DIGITALA SYSTEM

MOBILITET OCH SYSTEM

Fordonsdata till allmänhetens nytta - geofencing och affärsmodeller

Kristina Andersson, Håkan Burden, Mahdere DW Amanuel, Susanne Stenberg och Niklas Thidevall

RISE Rapport 2021:12

Fordonsdata till allmänhetens nytta - geofencing och affärsmodeller

Kristina Andersson, Håkan Burden, Mahdere DW Amanuel, Susanne Stenberg och Niklas Thidevall

Nyckelord: policylabb, avtal, fordonsdata, datadelning, integritet, tvång, geostaket

Key words: Policy lab, contract, vehicle data, data sharing, integrity, coercion, geofencing

RISE Research Institutes of Sweden AB

RISE Rapport 2021:12
ISBN:978-91-89167-95-7
Göteborg 2021

Abstract

Vehicle data for the benefit of the public – geofencing and business models

Vehicle data could be an asset to authorities in various ways. Despite the promises, the business opportunities are scarce. One of the few examples is public procurement of data to assess the need for calling out the snow ploughs and follow-up work about the quality performed. Even though there is an interest from both private and public actors to conduct business with vehicle data, the market is struggling to pick up speed.

The challenge in how to commercialize vehicle data with the public as buyer has therefor been investigated through Drive Sweden Policy Lab together with the CeViss project (Cloud enhanced cooperative traffic safety using vehicle sensor data). Two examples of use cases in CeViss project were to warn other drivers about elks on the road and inform the emergency services what to expect at an accident site.

The prerequisites for successful commercialization can be summarized under three headings – business, technology, and law. We see that the business lies within being able to offer aggregated and cross-fertilized data and thereby create a greater value, than the included amounts of data possess individually. Commercial actors point out that this role, of refining data, is the most interesting one, as it provides possibilities to develop services. Such a service presupposes access to a secure connection and transmission. However, it is resource intensive to refine data and control the correct transfer, as well as to review, adapt and produce legal agreements that enables such cross-fertilization of data and transfer of the correct data. Here, the individual's integrity versus society's need for data plays a major role. It is also not clear to what extent the public sector needs vehicle data and how it will obtain such data.

The challenge for the industry lies in daring to trust that there is a sustainable deal with the public sector in the long run, i.e. that there is a willingness to pay even when the data is considered critical to society. To promote commercialization, it is good to start with a specifically selected area to develop processes, agreements, technology solutions, business models and so on.

Geofencing could be an opportunity to create the boundaries needed for a first deal, while at the same time creating clarity about where and when data is collected from vehicles. Such a delimitation could also serve as a regulatory sandbox, to evaluate the possibility of agreements that are sustainable over time (i.e. where it is reasonable to use the data in new ways or for new purposes within certain limits).

The report concludes with a compilation of geofencing and data sharing from a legal perspective and a description of the Drive Sweden Policy Lab.

Innehåll

Förord

Den svenska regeringen har 17 strategiska innovationsprogram (så kallade SIPar). Drive Sweden är en av dessa. Drive Sweden består av medlemmar från akademi, industri och samhälle. Tillsammans arbetar medlemmarna med de utmaningar som är kopplade till nästa generations mobilitetssystem för människor och varor. SIParna finansieras av Sveriges innovationsmyndighet Vinnova, Formas, ett forskningsråd för hållbar utveckling och Energimyndigheten. Lindholmen Science Park AB är värd för Drive Sweden.

Följande rapport utgör en delrapport i projektet Drive Sweden Policy Lab. Projektet är dels finansierat av Vinnova genom Drive Sweden, dels av Trafikverket. Totalt har tre delrapporter publicerats. Projektet beskrivs mer utförligt i Appendix A nedan.

Projektet har pågått under tiden oktober 2019 till och med december 2020. RISE har varit projektledare. I projektet har följande parter ingått utöver RISE:

- Applied Autonomy AS
- Boliden AB
- Combitech AB
- Easy Mile GmbH
- Einride AB
- Göteborgs kommun
- Keolis Sverige AB
- Sveriges Åkeriföretag Västra Götaland
- Trafikverket
- Veoneer Sweden AB

Stort tack till Veoneer Sweden AB som bidragit med fallstudien till denna delrapport. Utan vårt systerprojekt hade det inte varit möjligt att genomföra detta delprojekt.

Stort tack till alla i övrigt som varit med och tyckt till och bidragit med sina åsikter och kunskap.

Fotot på framsidan är taget av Lisa Carlgren.

Vi vill särskilt påpeka att eventuella ståndpunkter och ställningstagande i denna rapport är författarnas egna. Andra parter eller representanter kan ha en annan analys och kommit till andra slutsatser.

Göteborg i januari 2021

Kristina Andersson, Håkan Burden, Mahdere DW Amanuel, Susanne Stenberg och Niklas Thidevall.

Sammanfattning

Fordonsdata kan i framtiden vara till stor nytta för myndigheter på olika sätt. Än så länge samlar myndigheter in fordonsdata i begränsad omfattning. Det kan t.ex. handla om att genom offentlig upphandling pröva nya sätt för att kontrollera kvaliteten på utförd snöröjning. Trots att det finns ett intresse från både privata och offentliga aktörer att genomföra affärer kring fordonsdata är det ändå svårt för marknaden att ta fart.

Frågan om hur fordonsdata kan kommersialiseras med offentliga aktörer som köpare har därför undersökts inom Drive Sweden Policy Lab i samarbete med CeViss-projektet (Cloud enhanced cooperative traffic safety using vehicle sensor data). CeViss-projektet har undersökt smarta kameror och hur de bl.a. kan användas för att varna andra förare för vilda djur vid vägen eller informera SOS Alarm om hur det ser ut vid en olycksplats.

Förutsättningarna för lyckad kommersialisering kan sammanfattas under tre rubriker - affären, tekniken och juridiken. Vi ser att affären ligger i förmåga att erbjuda aggregerade data där olika datamängder korsbefruktas och därmed skapar ett större värde än de ingående datamängderna besitter var för sig. Kommersiella aktörer pekar på att rollen att aggregera data, eller förädla den, är mest intressant, eftersom det innebär en möjlighet att utveckla tjänster. En sådan tjänst förutsätter tillgång till en säker uppkoppling och överföring. Det är också resurskrävande att förädla data och styra rätt överföring, liksom att se över, anpassa och ta fram avtal som gör korsbefruktning av data och överföring av rätt data juridiskt möjlig. Här spelar individens integritet kontra samhällets behov av data en stor roll. Det är inte heller klart vilket behov aktörer inom olika samhällssektorer har av fordonsdata, samt hur dessa kommer att få tag i fordonsdata.

Utmaningen för industrin ligger i att våga lita på att det finns en hållbar affär med myndigheten i längden, dvs. att det finns en tillräckligt stor betalningsvilja från samhällets sida även när data anses samhällskritisk viktigt. För att främja kommersialisering är det bra att börja med ett specifikt utvalt område för att utarbeta processer, avtal, tekniklösningar, affärs-modeller och så vidare.

Geofencing hade kunnat vara en möjlighet att skapa de avgränsningar som behövs för en första affär, samtidigt som det skulle skapa tydlighet om var och när data samlas in från fordon. En sådan avgränsning hade också kunnat tjäna som en regulatorisk sandlåda för att utvärdera möjligheten till avtal som är hållbara över tid, det vill säga där det är rimligt att inom vissa gränser använda data på nya sätt eller för nya syften.

Rapporten avslutas med en sammanställning av geofencing och datadelning ur ett juridiskt perspektiv samt en beskrivning av Drive Sweden Policy Lab.

1 Nya affärer på redan insamlad data

Data är det nya guldet. Mycket har sagts och skrivits om hur den affären realiseras mellan två kommersiella parter eller hur ett företag kan tjäna pengar på data som användarna av deras tjänst genererar. I den här rapporten ska vi undersöka förutsättningarna för att etablera nya affärer mellan privata och offentliga aktörer baserade på delning av data från fordonssensorer. Vi ser att både privata och offentliga aktörer har mycket att vinna på att samarbeta. Privata aktörer kan utveckla nya tjänster och affärer medan det offentliga kan erbjuda bättre service åt medborgarna, effektivare användning av skattemedel, en mer hållbar miljö etc.

Från utvecklingen av samhällets behov av mobildatatrafik finns många lärdomar att hämta. Erfarenheterna är intressanta eftersom de visar på att det offentliga är intresserade av att köpa data, men också att affären utvecklas över tiden, vilket i sin tur påverkar lönsamheten för de kommersiella aktörerna. Förenklat utvecklade det privata näringslivet en kommersiell tjänst för att hålla reda på vilka teleoperatörer som var med i ett samtal för att hantera inkomster och kostnader i samband med telefonsamtal som gick mellan två operatörer. Den tjänsten visade sig vara användbar i brottsutredningar för att kunna visa på vilka mobiltelefoner som varit i kontakt med varandra inom en viss tidsperiod s.k. masttömning/basstationstömning. Nästa steg blev att införa en lagringsskyldighet för vissa trafikuppgifter enligt lagen (2003:389) om elektronisk kommunikation för att möjliggöra masttömning i större skala. Den som lagrade uppgifterna hade vidare rätt till ersättning när uppgifterna lämnades ut. Ersättningen skulle betalas av den myndighet som begärt ut uppgifterna. När bestämmelsen först infördes beräknades ersättningen i princip utifrån varje enskilt fall (faktisk kostnad). De större operatörerna hade egna avtal om ersättning med de brottsbekämpande myndigheterna. Över tid växte det allmännas behov av mobiltrafikdata. Detta medförde i sin tur vissa problem t.ex. omfattande administrationen hos myndigheterna samt att ersättningsnivåerna till teleoperatörerna varierade, vilket upplevdes som orättvist. Post- och telestyrelsen beslöt därför att införa en föreskrift som reglerade ersättningsnivån utifrån en reglerad taxa (schablon).[1] Detta ledde till sänkta kostnaderna för det offentliga i form av t.ex. minskad administration, men minskade också operatörernas förhandlingsutrymme (en del hade tidigare förhandlat sig till mer lönsamma avtal, andra hade mindre lönsamma avtal).[2]

Kan vi lära oss något av historien om masttömning för att stimulera innovation inom delningen av fordonsdata så det både gynnar offentliga aktörer (och därmed samhället i stort) samt kommersiella aktörer? Om affären finnas blir det intressant för fordons-industrin att utveckla tjänster kring datadelning med myndigheter och andra offentliga aktörer. Hittills har myndigheter lämnat ersättning för fordonsdata utifrån antingen avtal, t.ex. ett köp baserat på offentlig upphandling (kontroll av utförd snöröjning), eller utifrån tvång, t.ex. som beslag. Ersättning har i beslagsfallet hittills utgått från faktisk

[1] Ersättning bestäms numera enligt post- och telestyrelsens föreskrifter (2013:5) om ersättning vid utlämnande av lagrade uppgifter för brottsbekämpande ändamål.
[2] Post- och telestyrelsen, *Konsekvensutredning avseende föreskrifter om ersättning vid utlämnande av lagrade uppgifter för brottsbekämpande ändamål*, 2013-06-18, diarienr 12–4585.

kostnad för att ta fram begärd information till myndigheten (t.ex. ta fram data från en s.k. svart låda i ett fordon).

