning som möjligt. Antagligen kommer Data Act att innehålla regler

[45] 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 (förordningen om integritet och elektronisk kommunikation) (COM/2017/10)
[46] Förslag till Europaparlamentets och rådets förordning om ändring av förordning (EU) 910/2014 vad gäller inrättandet av en ram för europeisk digital identitet (COM/2021/281)

för datadelning B2G och B2B och hur det ska ske på ett säkert sätt. Med tanke på att EU-kommissionen i andra regelverk är intresserade av data från fordonsindustrin kommer antagligen Data Act att få stor betydelse för fordonsindustrins datadelning.

5.9 Digital beskattning

Utvecklingen av digitala tjänster och nya affärsmodeller går mot att bli en allt större utmaning för skattesystemet. Mycket beroende på att vårt nuvarande skattesystem är baserat på fysisk varuproduktion och fysisk närvaro på en bestämd plats och inte på digitala tjänster, som kan utföras oberoende av en viss plats. Det framtida skattesystemet behöver således anpassas till den digitala ekonomin. En tanke är att beskattning i framtiden ska ske i försäljningslandet och inte i det land där produktionen av den digitala tjänsten sker. Än så länge diskuteras beskattning av digitala tjänster på en global nivå, men om en global lösning inte är möjlig kommer antagligen EU att ta fram egna regler för beskattning. EU-kommissionen har även framfört tankar kring en s k digital avgift i syfte att beskatta företag inom EU baserat på var den faktiska försäljningen sker och inte utifrån var ett visst företag har sitt fysiska säte. Något förslag om digital avgift har ännu inte lämnats av EU.

6 Avslutande kommentarer

Samhället genomgår en snabb digitalisering. Detta återspeglas också i de lagar och regler som ska reglera digitalisering och datahantering. Som genomgången ovan visar ska flera av de nuvarande lagarna göras om eller ersättas samtidigt som många helt nya regelverk är på gång. Detta är alltså ett område inom juridiken som står under en snabb förändring. Samtidigt synes det inte finnas någon egentlig samordning eller röd tråd för hur regelverken ska hänga ihop eller växa fram mycket beroende på att data som företeelse kan avse många olika saker och därmed ha olika regelgivare. Redan idag kan samma företeelse regleras i olika lagstiftningar. Exempelvis kan en och samma dataincident samtidigt träffa GDPR, säkerhetsskyddslagen och lagen om informationssäkerhet för samhällsviktiga och digitala tjänster, vilket i sin tur innebär att samma incident ska anmälas på olika sätt, med olika tidsfrister till olika myndigheter.

Regelverken kan även beskrivas som till viss del fragmenterat och svåröverskådligt samtidigt som det finns luckor i lagstiftningen. Historiskt har det varit mycket fokus på informationssäkerhet och personuppgifter. I framtiden kan det bli mer fokus på affären datadelning. Frågan är om t.ex. den kommande Data Act kan bidra till att fylla igen luckor på en generell nivå. Det finns många aspekter av datadelning som idag inte är reglerat genom något regelverk, t.ex. dela data som ej utgör personuppgifter, utan i stället kontrolleras genom avtal, vilket i sin tur innebär att avtalet mellan parterna blir avgörande. Avtalet blir således viktigt för de konkreta kraven på datadelningen då regelverk endast ger begränsad vägledning. Utmaningen för de enskilda avtalsparterna blir att de behöver ha god kännedom om vilka datamängder de har och innehållet i dessa för att i avtalet kunna reglera risker, hot och sårbarhet. Samtidigt lägger EU-kommissionen fram fler och fler förslag som syftar till att reglera datadelning för att skapa EU:s inre marknad för data. I denna del är det ett antal ledord som återkommer. Det handlar om att värna mänskliga rättigheter grundade i europeiska värderingar. Det

handlar också om att skapa en rättvis och fungerande konkurrens. Vidare handlar det om att tillgängliggöra data för att dela och vidareutnyttja genom öppna data för att skapa ett mervärde framför allt ifrån myndigheter. I detta ligger en målkonflikt mellan informationssäkerhet och öppna data som inte är enkel att lösa. Utmaning ligger i att varje enskilt dataset i sig behöver nödvändigtvis inte avslöja något känsligt. Men om många datasets läggs samman kan data på aggregerad nivå ändå avslöja för mycket.

HITS2024 fokuserar på citylogistik i bred bemärkelse. I projektet ryms t.ex. fordonsutveckling och digitalisering av logistikkedjan. Genomgången i den här rapporten visar att vissa sektorer är mer reglerade än andra. Mobilitet, fordon och transporter är ett område som har förhållandevis detaljerat regelverk och där mer lagstiftning är att förvänta, vilket i sin tur kommer att påverka utvecklingen av fordon och affärsmodeller. Det finns ett tydligt tryck från EU att få tillgång till mer och mer data från fordon. Samtidigt styrs teknikutvecklingen och marknadsutvecklingen av privata aktörer som behöver förstå vad som efterfrågas i god tid för att hinna med nödvändiga anpassningar och förändringar. Att förändra ett fordons elarkitektur tar tid. Att ta fram processer och dokumentation för att visa att en AI-produkt är säker att använda tar också tid.

