Tillväxt och samhällsbyggnad
Bo Baudin

Certezza AB
Andreas Dahlqvist
Thomas Nilsson

Referenskonsekvensbedömning – trafikanalys med multisensorer - Sammanfattning

Inledning

Den tekniska utvecklingen har lett till att trafiken i den offentliga miljön idag kan analyseras med ny avancerad teknik i form av exempelvis multifunktionssensorer med kamerabevakningsfunktion (multisensor).

Denna typ av sensorer kan skapa stora nyttor för kommuner men innebär samtidigt risker för fysiska personers rättigheter och friheter.

Sveriges Kommuner och Regioner (SKR) har tagit fram en referenskonsekvensbedömning är tänkt att utgöra ett stöd för kommuner som vill använda multisensorer för att analysera och använda uppgifter om trafikflöden till samhällets nytta. Detta dokument sammanfattar innehållet i referenskonsekvensbedömningen.

Vid användning referenskonsekvensbedömningen åligger det nyttjaren att säkerställa att de ingående värdena är relevanta för den nyttjande parten och vid behov göra nödvändiga justeringar.

Stöd till det operativa arbetet och vid ansökningar för kamerabevakningstillstånd

Referenskonsekvensbedömningen är tänkt att användas såväl inför upphandling av som vid användning av multifunktionssensorer. Referenskonsekvensbedömningen innehåller en riskanalys och förslag på åtgärder för att hantera riskerna antingen genom att minska frekvensen av att hot realiseras eller att minska konsekvenserna om ett hot realiseras.

Referenskonsekvensbedömningen kan också användas som underlag och stöd vid ansökningar om kamerabevakningstillstånd.

En ansökan om tillstånd till kamerabevakning ska innehålla:

1. uppgift om den som ska bedriva bevakningen och i förekommande fall den som ska ha hand om bevakningen för tillståndshavarens räkning,

2. uppgift om bevakningens ändamål,
3. en beskrivning av bevakningen, särskilt den utrustning som ska användas, var utrustningen ska placeras, det område eller typ av område som ska bevakas och de tider då bevakning ska ske,
4. en bedömning av behovet av bevakningen och bevakningens proportionalitet i förhållande till ändamålet,
5. en bedömning av riskerna för intrång i den personliga integriteten och en beskrivning av de åtgärder som planeras för att hantera riskerna, och
6. uppgift om de omständigheter i övrigt som är av betydelse för prövningen av ärendet.

En konsekvensbedömning avseende dataskydd ska innehålla samma uppgifter som framgår av punkterna 1–2 och 4–5. Det innebär således att en framtagen konsekvensbedömning avseende dataskydd uppfyller en stor del av de krav som en ansökan om tillstånd ska innehålla.

Det är möjligt att en enda konsekvensbedömning kan användas för att bedöma flera behandlingar som liknar varandra vad gäller art, omfattning, innehåll, ändamål och risker. Det finns inget behov av att utföra en konsekvensbedömning i situationer som redan har studerats. Så kan vara fallet när liknande teknik används för att samla in samma slags uppgifter för samma ändamål. Detta kan också göras för liknande behandlingar som planeras av olika personuppgiftsansvariga. I dessa fall bör en *referenskonsekvensbedömning* delas eller göras allmänt tillgänglig.

Detta dokument sammanfattar den referenskonsekvensbedömning som SKR tagit fram och som är allmänt tillgänglig för alla som planerar att använda multisensorer för trafikanalys. Det är SKR:s förhoppning att underlaget kan användas för att minska riskerna för enskildas fri- och rättigheter, öka transparensen kring användning av multisensorer, underlätta för medlemmarna i deras planering och användning av multisensorer, underlätta handläggning samt minska handläggningstider för tillståndsansökningar.

Avgränsningar

Referenskonsekvensbedömningen uppmärksammar och hanterar risker för enskilda registrerade och tar således dessas perspektiv. Det är alltså inte en fullständig riskhanteringsmodell för andra områden inom organisationen, exempelvis informationssäkerhet för verksamhetens behov. Underlaget kan därför behöva kompletteras med en riskanalys för verksamheten.

Referenskonsekvensbedömningen är också avgränsad till en viss specifik användning och för särskilt angivna ändamål. Om kamerabevakning ska användas för ändamål utöver vad som anges i referenskonsekvensbedömningen så måste detta kompletteras särskilt av den som vill använda multisensorerna för sådana utökade ändamål som exempelvis brottsbekämpning eller liknande trygghetsökande ändamål.