Trots de förväntade samhälleliga vinsterna går kommersialiseringen av fordonsdata relativt långsamt. Särskilt med tanke på att flera fordonstillverkare har uttalat att de är intresserade av att utöka befintliga affärsmodeller, som i dagsläget huvudsakligen går ut på att sälja hårdvara (fordon), till att allt mer inkludera digitala tjänster i samband med att mängden mjukvara ökar i fordon.

Men varför går kommersialiseringen av fordonsdata så långsamt? En delförklaring kan finnas i olika sektorers sammanhang och förutsättningar. Offentliga aktörers verksamhet bygger på vilket uppdrag eller mandat de har t.ex. myndighetens instruktion. Verksamheten är många gånger styrd av regler, och aktörerna kan ha typiska roller i förhållande till verksamhetens (eventuella) behov av fordonsdata som någon annan samlat in. Den klassiska rollen är den som beställare och inköpare, vilket för en offentlig organisation som huvudregel sker genom upphandling. Den diametralt motsatta rollen kan uppstå om behovet av fordonsdata är för myndighetsutövning, och ger då aktören utrymme att utöva makt för att få tillgång till data. Ett exempel på den förra är kommuners ansvar för underhåll av vägar eller snöröjning. Ett exempel på det senare är polisens ansvar för brottsbekämpning.

Den här rapporten ska ses i ett större sammanhang och kopplar till ett systerprojekt kallat CeViss (Cloud enhanced Vehicle – Intelligent Sensor Sharing).[3] CeViss var ett projekt som pågick under 2020 och delfinansierades av DriveSweden/Vinnova. Projektparterna var Carmenta, CEVT, Ericsson, Volvo Cars och Veoneer. I projektet undersöktes hur data från sensorer på uppkopplade fordon kunde användas för att göra trafikmiljön säkrare. Idéen bygger på att uppkopplade fordon kan kommunicera via fordonstillverkares moln och på så sätt varna för faror längs vägen. Föraren ska därigenom kunna få en förvarning och vidta lämpliga åtgärder i tid för att förhindra trafikolycka. I projektet demonstrerades ett antal scenarios på testbana för att visa hur datadelning mellan fordon via moln skulle kunna gå till t.ex. älgvarning, varning för stillastående fordon, varning för gående på väg, samla in data från en trafikolycka och leta efter en registreringsskylt.

Parallellt med CeViss genomförde vi projektet Drive Sweden Policy Lab (DSPL). Ett av syftena med DSPL var att stötta teknikutvecklingsprojekt där det dök upp utmaningar relaterade till regelverk och affärsmodell. DSPL leddes av RISE i samarbete med en rad aktörer. Vårt arbete utgick från ett scenario där fordonskameror används till att samla in data om infrastrukturen eller andra medtrafikanter, t.ex. att leta efter hål i vägbanan eller andra fordons registreringsskyltar på uppdrag från en myndighet. När fordonsdata har samlats in delas den sedan med myndigheten.

Vår uppgift blev att undersöka de affärsmässiga förutsättningarna för att bättre kunna avgöra om det var värt att driva innovationen på området vidare. Under arbetets gång identifierades sex aspekter som grupperades under teknik (cybersäkerhet och kapacitet), affär (hållbara avtal och kommersialisering) och juridik (individens integritet och tvång, dvs. regleringar om att tvingas dela data). En sammanfattande utmaning är hur avtalen kan vara tillräckligt dynamiska för att möta innovationens behov av variabilitet utan att

[3] https://www.drivesweden.net/en/projects-5/ceviss-cloud-enhanced-cooperative-traffic-safety-using-vehicle-sensor-data

utmana de demokratiska principerna. Ett sätt att gå vidare är att se geofencing utifrån ett avtalsperspektiv. Vi får då naturliga avgränsningar i tid och rum kring data-insamlingen samtidigt som det ger tydlighet om var avtalet gäller.

I avsnitt 2 beskrivs hur arbetet genomfördes i form av ett policylabb och avsnitt 3 detaljerar våra insikter och relaterar dem till den gemensamma marknaden inom EU. Avsnitt 4 lyfter blicken och sätter resultaten i ett större perspektiv genom att knyta an till geofencing som avtal. I slutet av rapporten kommer tre appendix med mer bakgrunds-information för den som vill fördjupa sig i geofencing, datadelning och projektet Drive Sweden Policy Lab.

2 Policylabb – hur vi arbetat

Vårt tillvägagångssätt har skett genom tre huvudsakliga aktiviteter: intervjuer, läsning av rapporter och omvärldsbevakning. Intervjuerna har varit med två privata aktörer, fem representanter från två myndigheter och en branschorganisationsrepresentant. Flera av representanterna har blivit intervjuade två gånger och vi har även haft en löpande dialog med två av aktörerna.

De insamlade resultaten har sen grupperats så att data med samma innebörd har blivit en kategori. Kategorierna har sedan satts i relation till varandra vilket lett till nya insikter som fångats i nya kategorier. Slutligen har kategorierna syntetiserats till större teman vilka presenteras som slutsatser ifrån studien. Dessa teman har kopplingar till varandra och i vissa fall en viss överlapp. De ska därför inte ses ortogonala utan som samverkande.

Frågeställningarna som handlar om affärsmodeller för fordonsdata är komplexa. För att öka förståelsen för problematiken har vi även tagit in andra perspektiv utöver ekonomi, såsom juridik och datavetenskap. Vi har däremot begränsat oss till att undersöka vilka förutsättningarna är för privata aktörer att etablera nya affärer med det offentliga. Den omvända frågan om hur det offentliga kan få tag i för dem eftertraktad data har vi inte tittat på. Frågorna är synbart snarlika men skulle kunna få väldigt olika svar.

Arbetet har bedrivits inom Drive Sweden Policy Lab, ett projekt finansierat av Vinnova genom det strategiska innovationsprogrammet Drive Sweden. Se Appendix C för mer information om projektet.

3 Affären, tekniken och juridiken

Det här avsnittet redogör för de affärsmässiga, tekniska och juridiska förutsättningarna för att skapa hållbara affärer mellan datadelare och offentliga aktörer. Avsnittet avslutas med en diskussion kring de tre aspekterna och hur de samverkar med varandra.

3.1 Affären

I relation till affären har vi två teman som står ut som intressanta: hur man etablerar en affär och hur man får den att leva vidare.

Kommersialisering: För att få en framgångsrik kommersialisering av fordonsdata är det högst relevant att man initialt fokuserar på att försöka sälja och köpa fordonsdata på ett

specifikt utvalt tillämpningsområde, såsom identifiering av potthål på en viss vägsträcka. Genom att välja ett mindre och därmed mer konkret område kan både samhället och industrin fokusera på att ta fram interna och externa arbetsprocesser, avtal, tekniklösningar, affärsmodeller o.s.v. för det fortsatta arbetet. På så sätt kan man säkerställa att den tekniska innovationen utvecklas tillsammans med den offentliga aktörens vilja att ingå en affärsöverenskommelse. Ett sätt att organisera kommersialiseringen på är genom innovationsupphandling.[4]

Hållbara affärsmodeller: För att det ska vara attraktivt för kommersiella aktörer att sälja fordonsdata behöver man kunna använda data man redan samlat in för nya ändamål eller i nya kontexter. Man behöver också få köparna (i det här fallet samhället) att vara beredda att använda sig av en förhandlad ersättning för data. Ett sätt att nå en förhandlad ersättning är genom upphandling där den privata aktören ger sitt pris för att leverera den sökta data. Även om den samhälleliga nyttan är viktig för industrin så är den viktigaste drivkraften bakom datadelningen möjligheten att etablera nya och lönsamma affärer. Därför behöver industrin veta att det finns en betalningsvilja hos myndigheter och att det går att ha en löpande affär, enstaka försäljningar med hög lönsamhet är sämre än en kontinuerlig affär med liten lönsamhet över tid. Annars kommer andra marknader vara mer lönsamma, såsom att sälja samma data i en annan tjänst direkt till privata slutkonsumenter eller på en annan marknad där det offentliga vill eller kan erbjuda en bättre ersättning.

En fråga som snabbt blev tydlig utifrån intervjuerna var behovet av att kunna korsbefrukta olika mängder av fordonsdata. En sådan möjlighet kan avhjälpa om en specifik mängd data är ofullständig eller ger en partisk bild och möjliggöra en balanserad och fullständig bild av en viss situation eller fenomen. Att jämföra och komplettera olika datamängder med varandra ger helt enkelt ofta en mer kvalitativ bild. Samtidigt är det problematiskt om detta inte tillåts i de avtal som tecknats för varje enskilt datainsamlande. Att ändra på avtalen eller skapa nya för att möjliggöra korsbefruktning av data är en tidskrävande process, vilket gör att det uppstår ledtider i affärerna.

3.2 Tekniken

Under aspekten tekniken har vi identifierat förmåga, förädling och cybersäkerhet som viktiga teman att ta hänsyn till.

Förädling. Fordonsdata kan delas in i tre nivåer:

1. Rådata: data från sensorer och liknande som kan skickas obehandlat till en molntjänst. Positionsdata är ett exempel på rådata.
2. Aggregerade data: data från flera källor som skickas som en enhet. Positionsdata tillsammans med tidsstämpel och hjulens rotationshastighet utgör aggregerade fordonsdata.
3. Tjänst: utifrån aggregerade data kan man skapa tjänster. Halkvarning är ett exempel på en tjänst som beror på åtkomsten av aggregerade data.

Aggregerade data och tjänst är exempel på förädling där rådata fått ett nytt värde av att kombineras med något annat. Detta andra kan vara andra datakällor eller någon form av

[4] https://www.upphandlingsmyndigheten.se/innovation-i-upphandling/

behandling av data. Exempel på behandling kan vara att filtrera bort anomalier i datamängden eller att anonymisera personer genom att sudda ut deras ansikten.

Det är framförallt aggregerad fordonsdata som de kommersiella aktörerna ser ett värde i att erbjuda. Vidare kan fordonsdata vara intressant som massdata (t.ex. planering av snöröjning utifrån stora mängder fordonsdata) eller individdata (har någon t.ex. sett en vit Audi med körförbud?).