Logistik är mindre reglerat vertikalt och styrs mer utifrån att vissa varugrupper såsom tobak har ett eget regelverk för datadelning. I framtiden skulle fler varugrupper t.ex. kläder kunna bli föremål för lagstiftning och då ur ett hållbarhetsperspektiv (återvinning av material). Här kan noteras att EU i nyare lagstiftning har valt modellen att data ska samlas i en punkt hos en central aktör (jfr ekrar och nav i ett hjul). Eftersom logistikområdet inte har ett lika tydligt vertikalt tryck från EU på datatillgång kommer det horisontella regelverket att få större betydelse och därmed blir avtalslösningar fortsatt viktiga. Den kommande Data Act kan t.ex. få stor betydelse eftersom den kommer att reglera datadelning B2B. Även hanteringen av personuppgifter kommer att vara fortsatt viktig.

Slutligen kan konstateras att ur ett regelperspektiv går data från fordon, mobilitet och transporter i ett ”stuprör” och data om varor och varuflöden i ett annat ”stuprör”. Frågan är om det är hållbart i längden för att uppnå målen i Agenda 2030.

7 Referenser

7.1 Regelverk

EU-lagstiftning:

Europaparlamentet och rådets direktiv 1999/94/EG av den 13 december 1999 om tillgång till konsumentinformation om bränsleekonomi och koldioxidutsläpp vid marknadsföring av nya personbilar.

Europaparlamentet och rådets direktiv 2007/2/EG av den 14 mars 2007 om upprättande av en infrastruktur för rumslig information i europeiska gemenskapen (Inspire).

Europaparlamentet och rådets direktiv 2009/73/EG av den 13 juli 2009 om gemensamma regler för den inre marknaden för naturgas och om upphävande av direktiv 2003/55/EG.

Europaparlamentet och rådets direktiv (EU) 2015/2366 om betaltjänster på den inre marknaden.

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

Europaparlamentet och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation.

Europaparlamentet och rådets direktiv (EU) 2019/770 av den 20 maj 2019 om vissa aspekter på avtal om tillhandahållande av digitalt innehåll och digitala tjänster.

Europaparlamentet och rådets direktiv (EU) 2019/ 790 av den 17 april 2019 om upphovsrätt och närstående rättigheter på den digitala inre marknaden och om ändring av direktiven 96/ 9/ EG och 2001/ 29/ EG.

Europaparlamentet och rådets direktiv (EU) 2019/944 av den 5 juni 2019 om gemensamma regler för den inre marknaden för el och om ändring av direktiv 2012/27/EU.

Europaparlamentet och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn.

Europaparlamentets och rådets förordning (EG) nr 178/2002 av den 28 januari 2002 om allmänna principer och krav för livsmedelslagstiftning, om inrättande av Europeiska myndigheten för livsmedelssäkerhet och om förfarande i frågor som gäller livsmedelssäkerhet.

Europaparlamentet och rådets förordning (EG) 1907/2006 av den 18 december 2006 om registreringutvärdering, godkännande och begränsning av kemikalier.

Europaparlamentet och rådets förordning (EG) 715/2007 av den 20 juni 2007 om typgodkännande för lätta personbilar och lätta nyttofordon (Euro 5 och 6) och om tillgång till information om reparation och underhåll av fordon.

Europaparlamentet och rådets förordning (EG) 595/2009 av den 18 juni 2009 om typgodkännande av motorfordon och motorer vad gäller utsläpp från tunga fordon (Euro 6) och om tillgång till information om reparation och underhåll av fordon förordning.

Europaparlamentet och rådets förordning (EU) nr 2014/15 av den 4 februari 2014 om färdskrivare vid vägtransporter, om upphävande av rådets förordning (EG) nr 3821/85 om färdskrivare vid vägtransporter och om ändring av Europaparlamentets och rådets förordning (EG) nr 561/200 om harmonisering av viss sociallagstiftning på vägtransportområdet.

Europaparlamentet och rådets förordning (EU) 536/2014 av den 16 april 2014 om kliniska prövningar av humanläkemedel och om upphävande av direktiv 2001/20/EG

Europaparlamentet 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 upphävandet av direktiv 95/46/EG.

Europaparlamentets och rådets förordning (EU) 2017/745 av den 5 april 2017 om medicintekniska produkter.

Europaparlamentet och rådets förordning (EU) 2018/1807 av den 14 november 2018 om ram för det fria flödet av andra data än personuppgifter i Europeiska unionen.

Europaparlamentet och rådets förordning (EU) 2019/631 av den 17 april 2019 om fastställande av normer för koldioxidutsläpp för nya personbilar och för nya lätta nyttofordon och om upphävande av förordningarna (EG) nr 443/2009 och (EU) nr 510/2011.

Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013.

Europaparlamentet och rådets förordning (EU) 2019/1150 av den 20 juni 2019 om främjande av rättvisa villkor och transparens för företagsanvändare av online baserade förmedlingstjänster.

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 (förordningen om integritet och elektronisk kommunikation) (COM/2017/10).

Förslag till Europaparlamentets och rådets förordning om dataförvaltning (COM/2020/0304).

Förslag till Europaparlamentets och rådets förordning om en inre marknad för digitala tjänster (rättsakten om digitala tjänster) och om ändring av direktiv 200/31/EG (COM/2020/825).

Förslag till Europaparlamentets och rådets förordning om öppna och rättvisande marknader inom den digitala sektorn (COM/2020/842).

Förslag till Europaparlamentets och rådets förordning om ändring av förordning (EU) 910/2014 vad gäller inrättandet av en ram för europeisk digital identitet (COM/2021/281).

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

Kommissionens delegerade förordning (EU) 2015/962 av den 18 december 2014 om komplettering av Europaparlamentet och rådets direktiv 2010/40/EU vad gäller tillhandahållande av EU-omfattande realtidstrafikinformationstjänster.

Kommissionens delegerade förordning (EU) 2017/1926 av den 31 maj 2017 om komplettering av Europaparlamentet och rådets direktiv 2010/40/EU vad gäller tillhandahållande av EU-omfattande multimodala reseinformationstjänster.

Kommissionens förordning (EU) 2015/703 av den 30 april 2015 om fastställandet av nätföreskrifter med regler för driftskompabilitet och informationsutbyte.

Kommissionens förordning (EU) 2017/1151 av den 1 juni 2017 om komplettering av Europaparlamentet och rådets förordning (EG) nr 715/2007 om typgodkännande av motorfordon med avseende på utsläpp från lätta personbilar och lätta nyttofordon (Euro 5 och Euro 6) och om tillgång till information om reparation och underhåll.

Kommissionens förordning (EU) 2017/1485 av den 2 augusti 2017 om fastställande av riktlinjer för driften av elöverföringssystem.

Kommissionens rekommendation (EU) 2018/790 av den 25 april 2018 om tillgång till och bevarande av vetenskaplig information.

Nationell lagstiftning:

Avgasreningslagen (2011:318)

Kamerabevakningslagen (2018:1200)

Konkurrenslagen (2008:579)

Lagen (2003:389) om elektronisk kommunikation

Lagen (2007:528) om värdepappersmarknad

Lagen (2010:566) om vidareutnyttjande av handlingar från den offentliga förvaltningen

Lagen (2010:751) om betaltjänster

Lagen (2010:1767) om geografisk miljöinformation

Lagen (2016:319) om skydd för geografisk information

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

Lagen (2018:558) om företagshemligheter

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

Lagen (2018:2088) om tobak och liknande produkter

Lagen (2021:553) med kompletterande bestämmelser till cybersäkerhetsakten

Offentlighets- och sekretesslagen (2009:400)

Skyddslagen (2010:305)

Säkerhetsskyddslagen (2018:585)

Tryckfrihetsförordningen (1949:105)

Upphovsrättslagen (190:729)

7.2 Övrigt

EU-commission (2017) Study on emerging issues of data ownership, interoperability, (re-) usability and access to data, and liability.

European Commission, (2020) Recovery Plan for Europe – Next Generation EU.

European Commission, White paper On Artificial Intelligence – A European approach to excellence and trust (COM/2020/65).

Communication from the Commission to the European Parliament, the Council and Social Committee and the Committee of the Regions – *Towards a common European Data Space*, (COM/2018/232).

SOU 2020:51 *En ny lag om konsumentskydd vid köp och vissa andra avtal*.

Sveriges regering (2017) *En nationell strategi för samhällets informations- och cybersäkerhet* (skr. 2016/17:213).

Through our international collaboration programmes with academia, industry, and the public sector, we ensure the competitiveness of the Swedish business community on an international level and contribute to a sustainable society. Our 2,800 employees support and promote all manner of innovative processes, and our roughly 100 testbeds and demonstration facilities are instrumental in developing the future-proofing of products, technologies, and services. RISE Research Institutes of Sweden is fully owned by the Swedish state.

I internationell samverkan med akademi, näringsliv och offentlig sektor bidrar vi till ett konkurrenskraftigt näringsliv och ett hållbart samhälle. RISE 2 800 medarbetare driver och stöder alla typer av innovationsprocesser. Vi erbjuder ett 100-tal test- och demonstrationsmiljöer för framtidssäkra produkter, tekniker och tjänster. RISE Research Institutes of Sweden ägs av svenska staten.

RISE Research Institutes of Sweden AB
Box 857, 501 15 BORÅS
Telefon: 010-516 50 00
E-post: info@ri.se, Internet: www.ri.se

Mobilitet och system
RISE Rapport 2022:57
ISBN: 978-91-89561-97-7