Ett erbjudande kring aggregerade data kräver egentligen tre olika roller för att realiseras. Den första rollen är insamlaren som har tillgång till fordonsdata. Det kan vara en kameratillverkare som har en bildström att dela eller en fordonstillverkare som kan dela hastighet. Den andra rollen är förädlaren. Idag är det antingen fordonstillverkarna själva som förädlar data till aggregerade data eller tjänster, eller så görs det av små eller medelstora företag som ser nya marknadsmöjligheter. För förädlaren är det viktigt att kunna korsbefrukta olika fordonsdata för att få fram relevant information. Den sista rollen är konsumenten av fordonsdata. Det kan vara samhället i form av rapporter om eftersatt väglag eller slutkonsumenter som vill ha tjänsterna när de kör eller planerar sin resa. Det är framförallt förädlaren som har möjlighet att utveckla nya tjänster. Men då krävs också tillgång till en uppkoppling från fordonet till en molntjänst. På personbilssidan är det många gånger bara fordonstillverkaren som har tillgång till fordonets uppkoppling.

Förmåga. Att förädla data är en fråga om förmåga, både i form av att ha tillräckligt med processorkraft och rätt algoritmer som kompetensen till att veta hur man ska förhålla sig till utkomsten av algoritmerna eller anpassa dem till ens egna behov. Förädling kräver alltså resurser, både i form av teknik och kompetens. Att analysera och paketera stora datamängder kräver stor beräkningskapacitet vilket i sin tur kräver mycket energi. Ska sedan resultatet av beräkningarna vara värda något behövs relevant kompetens i form av bl.a. AI och nätverksteknik. Något som i dagsläget är en bristvara. Utifrån intervjuerna kan vi se att inte alla offentliga aktörer besitter förmågan att förädla data för sina egna syften och att de i vissa fall inte vill eller kan vara tydliga i vilka förädlingsbehov de har. Det beror både på att det ibland är svårt att beskriva det man inte vet, men kan också komma sig av att det är känsligt att berätta vad man letar efter, t.ex. vid brottsutredningar eller i arbetet med att förebygga terrorism.

Cybersäkerhet. En risk som uppstår när man delar stora mängder fordonsdata är risken att någon obehörig kan få en direktaccess in i fordonet. Risken för terrorism, kapning av fordon eller konton etc. måste vägas mot fördelarna med att ha tillgång till data. Samtidigt kommer teknikutvecklarna själva vilja ha tillgång till data i realtid i många fall. Att arbeta proaktivt med säker datadelning, oavsett om mottagaren är en egen enhet inom organisationen eller en myndighet, kommer att vara viktigt.

3.3 Juridiken

Under juridik återfinns myndigheternas dubbla roll som maktutövare och leverantörer av samhälleliga tjänster.

Tvång: För att motivera industrin att utveckla tjänster för att sälja fordonsdata till samhället behöver man undvika att tvinga fram datadelning genom regler som omintetgör en affär. Det är så affärsmodellen har utvecklats för teleoperatörerna i relation till

offentliga myndigheter, t.ex. vid brottsutredningar. En modell byggd på tvång för att dela fordonsdata skulle göra det mindre attraktivt att utveckla tjänster i Sverige. Det i sin tur skulle bidra till att innovations-klimatet i Sverige påverkas negativt.

Individens integritet. Fordonsdata omfattar inte endast data från den insamlande enheten, dvs. själva kameran i ett visst fordon (och där fordonstillverkare får tillgång till överförd data), och om de personer som använder fordonet eller på något sätt har en skyldighet kopplad till fordonet, utan också data om annat (och därmed ibland om andra personer) än den som använder fordonet. Detta väcker frågor om integritet kontra samhällskritisk verksamhet och affärs- eller systemmodeller på olika nivåer. Det handlar om att balansera mellan individers rätt till skydd för sin integritet och att erbjuda överföring av för offentliga aktörer värdefull fordonsdata utifrån det legala ramverket, dvs. till gagn för andra individer eller ett särskilt viktigt samhällsintresse.

Nödsituationer är situationer där kravet på snabb tillgång till information för att bistå en nödställd kan överväga det integritetsintrång som det typiskt sett innebär att sända viss fordonsdata om medtrafikanter utan deras uttryckliga tillåtelse.

En utmaning är på vilket sätt avgränsar man den data som ska överföras till någon annan? Det kan finnas kameror både utåtriktat runt fordonet och inåtriktat inuti fordonet, hur mycket ska sparas och delas? Det är en fråga om kapacitet, men också om integriteten för de människor som kamerornas insamlade data berör. Dessa är fordonsägare och passagerare samt medtrafikanter.

Ur ett samhällsperspektiv är både massdata (data från många fordon) och individdata (data från ett fordon) intressanta. Samtidigt finns det en känslighet kring hur samhället visar sin vilja att betala för viss information. Det är skillnad på att vara öppen med att Trafikverket samlar in data för att optimera snöröjningen jämfört med att polisen spanar efter en viss bil. Men även inom en myndighet kan det finnas nyansskillnader i graden av öppenhet. Det är mindre känsligt att samla in fordonsdata som underlag för behov av snöröjning medan det är mer känsligt att använda samma data som underlag för att bedöma hur väl snöröjningen sköts av den som vunnit upphandlingen. I det senare fallet pekas en specifik aktör ut vilket kan få konsekvensen under förutsättning att man antar att snöröjningen inte sköts ordentligt.

Ofta beror känsligheten på att fordonsdata blir knuten till en individ (personuppgift) och motmedlet blir att anonymisera data. Men då tappar man också möjligheten att erbjuda individualiserade erbjudanden eller personliga analyser. Värdet på erbjudandet går då ned. Om den aggregerade massdata visar att det enda fordonet som slirar med däcket är din bil så kan du erbjudas information om närmaste verkstad. Om analysen istället visar på att det är halt kan rätt aktör kallas till platsen för att bekämpa halkan. Om din data är anonymiserad kan du inte få erbjudandet om däckbyte. Men du kanske valde att vara anonym för att du inte ville ha reklam för närmaste verkstad med följden att du är en trafikfara? Det här öppnar upp en fråga om vilken data man kan avsäga sig att dela och ta emot och hur erbjudanden paketeras.

En intressant iakttagelse är att det ofta hänvisas till GDPR som en anledning till att man inte samlar in eller utvecklar tjänster kring fordonsdata. Detta kan också vara en mental spärr utifrån att man är rädd att göra fel så då är det bäst att inte göra något alls.

3.4 Diskussion

Som nämndes i metodsektionen så är inte temana ortogonala. Det finns t.ex. uppenbara kopplingar mellan hållbara affärsmodeller och kommersialisering. En skillnad är att kommersialisering siktar på hur förutsättningarna för en första affär kan skapas medan hållbara affärsmodeller istället fokuserar på hur den affären kan organiseras så den består och utvecklas över tid. Här är t.ex. innovationsupphandling en möjlighet att skapa en första affär, både ur ett juridiskt och ett tekniskt perspektiv, men det bygger inte en hållbar affär på lång sikt.

Det är också tydligt att det finns en motsättning mellan hur de kommersiella datasäljarna vill kunna utveckla sitt erbjudande och hur de existerande avtalen kan bromsa den utvecklingen. Lösningen är inte svår i juridisk bemärkelse, det går att omförhandla avtalen, men öppnar för komplexitet i sitt genomförande – om det finns mer pengar att tjäna kommer avtalsparterna bevaka sina intressen och andra intressenter kan mycket väl se sig som parter och vilja vara med i de nya avtalen. Här kan det behövas mer arbete för att skapa tydlighet kring vem som är part och vad som är en rimlig ersättning för vem samt vad GDPR egentligen innebär för upprättandet av sådana avtal.

Utmaningen är att avtalsmässigt hantera variationen med olika parametrar/olika data och datamängder för olika situationer. Det går att dra paralleller mellan geofence-zonen och ett avtal. Variationen av vilken data som ska ingå kan hanteras i avtal, men kräver resurser att samordna och anpassa samt behöver uppdateras varje gång det sker en förändring i vilken data som samlas och för vilka syften den används.

3.5 En gemensam inre marknad för fordonsdata

Över tid kommer innovation kring fordonsdata behöva relatera till vad som händer på den europeiska marknaden. Det ger skapar både möjligheter och utmaningar, allt ifrån harmoniserade standarder till reglering av vilka möjligheter det finns för det offentliga att tvinga sig till data.

Vilka fordon som i praktiken får användas på vägarna bestäms i delar baserat på EU-regler, till viss del av svenska regelverk. Det innebär att ett fordon som är typgodkänt och registrerat i ett annat EU-land som utgångspunkt också kan färdas på svenska vägar. Det blir därmed i praktiken svårt för svenska staten att som enda land kräva av fordonstillverkarna att de ska installera de nödvändiga systemen som krävs för att samla in fordonsdata utifrån grunden beslag. Det är inte heller möjligt att utgå ifrån att fordonsdata lagras eller processas i Sverige bara för att den samlats in där.

Eftersom trafik till sin natur både är nationell och internationell kommer det att behövas gemensamma regler inom EU för myndigheters tillgång till fordonsdata. Ett system som innebär en ständig informationsinhämtning/övervakning eller lagring av stora mängder fordonsdata för det fall att uppgifterna behövs för brottsbekämpning kan ifrågasättas juridiskt. Ett sådant system skulle bli föremål för samma överväganden som lett till att EU-domstolen och flera nationella domstolar i EU underkänt lagstiftning för lagring av

trafikdata från mobiltelefoner för brottsbekämpande ändamål.[5] Systemet med e-call,[6] som tagits fram på EU-nivå, är av integritetsskäl utformat på sådant sätt att det inte är möjligt att samla in uppgifter förrän det aktiverats i fordonet genom en olycka eller manuellt.[7]

Det är således nödvändigt att dela fordonsdata endast för begränsade och väl definierade ändamål och att behandlingen av de data som samlas in hanteras på ett kontrollerat sätt. En väg framåt är att öppna upp för mer dynamiska avtal inom ett specifikt rum som är avgränsat i geografi och tid. Att då vistas i rummet är likställt med att gå med på datainsamlingen. Vi har valt att kalla det förfarandet för geofencing som avtal.

4 Geofencing som avtal

I det här avsnittet preciserar vi först vad vi menar med geofencing och avtal, för att sedan diskutera avtalsrymden och hur den kan användas för att identifiera de kvaliteter som vi tror utmärker lämpliga första områden för det privata att erbjuda fordonsdata kring.

4.1 Geofencing

Geofencing innebär att man skapar geografiska områden på en digital karta och kommunicerar regler till och för fordonen som kör inom området. Detta förutsätter att fordonen är uppkopplade, liksom att myndigheter och fordonsindustri är överens om regelverk (och standarder) kring begränsningar och möjligheter i det geografiska området och kommunikationen av detta. Möjliga tillämpningar som har blivit lyfta tidigare är t.ex. att bara behöriga fordon kan köras inom t.ex. en miljözon, att säkra hastighetsbegränsningar utanför skolor eller anpassa drivlinan på fordonet så att det i området bara kan köras på eldrift. Eftersom uppkopplade fordon kan visa att de har följt trafikregler eller andra anvisningar (t.ex. enligt ramavtal vid upphandling) finns vinster för regelefterlevnad. Vi har samlat mer information om geofencing ur ett juridiskt perspektiv i Appendix A.

4.2 Avtal

Vår ansats är inte att vara uttömmande om avtal utan att ge en kort överblick för att etablera ett gemensamt begrepp.

När jag väljer att söka via en viss sökmotor eller går in på nyhetssajt så går jag också med på att dela med mig av min data. Det finns ett utrymme för hur mycket data jag delar

[5] Se exempelvis EU-domstolens domar i de förenade målen C-293/12 och C-594/12, de förenade målen C-203/15 och C-698/15 samt C-623/17 som handlat om lagring av och tillgång till trafikuppgifter (telekommunikation) för brottsbekämpande ändamål.
[6] Alla nya bilar i EU skickar automatiskt ett meddelande till det enhetliga europeiska larmnumret 112 i händelse av en allvarlig olycka, upptäckt genom aktivering av en eller flera sensorer eller processorer i fordonet, på unionens territorium. Se EUROPAPARLAMENTETS OCH RÅDETS BESLUT nr 585/2014/EU av den 15 maj 2014 om införande av en interoperabel EU-omfattande eCall-tjänst.
[7] Art. 6 EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2015/758 av den 29 april 2015 om typgodkännandekrav för montering av eCall-system som bygger på 112-tjänsten i fordon och om ändring av direktiv 2007/46/EG.

med mig av och det finns dessutom en möjlighet att välja andra sökmotorer eller nyhetssajter. I många fall finns det dessutom andra alternativ, jag kan gå till biblioteket och anonymt läsa i uppslagsverken eller tidningen, eller välja ett inkognitofönster i webbläsaren.

För det fortsatta resonemanget är det viktiga här att avtalet med sökmotorn, tidningen eller biblioteket är frivilligt att ingå. När jag ingår avtalet anges också vad som gäller, specifikt i form av ersättning. Att avtal kan vara svåra att läsa och förstå är en annan fråga som vi lämnar utanför resonemanget för stunden. Det finns också andra avtal som inte är valbara att ingå eller där du inte blev informerad om villkoren när du ingick avtalet. Rätten till liv till exempel. Du fick inte välja det avtalet och du blev inte heller informerad av vad avtalet består av men du omfattas ändå av ett samhällskontrakt som medborgare. Vi hänvisar till Appendix B för en utförligare beskrivning av tvång och datadelning.

Vikten av att kunna erbjuda alternativa zoner beror på hur kritiskt det är för samhället att få tillgång till data. Om det visar sig att data behövs för brottsbekämpning kan det legitimera att inte erbjuda alternativa vägsträckor eller områden. Att delta i datainsamlingen är då inte ett val individen äger. Om data däremot är önskvärd, men inte kritisk kan det berättiga att man säkerställer att det finns parallella vägar eller alternativa områden där det inte sker datainsamling. Som individ kan man då välja att delta i datainsamlingen eller inte.

4.3 Avtal i kvadrat

Avtal gäller som huvudregel mellan de ingående parterna, och inte i förhållande till annan part. Eftersom fordonskamerorna delar data också om medtrafikanter behöver det finnas något sätt att reglera den datainsamlingen och datadelningen. Ett sätt att göra det på är att tydligt begränsa var och när data samlas in genom geofencing. Det skulle kunna ge tydlighet åt alla intressenter att här samlas data in. Men också ge de konkreta förutsättningarna för kommersialisering och styra datainsamlingen utifrån förmågan att förädla densamma, se avsnitt 3 eftersom det blir färre och mindre datamängder att hantera.

Inom den geofencade zonen skulle det kunna finnas friare ramar för insamling och förädling – tänk regulatorisk sandlåda eller testbädd[8]. Det öppnar upp för mer dynamiska avtal som är flexibla i vad de tillåter i form av datainsamling, förädling och användning.

Titeln på avsnittet anger att vi har med två avtalsrymder att göra – en för frivilligheten att ingå avtalet och en för ersättningen för den delade data. Om man kombinerar de två får man en matris som återges i Bild 1. På den horisontella axeln återfinns då samhällskontraktet med individens orubbliga integritet i ena änden och samhällets odiskutabla rätt att sätta allas bästa framför individuella särintressen. På den vertikala axeln speglas den ersättning som utgår för att dela data inom det avgränsade rummet. Där har vi i ena änden den reglerade, fasta ersättningen och i den andra änden finns det förhandlade avtalet som bestäms utifrån marknadens utbud och efterfrågan. I bild 2 ger vi fyra exempel, ett för varje kvadrant i matrisen.

[8] https://www.kometinfo.se/wp-content/uploads/2020/01/Försök-för-teknologisk-innovation_Komet-beskriver-2019_09.pdf

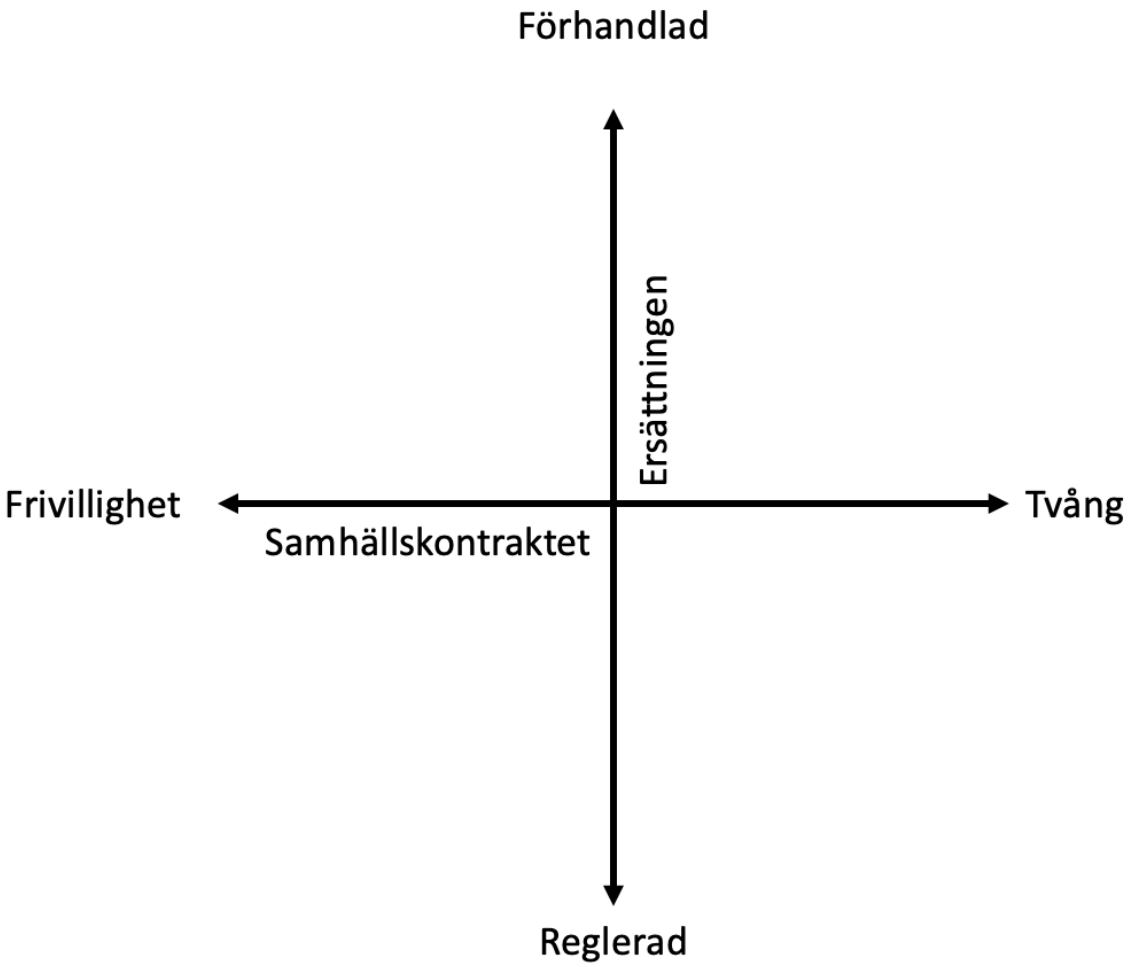

Bild 1: Geofencing som avtal i teorin. På den horisontella axeln återges individens möjlighet att acceptera ett avtal om att vara en part i datainsamlingen, på den vertikala axeln visas ersättningen som fås av att delta.

I det övre vänstra hörnet hittar vi offentligt uppköpt snöröjning. Den offentliga väghållaren har då lagt ut en upphandling på snöröjning och det anbud som bäst matchar villkoren får kontraktet. Det är frivilligt att delta i upphandlingen och man kan påverka vilken ersättning man får genom det pris man anger i sitt bud.

I det övre högra hörnet har nu frivilligheten gått över till tvång, men vi har fortfarande marknadsmässig ersättning för tjänsten (faktisk kostnad). I det här hörnet hittar man t.ex. fallet med tolkning av den svarta lådans innehåll. För att utreda en dödsolycka kan tillverkaren av olycksfordonet få i uppdrag att tolka data från lådan för att bistå i utredningen. Ersättningen är då i proportion till hur mycket arbete som krävs för att utföra uppdraget.

I det nedre vänstra hörnet hittar vi t.ex. skolpengen. Här är det frivilligt att starta en friskola men ersättningen per elev är fast utifrån schablon. Förmågan att gå med vinst i en sådan modell beror på hur man balanserar antalet elever emot kostnaden för undervisningen man erbjuder.

Slutligen har vi det nedre högra hörnet där vi hittar våra teleoperatörer. Deras tjänst är så viktig att de är tvingade genom lag att bistå de brottsbekämpande myndigheterna med data. Samtidigt är trafikdata från mobiltelefoner eftertraktat av de brottsbekämpande myndigheterna, vilket leder till ökad administration och därmed ökade kostnader för

samhället. För att förenkla hanteringen för samhället får inte längre teleoperatörerna ersättning för faktisk kostnad utan operatörerna ersätts istället utifrån ett schablonbelopp oavsett vad det kostar att ta fram den begärda data.

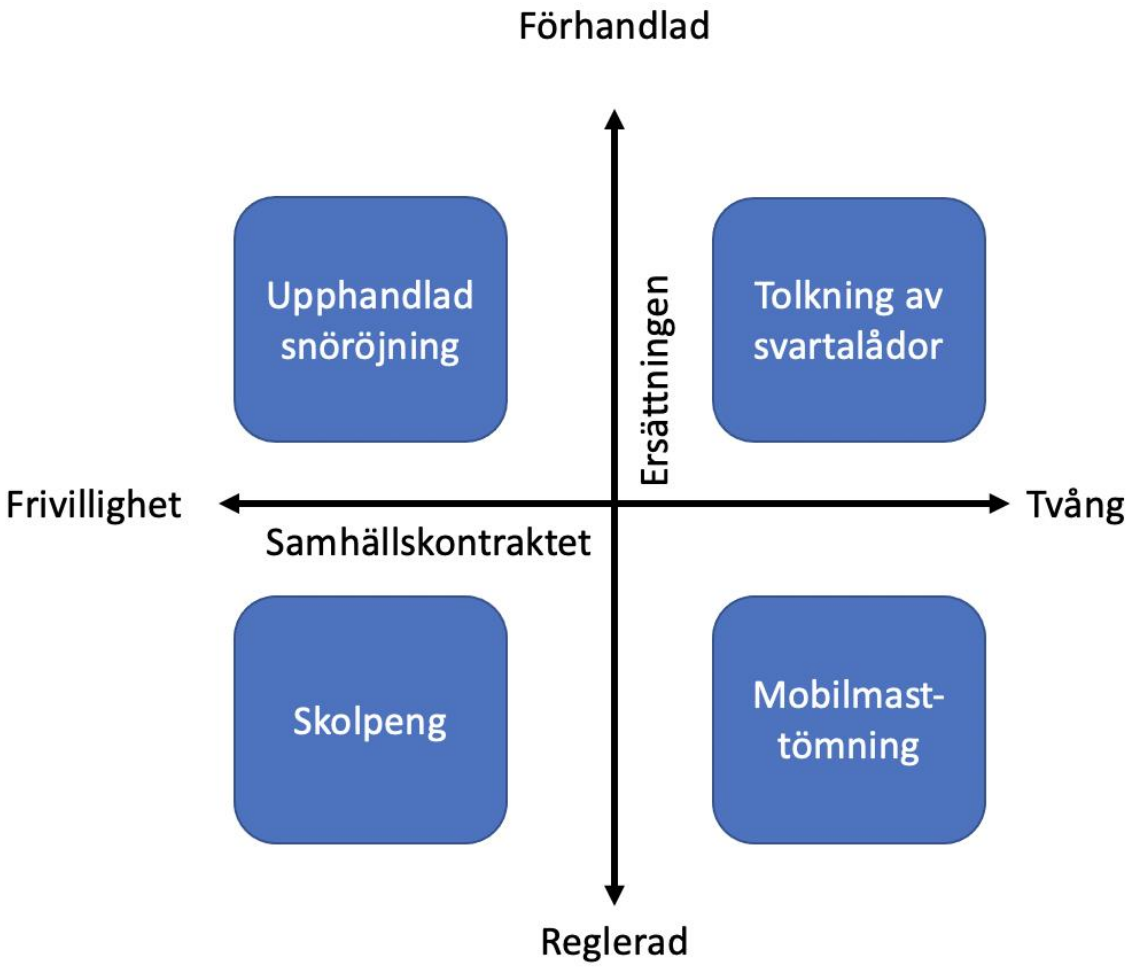

Bild 2: Snöröjning och brottsutredning som exempel på avtal inom en geofencad zon. Här är brottsutredningar så viktiga att individen inte kan tacka nej till att delta men ersättningen för den insamlade data behöver inte utgå från en schablon. Detsamma gäller snöröjning. Beroende på var datainsamlingen sker kan snöröjning tilldelas olika vikt i relation till samhällsintresset och ersättas olika beroende på vilka avtal som sluts.

Vår spaning är att förhandlad ersättning (faktisk kostnad i varje fall) går över till reglerad ersättning (schablon) när efterfrågan på data från samhällets sida ökar. Med det menas att ju oftare tjänsten efterfrågas desto bättre underlag får man för att hitta ett genomsnitt för vad det kostar (tänk skolpeng) alternativt så stiger den totala kostnaden då tjänsten blir allt mer oumbärlig för samhällelig verksamhet där tvång kan anses berättigat. Givet det så verkar det mest gynnsamt att utforska möjligheten till innovation genom upphandling av verksamhet där frivillighet för de ingående parterna är önskvärd samt att det inte finns en etablerad leverantör redan, se bild 3.

Att fokusera på den övre vänstra kvadranten är också lämpligt ur ett internationellt perspektiv. Finns inte tjänsten finns det antagligen också ett större manöverutrymme för

att utforska tekniska lösningar eftersom standardiseringsinitiativen inte hunnit dit än. Man kan då både påverka hur affären ska se ut och hur framtida standarder på en harmoniserad marknad kan utformas.

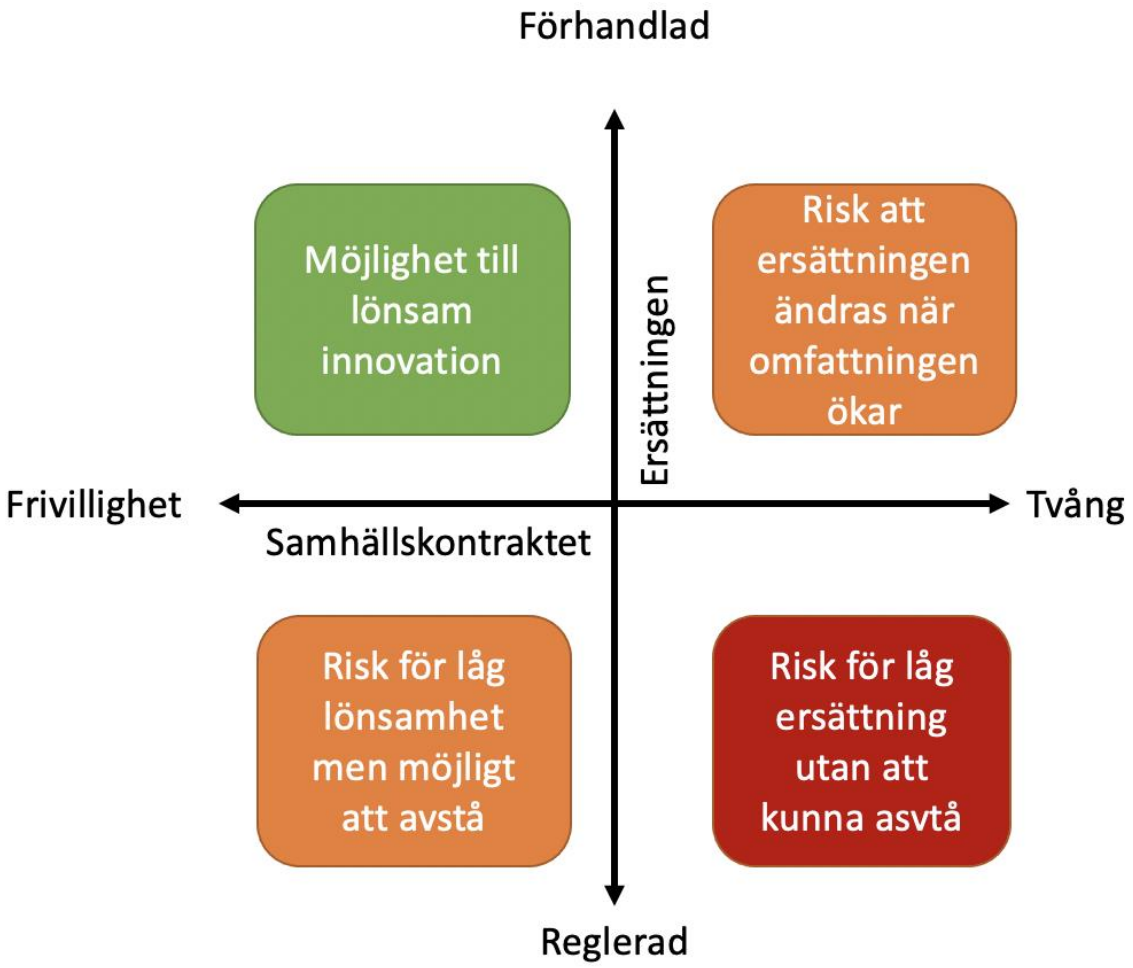

Bild 3: Ersättning för fordonsdata utifrån olika scenarier.

4.4 Ett varningens finger

Vem sluter avtalet och vem får ersättning? Vår modell säger inget om vilka avtalsparterna är. Det är möjligt att om det uppstår affärer där säljaren har en möjlighet att gå med vinst så kommer fler vilja ha en del av förtjänsten. Om avtalet sluts med det offentliga som köpare, vem är då säljare? Vi ser att det finns ett antal tänkbara alternativ. Är det t.ex. kameratillverkaren, fordonstillverkaren, ägaren till fordonet eller den som kör fordonet? Kanske alla ser sig som säljare av fordonsdata och därmed vill vara med i avtalet. Men det kan också bli så att någon aktör ser till så att den blir ensam innehavare till fordonsdata och därmed ensam säljare av fordonsdata.

Samtidigt som det finns stora möjligheter för att stötta teknikutvecklingen genom innovationsupphandling eller policyutveckling ska vi komma ihåg att ibland är det bra att regelverken bidrar med tröghet i relation till introduktionen av ny teknik. Trögheten skapar en plattform för att göra säkrare förutsägelser om framtiden, t.ex. vid investeringar eller i relation till våra demokratiska rättigheter.

Ett konkret exempel kommer från San Diego, Kalifornien, där myndigheterna valt att stänga ner 3200 smarta trafikljus[9]. Anledningen var att det saknades en tydlighet om hur den insamlade data får eller inte får användas för andra syften än de tänkta. I trafikljusens fall var det ursprungliga syftet att öka trafiksäkerheten men snart kunde man se att videoströmmarna från stolparna också kunde användas för att klara upp brott. Men det fanns ingen demokratisk process som hade godkänt ett sådant användande. Sannolikt kommer trafikljusen att åter tas i bruk och användas för brottsbekämpning men då efter att beslutet tagits genom den vedertagna demokratiska processen[10]. Att teknikutvecklingen går i samma takt som den demokratiska processen är viktigt för att etablera samhällelig tilltro till både de tekniska och demokratiska systemen.

Utifrån våra diskussioner om geofencing hade en möjlig väg framåt varit att låta trafikljusen installeras i en geofencad zon där avtalen tillät andra användningsområden än det uttalade. Då hade man haft en konkret situation att utgå ifrån när man diskuterar lämpligheten av sådana zoner och randvillkoren för att upprätta dem.

[9] https://www.bloomberg.com/news/articles/2020-08-06/a-surveillance-standoff-over-smart-streetlights Publicerad 2020-08-06
[10] https://cities-today.com/how-cities-are-defining-the-rules-of-engagement-for-emerging-technology/ Publicerad 2020-11-16

Appendix A: Geofencing ur ett juridiskt perspektiv

Det här avsnittet utgör en sammanfattning av de diskussioner vi haft om geofencing ur ett juridiskt perspektiv i relation till det aktuella projektet. Den här sammanställningen är alltså inte uttömmande utan ska ses som ett levande material som kommer att uppdateras efter behov och när nya fakta tillkommer.

Frågan om geofencing aktualiserades för breda massor på allvar första gången efter terrordådet på Drottninggatan i Stockholm den 7 april 2017, bl.a. genom ett regeringsinitiativ om att kraftsamla kring hur man gemensamt kan ta tillvara digitaliseringens möjligheter och som ett första steg påbörja ett arbete som kunde utmynna i att demonstrationer med geofencing blev verklighet.[11] Handlingsplanen som initiativet mynnade ut i pekade ut behovet av att verka för lagstiftning och regelverk som stöttar implementering av geofencing samt att utveckla organisatoriska och digitala processer samt data för geofencing-zoner.[12] Någon rättslig definition av geofencing som kan användas på det fall vi nu utreder finns ännu inte. Som framgår av legalitetsprincipen ställer verksamhet inom det allmänna kravet på författningsstöd.[13] Det finns vidare krav i regeringsformen att ett koncept av nu aktuellt slag, som innebär ingrepp i enskildas personliga förhållanden, regleras i lag.[14] Om det allmänna ska besluta om tillgång till data med hjälp av geofencingteknik krävs därför att frågan författningsregleras i någon form för att det allmänna ska såväl få ägna sig åt verksamheten som kunna framtvinga inhämtning.

En framtida legal definition för regelgivning riktad mot fordon i trafik skulle kunna utgå från någon eller en kombination av följande utgångspunkter.

- En eller flera platser och ett visst avstånd från dessa. Det kan i nu aktuellt exempelvis vara en plats för olyckan och ett visst avstånd från detta. Det kan även kompletteras med olika avstånd i olika riktningar (för att så långt som möjligt inte i onödan träffa exempelvis en lokalgata bredvid eller bro/tunnel som är separerad från avsedd plats).[15]
- En eller flera punkter som tillsammans markerar gränserna för ett område, exempelvis hörnen på en rektangel på marken eller tredimensionell kub.[16]

---

[11] https://www.regeringen.se/pressmeddelanden/2017/05/handslag-om-digitalisering-och-geofencing/

[12] https://www.trafikverket.se/contentassets/dbf70a5e74b745be8551f3fbde590f00/handlingsplan---gemensam-kraftsamling-kring-digitalisering-for-sakra-och-smarta-stadsmiljoer.pdf, s. 5.

[13] Se 1 kap. 1 § 3 st regeringsformen och 5 § 1 st förvaltningslagen (2017:900).

[14] 8 kap. 2 § 2 regeringsformen. Det går dock i lag att delegera till regeringen eller den myndighet regeringen utser.

[15] Såvitt vi förstått är det att utgå från en position i form av en punkt som ligger närmast hur SOS Alarm idag arbetar. Det kräver dock antagligen att det finns andra lösningar för att hantera fallet med att identifiera så att regeln tillämpas rätt på platser med samma höjd eller sidledsegenskaper.

[16] En variant på detta skulle kunna vara att basera det på fastigheter eller delar av fastigheter (inkl. tredimensionella fastigheter). Denna aspekt har vi inte behandlat närmare.

- En sektion av en sträckning på en vägkarta eller motsvarande inklusive i förekommande fall vissa körfält, körriktning osv.

Det finns en risk för att det sätt som används för att beskriva geodata som tas fram inom ramen för vad som gäller för det allmännas verksamheter inte med enkelhet på ett automatiserat sätt kan överföras till fordonstillverkares system som utgår från andra lösningar kompatibla i flera länder. För att ett system för automatiserad geofencing i trafiken är det viktigt att reglerna blir exakta nog för att inte omfatta en väg vid sidan om, över eller under avsedd vägsträcka (exempelvis olycka på motorväg men inte på lokalgata på bro ovanför) om det inte just är ett större område som avses (exempelvis ett utsläpp i luften av farliga ämnen). Det är i dagsläget oklart hur det ska förenas med ett positionsbaserat system som inte utgår från en offentligt tillgänglig vägkarta. Det är möjligt att de som utvecklar navigeringssystem av olika slag och offentliga aktörer som ansvarar för olika IT-system kan hitta lösningar på detta, men det blir principiellt problematiskt om tillämpningen av regler blir beroende av mellanhänder som behöver tolka och sätta regler i ett sammanhang i för stor utsträckning. Den straffrättsliga legalitetsprincipen[17] ställer krav på att författningar ska vara tillgängliga för var och en i en läsbar form. Förenklat kan det komma att kräva lagändringar om trafikregler ska förutsätta stöd av mellanhänder. En sådan utveckling kan få svåröverblickbara konsekvenser.

Vid en mer planerad regelgivning som kungörs i god tid är utmaningarna på vissa plan mindre då det i princip kan ritas ut manuellt på en traditionell karta och sedan kungöras tillsammans med föreskriften och därmed lämnas till fordonstillverkarna och eventuella mellanhänder för att inarbetas i deras system. Ett automatiserat system är dock nödvändigt för omedelbart ikraftträdande men fungerar även med andra permanenta ändringar såsom hastighetsbegränsningar, information på vissa vägar, miljözoner m.m. Utvecklingen går mot fler och fler regler med tiden, varför det finns starka skäl att överväga ett system som inte kräver manuellt arbete.

Det är således relevant att, vid ett framtida lagstiftningsarbete för att få till automatiserad geofencing med hög precision, utgå från en teknisk lösning som från början är anpassad för att möjliggöra sömlös översättning in till olika fordonstillverkares vägdatabassystem. Här kan särskilt lyftas fram skillnaden mellan ett system som avser (i) mindre förfinad information om exempelvis fordon i ett visst geografiskt område/avstånd från punkt som torde kunna genomföras genom regelgivning med angivande av koordinater enligt nationell eller internationell standard, (ii) viss vägsträcka där författningen behöver granskas och översättas i en mer eller mindre manuell process för att fungera med den aktuella fordonstillverkarens system och (iii) viss vägsträcka där författningen utformats på ett sådant sätt att fordonstillverkares system omedelbart och automatiskt kan tillämpa den.

I linje med ovan nämnda handlingsplan behöver arbetet med den digitala regelgivningen på trafikområdet intensifieras. Avståndet mellan möjligheterna till regler för fordons användning som kommer från fordonstillverkarna själva eller olika former av privata initiativ och regler från det allmänna är för stort. I dagsläget är det långt bort innan det är såväl lagtekniskt som praktiskt möjligt att införa den typen av geofencingbaserade system som avses. Vi skulle gärna se att det vidtogs fler initiativ från det allmänna (gärna

[17] 2 kap. 10 § regeringsformen.

på EU-nivå) att finansiera arbetet med att lösa de nödvändiga tekniska frågorna i tät dialog med näringslivet.

Det finns möjlighet att på privat/avtalsväg införa egna geofencing-lösningar och det har tillämpats i begränsad skala. Det kan handla om att företag spärrar sina egna fordon till vissa områden, att de begränsar förares möjlighet att bryta mot trafikregler (exempelvis hastighet), informerar om att ett fordon är framme vid en lastkaj eller skräddarsyr kommersiell information/reklam efter plats. Större samarbeten genomförs främst inom området säkerhetskritisk information som skulle kunna få stort genomslag i framtiden.[18]

Det allmänna kan agera inom ramen för offentlig upphandling, genom att upphandla baserat på funktionskrav som leder till behov av geofencingteknik. Det ska inte underskattas den möjlighet som finns redan idag att hitta geofencinglösningar för den verksamhet som bedrivs och finansieras av det allmänna.

Det finns även en stor mängd trafikinformation som är tillgängliga för olika privata företag som utvecklar kart/navigeringssystem m.m. via API:er och europeiska standardformatet DATEX II. Via fysiska skyltar finns även möjlighet att stänga av filer, reglera hastighet m.m.

Ett exempel på frivillig lösning är den positionsanpassade information som tillgängliggörs om olyckor i närheten av användaren och position som skickas till SOS Alarm vid larm till larmnumret 112 via SOS Alarms app.[19] Positionen vid larmsamtal delas även från många smarta telefoner genom systemet Advanced Mobile Location (AML). Från den 17 mars 2022 blir systemet obligatoriskt i smarta telefoner i EU.[20]

Trafikföreskrifter meddelas primärt av kommunerna, länsstyrelserna och Trafikverket. Det finns även andra myndigheter som i mindre omfattning meddelar trafikföreskrifter.[21] När det gäller enskilda vägar får idag ägaren av vägen besluta om vissa begränsningar.[22] Det kan övervägas i vart fall en ordning där ägare av enskilda vägar som är öppna för allmän trafik eller det annars finns särskilda skäl ska kunna begära hos myndighet att de beslutar om geofencingregler inom rimliga gränser.

Regler med geofencing bör kunna beslutas om för såväl permanenta som tillfälliga regleringar. Permanenta regleringar med sedvanlig beredning och remissförfarande bör fortfarande vara en stark huvudregel. De beslut som kan fattas i god tid innan ett tänkt ikraftträdande kan som beskrivits i avsnitt **Error! Reference source not found.** införas innan det finns möjlighet till digital regelgivning som kan tillämpas först efter ett manuellt förfarande hos fordonstillverkaren.

---

[18] Se bl.a. samarbetet Data for Road Safety, https://www.dataforroadsafety.eu/.

[19] https://www.sosalarm.se/pressrum/nyheter/2019/112-appen/
På frivillighet bygger dock inte systemet med E-call. Det systemet skickar information om bl.a. geoposition vid olycka men kan inte fjärrstyras för att hämta in information. Se avsnitt **Error! Reference source not found.** nedan.

[20] KOMMISSIONENS DELEGERADE FÖRORDNING (EU) 2019/320 av den 12 december 2018 om komplettering av Europaparlamentets och rådets direktiv 2014/53/EU vad gäller tillämpningen av de väsentliga krav som avses i artikel 3,3 g i det direktivet i syfte att säkerställa lokalisering av nödsamtal från mobila enheter. Att systemet på införts utan lagkrav med stöd av allmänna villkor som få konsumenter läser kan uppfattas som kontroversiellt.

[21] Se bl.a. 10 kap. trafikförordningen (1998:1276).

[22] Se 10 kap. 10 § trafikförordningen (1998:1276).

Det är möjligt att med kortare varsel fatta beslut om föreskrifter om ett beslut av kommunen eller länsstyrelsen inte kan avvaktas utan särskild olägenhet eller det i övrigt är nödvändigt för vissa ändamål.[23] Det är idag framförallt Polismyndigheten som har den möjligheten. Gränsdragningen mellan vad som snarare är lämpat som förvaltningsbeslut bör studeras närmare.

[23] 10 kap. 3 § 2 st. och 14 § trafikförordningen (1998:1276).

Appendix B: Datadelning ur ett juridiskt perspektiv

Det här avsnittet utgör en sammanfattning av de diskussioner vi haft om datadelning ur ett juridiskt perspektiv inom projektet. Det finns mer att säga i frågan, men det får bli i ett annat sammanhang.

Bestämmelser om inhämtning av data från vägtrafiken är av en annan karaktär än övriga bestämmelser som syftar till att reglera trafiken som sådan och täcks därmed inte av det bemyndigande riksdagen lämnat till regeringen i lagen (1975:88) med bemyndigande att meddela föreskrifter om trafik, transporter och kommunikationer. Inhämtning av data kräver således stöd i lag beslutat av riksdagen. Givet det integritetsintrång det kan bli fråga om bör det enligt oss starkt övervägas att inte reglera mer än absolut nödvändigt på förordnings eller föreskriftsnivå.[24]

Det kan tänkas finnas tillfällen där det inte är lämpligt att fullt ut informera enskilda om skälen bakom att inhämta eller inte inhämta data från fordon. Det är också en fråga om i vilken utsträckning myndigheter vill avslöja vad de letar efter till privata aktörer, samtidigt har de inte alltid egen förmåga att samla in eller förädla data vilket öppnar för tvång som en möjlig väg att få data utan att fullt ut ersätta kostnaderna för den. Även beträffande traditionell övervakning av telefontrafik får dock privata aktörer kännedom om känsliga uppgifter. I längden tror vi att det blir svårt att undvika ett liknande system för fordonssektorn om data anses vara samhällskritisk.

Redan idag finns det i extrema fall möjligheten att gå så långt som att använda bl.a. hemlig rumsavlyssning (buggning) och hemlig dataavläsning (lagligt dataintrång i mobiltelefoner m.m.) för att samla in uppgifter.[25] Det är dock viktigt att det i så långtgående fall finns ett väl etablerat skydd för den personliga integriteten. Givet att det samlade statliga integritetsintrånget ökat och skulle öka än mer bör ytterligare skyddsmekanismer än de som finns för dagens insamling övervägas.

För polismyndigheten kan det vara känsligt att för utomstående berätta om de är intresserad av ett visst fordon eller inte när de bedriver spaning. Den informationen vill de behålla för sig själva. Däremot skulle det vara intressant att samla in data från fordons sensorer i efterhand för att utreda brottslighet. Att i efterhand tillgripa data förutsätter dock att uppgifterna av andra skäl samlas in på ett sådant sätt att det är möjligt. Det kan ifrågasättas om strömmande video och annan sensordata frivilligt skulle sparas i den omfattningen som skulle krävas.[26] Frågan är dock i vilken utsträckning som det kommer

[24] Jmf 33 § lagen (2020:62) om hemlig dataavläsning där det endast är vissa enstaka frågor av mindre vikt som överlåtits till regeringen eller den myndighet som regeringen bestämmer. Det finns även tveksamheter utifrån nuvarande system att låta myndigheter meddela föreskrifter som träder i kraft samma stund som de publiceras. Det är även problematiskt att hemlighålla föreskrifter även så länge det finns sekretesskäl.

[25] Se lagen (2007:978) om hemlig rumsavlyssning och lagen (2020:62) om hemlig dataavläsning.

[26] Att proaktivt spara information för att det skulle kunna komma att begäras ut av brottsbekämpande myndigheter kan i ljuset av frågan om lagring av trafikuppgifter (telekommunikation) kan ifrågasättas om det är rättsligt möjligt. Se exempelvis EU-domstolens domar i de förenade målen C-293/12 och C-594/12, de förenade målen C-203/15 och C-698/15

finnas en vilja att utveckla sådana system som det allmänna med lätthet kan använda sig av om det inte finns en uttalad vilja från det allmänna att i förväg eller genom marknadsmässig ersättning i efterhand finansiera framtagandet. Detta ska ses mot bakgrund av de ingrepp i den personliga integriteten systemen medför (som ska vägas mot fördelarna) kan komma att leda till svårigheter att använda delar av systemen för andra ändamål här i landet. Det är dock möjligt att det finns andra marknader där acceptansen för sensorer såsom kameror är större.[27]

Om möjligheten öppnas upp för staten att tillgripa bildmaterial från fordon till skydd för olyckor kommer frågan uppkomma om material även ska tillgängliggöras för vissa andra mycket angelägna behov. Sedan den 1 april 2020 finns möjlighet att genom beslut enligt lagen (2020:62) om hemlig dataavläsning i hemlighet inhämta mycket integritetskänsliga uppgifter från enskildas tekniska utrustning såsom mobiltelefoner.

Frågan om datainsamling är känslig givet att allt fler möjligheter till statlig övervakning sammantaget innebär en allt större risk för enskildas personliga integritet. Det är rimligt att förutse att lagstiftarens utrymme att begära åtkomst till och i än större utsträckning lagring av uppgifter kan komma att begränsas kraftigt av EU-domstolen.[28] Det europeiska systemet för e-call är t.ex. inte möjligt att användas till övervakning då det ansetts för känsligt.[29]

Det finns uppgifter som är extra känsliga att samla in. Det kan exempelvis röra uppgifter som kan röja skyddsobjekt och annan känslig offentlig verksamhet eller privata uppgifter som normalt utesluts från hemliga tvångsmedel såsom grundlagsskyddade medier, advokater, sjukvårdspersonal och präster.[30] Skyddandet av sådana platser och individer är en aspekt som måste hanteras när man beslutar om datainsamling.

Vidare behöver det övervägas hur riskerna för dataintrång, för att därigenom på olovlig väg bereda sig tillgång till data från känsliga platser, ökar om det skulle tas fram ett system där myndigheter från utsidan i praktiken skulle ha direktaccess till data. Det ska jämföras med tvångsmedel som riktar in sig på telekommunikation där det saknas sådan direktaccess utan manuell inkoppling behöver ske.

Om det tas fram ett system där det är möjligt att tillgripa uppgifter från fordon är det i förlängningen mycket svårt att inte ge tillgång till dessa uppgifter för att tillgodose särskilt viktiga samhällsintressen om det sker under väl reglerade former. År 2020 infördes jämförelsevis möjligheten till hemlig dataavläsning vid bl.a. utredning av allvarlig brottslighet. Det är i sig ett mycket ingripande hemligt tvångsmedel givet den

samt C-623/17. På telekommunikationssidan finns dock en stor del uppgifter som av olika skäl ändå sparas en viss tid även om uppgifterna minskat sedan behovet av att spara dem för faktureringsändamål minskat efter att fastprisabonnemang blivit vanligare.

[27] Frågan kan bli känslig – kommer svenska skattemedel finansiera system som i andra länder kan användas på ett sätt som vi inte skulle acceptera? Samtidigt, kan vi tillsammans med andra likasinnade länder gå före med att ta fram system som från början balanserar olika intressen på ett klokt sätt som kan tjäna som förebild?

[28] Se exempelvis EU-domstolens domar i de förenade målen C-293/12 och C-594/12, de förenade målen C-203/15 och C-698/15 samt C-623/17 som handlat om lagring av och tillgång till trafikuppgifter (telekommunikation) för brottsbekämpande ändamål.

[29] Artikel 6 EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2015/758 av den 29 april 2015 om typgodkännandekrav för montering av eCall-system som bygger på 112-tjänsten i fordon och om ändring av direktiv 2007/46/EG.

[30] Jmf. 11 § lagen (2020:62) om hemlig dataavläsning.

stora del av människors liv som finns dokumenterade i exempelvis en mobiltelefon och i övrigt kan uppfattas med dess sensorer. Sedan innan finns möjligheten till hemlig rumsavlyssning av konversationer i ett fordon och i övrigt i privata miljöer med hjälp av installerad utrustning.

I stort kan reglerna för hemlig dataavläsning[31] användas som riktmärke för en sådan reglering. Det kan översatt till fordonsvärlden exempelvis innebära att uppgifter från misstänkts fordon kan inhämtas men även varje fordon som passerar viss plats av relevans för förundersökning skickar bilder (på samma sätt som exempelvis annan än misstänkts bostad i undantagsfall kan avlyssnas) eller att fordonen som misstänkta använder skickar information.

För det fall att uppgifter samlats in om exempelvis en trafikolycka och det inte bedöms finnas något motstående intresse av vikt i att meddela att övervakning skett bör det kunna ske till de som är kända (för att de exempelvis registrerats i en polisrapport med anledning av händelsen) och publiceras utan personuppgifter på hemsida. Det gör det möjligt för personer som anser att beslutet varit felaktigt och kränkt deras rätt har möjlighet att tillvarata sin rätt genom exempelvis Säkerhets- och integritetsskyddsnämnden (SIN). Användningen av möjligheterna blir därmed även tillgängliga för granskning av media. Det kan dock finnas ärenden med uppgifter som är känsliga och det bör övervägas en ordning, exempelvis endast granskning genom SIN.

För det fall att inhämtningen är att jämställa med ett hemligt tvångsmedel motsvarande exempelvis hemlig dataavläsning bör underrättelse ske till de som varit föremål för inhämtningen så snart det kan ske utan att röja särskilt viktiga uppgifter.[32] Här kan exempelvis förundersökningsskäl tala för att även om underrättelse bör ske så kan det vara lämpligt att göra så i senare skede. Även här kan publicering på hemsida övervägas om oidentifierade personer övervakats. Enligt dagens system behöver dock ingen underrättelse lämnas om det inte kunnat ske inom ett år och för vissa brott ska inte underrättelse alls ske. Det bör övervägas om inte underrättelse bör ske i fler fall även om det är så att det får ske långt eller i vissa fall mycket långt efter det att intrånget skedde. Det kan också övervägas om det bör ske en särskild granskning för att tillvarata enskilds intresse när underrättelse inte kan ske utöver den allmänna tillsyn SIN bedriver.

Idag fattas flera ingripande beslut om tillstånd för hemliga tvångsmedel av en enskild åklagare (i brådskande fall). Dessa beslut prövas sedan skyndsamt av domstol. Det finns således en granskning av såväl en oberoende funktion som fler ögon.[33] Det har dock visat sig i granskning av Säkerhets och integritetsskyddsnämnden att det förekommer brister i handläggningen där misstag begåtts av enskilda åklagare som lett till tvångsmedelsanvändning utan laglig grund.[34] Ett sätt att stärka processen är att i större utsträckning kräva att flera personer granskar och står bakom besluten. Det är visserligen kostnadsdrivande men är därigenom också en naturlig begränsning av hur omfattande övervakningen kan bli. Det kan ske såväl genom att flera åklagare i förening ska fatta besluten som att domstolsprövning införs i fler fall genom att stärka domstolarnas jourberedskap. När domstolarna nu har en mer omfattande

[31] Lag (2020:62) om hemlig dataavläsning.
[32] Se 27 kap. 31–33 §§ rättegångsbalken (1942:740).
[33] Se 14–17 §§ lagen (2020:62) om hemlig dataavläsning. I domstolsförfarandet finns även möjlighet till ett offentligt ombud.
[34] Se Säkerhets- och integritetsskyddsnämndens dnr 17–2020.

jourverksamhet är det naturligt att detta även kommer att minska åklagares rätt att fatta beslut om tvångsmedel med hänvisning till att domstolsprövning inte kan inväntas.[35]

Utredningen om ett förstärkt straffrättsligt skydd för vissa samhällsnyttiga funktioner och några andra straffrättsliga frågor (Ju 2020:12) har till uppdrag att bl.a. överväga och ta ställning till om det straffrättsliga ansvaret för tjänstefel bör utvidgas, samt överväga och ta ställning till om straffskalan för brott mot tystnadsplikten bör skärpas. Trots fall av brister i handläggningen av ärenden om hemliga tvångsmedel där det i granskning framkommit ”anmärkningsvärda och upprepade fel i handläggningen” beslutas det inte om åtalsanmälan.

I en stor del av de fåtalet fall som under åren överlämnats till Åklagarmyndigheten i enlighet med 20 § förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden har det inte lett till åtal med anledning av att det ansetts som ringa tjänstefel. Ringa tjänstefel är inte straffbart.[36] Denna bedömning har även gällt fall där Säkerhets- och integritetsskyddsnämnden funnit att

- åtgärder (olovligen) inriktats mot person under 15 år,[37]
- Polismyndigheten fortsatte verkställa hemlig rumsavlyssning trots att åklagaren hade hävt tvångsmedelsåtgärden,[38]
- Polismyndigheten beslutade om inhämtning av uppgifter om elektronisk kommunikation enligt inhämtningslagen utan lagligt stöd,[39]
- hemlig avlyssning avseende ett telefonnummer utfördes trots avsaknad av tillstånd,[40] och
- åklagare ansökte om och beviljades tillstånd till hemlig kameraövervakning och hemligt tillträde för installation av tekniska hjälpmedel enligt 27 kap. 25 a § rättegångsbalken (1942:740) trots att tillstånd till hemlig rumsavlyssning inte hade begärts eller beviljats.[41]

Av uppgifter från Säkerhets- och integritetsskyddsnämnden att döma har endast en åtalsanmälan lett till lagföring genom strafföreläggande.[42] I pågående översyn av tjänstefelsansvaret bör det övervägas att uttryckligen ställa särskilt höga krav vid användning av hemliga tvångsmedel och liknande verksamhet som omgärdas av stark sekretess. Som ovan nämnts kan risken för misstag minska om beslut fattas av mer än en person.

3535 Se införandet av utökad jourberedskap för att domstolar ska kunna förordna offentliga försvarare infört genom förordning (2019:673) om ändring i förordningen (1988:31) om tingsrätternas beredskap för prövning av häktningsfrågor m.m. Förslaget tillkom sedan riksdagen avslagit en proposition med förslaget att åklagare vid vissa tider på dygnet skulle kunna förordna offentliga försvarare.

36 20 kap. 1 § 1 st brottsbalken (1962:700).

37 Se Säkerhets- och integritetsskyddsnämndens dnr 88–2018.

38 Se Säkerhets- och integritetsskyddsnämndens dnr 196–2017.

39 Se Säkerhets- och integritetsskyddsnämndens dnr 169–2015 samt 130–2016.

40 Se Säkerhets- och integritetsskyddsnämndens dnr 66–2017 samt 144–2016.

41 Se Säkerhets- och integritetsskyddsnämndens dnr 111–2017.

42 Se Säkerhets- och integritetsskyddsnämndens dnr 52–2015 och Åklagarmyndighetens ärendenummer AM-72484-15. Det kan finnas fall som lett till arbetsrättsliga konsekvenser, straffrättsliga åtgärder som inte skett med anledning av Säkerhets- och integritetsskyddsnämndens granskning eller andra konsekvenser utan att det föranlett åtalsanmälan.

Det bör i det system som föreslås särskilt övervägas ett starkt sekretesskydd hos såväl myndigheter som företag som har att följa beslut med anledning av ett genomfört system med åtkomst av fordonsdata. Detta borde kunna hanteras utan större problem i linje med liknande regelverk. Uppgifter som fordonstillverkare och andra fått del av kring vilka uppgifter som begärts ut och innehållet i dessa borde normalt omfattas av tystnadsplikt.[43]

[43] Jmf. 32 § lagen (2020:62) om hemlig dataavläsning.

Appendix C: Drive Sweden Policy Lab

Drive Sweden Policy Lab initierades 2019 av Drive Sweden som ett initiativ för att stötta teknikutvecklingsprojekt inom Drive Swedens portfölj som hade stött på regulatoriska utmaningar. Tanken var då att dessa projekt skulle löpa på som planerat men att intressenterna i de projekten tillsammans med RISE skulle undersöka policy-aspekterna i ett systerprojekt, Drive Sweden Policy Lab (DSPL). Som namnet antyder skulle verksamheten bedrivas som ett policy lab utifrån erfarenheterna av tidigare policy-projekt inom Drive Swedens regi.[44]

Fördelarna med upplägget var att de ursprungliga projekten på så sätt inte behövde omfördela budget eller ändra sin planerade verksamhet inom projektet. Samtidigt kunde fler av Drive Swedens medlemmar ansluta till policy-arbetet om de såg liknande frågor utifrån sin egen verksamhet. För att möjliggöra en sådan lösning blev varje policy-fråga ett eget arbetspaket inom Drive Sweden Policy Lab med sin egen budget. Vidare lät vi den totala budgeten vara öppen så att det gick att ansluta nya arbetspaket under projektets gång. Projektformen i sig är alltså ett bidrag från projektet då det var ett nytt sätt att organisera projekt för att möta regulatoriska utmaningar i teknik-fokuserade utvecklingsprojekt.

DSPL startade med ett första möte i november 2019 med löptid fram till december 2020. Vid starten hade vi två arbetspaket, ett kopplat till CeViSS-projektet (Cloud enhanced cooperative traffic safety using vehicle sensor data)[45] och ett kopplat till Keolis och Volvos försök med självkörande stadsbussar.[46] [47]

För CeViSS var frågan hur fordonssensorer kan bidra med data till allmänhetens tjänst? I arbetet med den frågan såg vi att det finns ett intresse från myndigheters sida att upphandla fordonsdata men också en osäkerhet kring hur det ska gå till. Om polisen spanar efter en vit Audi i Solna kan fordon i närheten mycket väl ha data om fordonet utifrån olika sensorer. Men polisen vill knappast göra sin spaning publik på en öppen marknad. Samtidigt kan det finnas ett behov av historiska data i utredningsarbetet och det är ett spår som antagligen kan behöva följas upp. Här vill teknikleverantörerna gärna se en annan affärsmodell än den som teleoperatörerna har gentemot myndigheterna. Finns det inte en affär för dem är det inte heller lönt att utveckla tjänsten. Ur ett regelperspektiv är frågan inte komplicerad, det viktiga är under vilka avtal data samlas in och om de avtalen tillåter den sortens delning som myndigheterna kan vara intresserade av. Annars måste avtalen skrivas om för att möjliggöra nya tjänster. Framförallt finns affären i förädling av sammanslagna datamängder, något som få avtal stöder idag.

För Keolis och Volvo var frågan vilka regelverk som gäller för en självkörande buss i depå-miljö? Eftersom bussen bara skulle vara självkörande inne på depåområdet men manuellt framförd på allmän väg innebär det att bussen ska självcertifieras under Arbetsmiljöverkets tillsyn gentemot maskindirektivet istället för att

[44] https://www.drivesweden.net/projekt-3/platt
[45] https://www.drivesweden.net/en/projects-5/ceviss-cloud-enhanced-cooperative-traffic-safety-using-vehicle-sensor-data
[46] https://www.drivesweden.net/nyheter/unik-demonstration-av-sjalvkorande-buss-0
[47] https://www.drivesweden.net/projekt-3/automatisering-av-stadsbussar

Transportstyrelsen granskar den i relation till försöksförordningen. Vi såg dessutom en allmän trend i att självcertifiering blir allt viktigare inom fordonsindustrin, både för att hantera självkörande funktioner och för de nya dynamiska fordonskoncept som möjliggörs av löpande omkonfigurering av den fysiska plattformen samtidigt som säkerhetskritisk fordonsprestanda kommer ifrån olika molntjänster. Arbetet har presenterats för bl.a. BILSweden och Volvo samt Komet - Kommittén för teknologisk innovation och etik.

Arbetet med det tredje arbetspaketet påbörjades hösten 2020 efter en förfrågan från Trafikverket. Kontakten föranleddes av att Trafikverket fått ett regeringsuppdrag med målet att utarbeta förslag på system för informationsutbyte och öppna data för horisontell samordning.[48] Uppdraget löper 2018–2029 och fram till idag har uppdraget resulterat i två tidigare rapporter varav en presenterades 31 maj 2019 och den andra rapporten presenterades 30 juni 2020. Uppdraget förväntas leda till ökad transporteffektivitet och minskad klimatpåverkan. Frågan RISE fick på sitt bord var vilka legala aspekter det fanns kring horisontell datadelning för att effektivisera Sveriges transporter? Vi har sett att frågan är komplicerad ur ett konkurrensperspektiv. Vi kan också se att det finns en rad initiativ kring datadelning, men de har svårt att ta fart utifrån att marknaden är fragmenterad. Däremot har flera speditörer arbetat med att effektivisera sin marknadsdel, t.ex. Schenker för leverans av paket, och vi kan se hur IKEA och GreenCargo samarbetar för att få upp effektiviteten på tågsidan.

Resultatet från respektive arbetspaket går att få genom RISE rapport-serie från 2021.

[48] https://www.regeringen.se/regeringsuppdrag/2018/08/uppdrag-att-utarbeta-forslag-om-horisontella-samarbeten-och-oppna-data-for-okad-fyllnadsgrad/ Publicerad 28 augusti 2018.

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 2021:12 ISBN: 978-91-89167-95-7