Behandlingens art, omfattning och ändamål

Användningen av multisensorer syftar till att analysera trafikantslag, trafikvolymer, trafikbeteenden, trafikflöden, trafikvariation, fordonsmodell samt behov av exempelvis vägunderhåll och renhållning på vissa givna platser. Tekniken kan också användas för att upptäcka trafikolyckor och identifiera och motverka trafikfarliga situationer samt vid behov dirigera trafik. Samtidigt mäts andra uppgifter om miljön i området där sensorn är placerad som till exempel, temperatur, vägtemperatur, väglag, pollenhalt, lufttryck, partikelhalt m.m..

De personuppgifter som registreras är bilder på alla fysiska personer som rör sig i kamerans upptagningsområde samt registreringsnummer på fordon.

Genom uppgift om trafikslag, trafikvariation, rörelsemönster, hastighet, fordonsmodell i kombination med andra sensoruppgifter kan bland annat följande mål uppnås:

- Förbättring av miljö och klimat,
- förbättring av trafikflöden och minskad trängsel,
- förbättrad framkomlighet för kollektivtrafik,
- förbättrat underlag för stadsplanering och detaljplanering,
- förbättring och effektivisering av renhållning och väghållning, samt
- ökad säkerhet för trafikanter.

Dessa förbättringar förväntas leda till stora samhällsekonomiska vinster som är kopplade till resurs- och energieffektiviseringsvinster, miljö- och klimatvinster samt hälsovinster för enskilda. Användning och implementering av sensorsystem kan på olika sätt leda i samma riktning som FN:s globala mål. De mål som man arbetar för i samband med användning av multisensorer är följande:

Laglig grund för behandlingen

Den verksamhet som en kommunal myndighet bedriver, inom ramen för sin befogenhet, är av allmänt intresse. Det är därmed den rättsliga grunden i artikel 6.1 e i

dataskyddsförordningen som vanligen bör tillämpas av myndigheter, även utanför området för myndighetsutövning.

Utöver detta är kommuner i vissa fall väghållare inom kommunen. När en kommun är väghållare är den kommunala nämnd som kommunfullmäktige utser väghållningsmyndighet, (5 och 6 §§ väglagen (1971:948). Väghållning omfattar byggande av väg och drift av väg. Vid väghållning ska tillbörlig hänsyn tas till enskilda intressen och till allmänna intressen såsom trafiksäkerhet, miljöskydd, naturvård och kulturmiljö, (4 § väglagen).

Behov och proportionalitet

De positiva konsekvenserna kan bland annat sammanfattas i bättre miljö och klimat i form av minskade koldioxidutsläpp och partikelhalter i trafikmiljön. Detta kan i sin tur förväntas leda till bättre möjlighet att uppnå miljömål och minska personligt lidande för enskilda genom att dessa i lägre grad utsätts för skadliga partiklar och risker för sjukdomar därmed minskar.

Förbättrade trafikflöden och minskad trängsel kan leda till positiva effekter för framkomligheten och minskade restider vilket i sig kan medföra minskade utsläpp, lägre stress i trafiken och ökad produktiv tid. Minskad trängsel på gator och torg kan därtill leda till minskad smittspridning i samhället av såväl vanligt förekommande virala sjukdomar som i händelse av pandemier vilket i sin tur kan leda till lägre belastning på vården och mindre lidande för enskilda.

Ökad framkomlighet för kollektivtrafik innebär bättre arbetsmiljö för yrkeschaufförer, säkrare tidtabeller i kollektivtrafiken, minskad stress och bättre miljö.

Förbättrat underlag för stads- och detaljplanering hjälper kommuner att planera för och bygga bort sådana saker som utgör störningsmoment i trafikmiljön för en säkrare och tryggare trafikmiljö.

Genom att kommunen i realtid kan uppmärksammas på vägförhållanden och andra förhållanden som t.ex. fyllnadsgrad på offentliga soptunnor kan väghållnings- och renhållningsåtgärder vidtas mer effektivt vilket i sin tur kan leda till minskad trängsel, ökad framkomlighet samt säkrare trafikförhållanden och färre olyckor.

Uppgifter om trafikincidenter kan också medföra att problematiska trafikmiljöer identifieras och därmed kan modifieras på lämpligt för att minska riskera för olyckor i framtiden.

Inget behov av personuppgifter

De uppgifter som man är intresserade av att mäta med multisensorerna utgör inga personuppgifter. För de ändamål som ska uppnås behövs inga personuppgifter. Kamerafunktionalitet innebär emellertid att personuppgifter ändå kommer att behandlas. För att minimera konsekvenserna för enskilda förutsätter därför användningen av multisensorerna för dessa ändamål att personuppgifter gallras genom

att uppgifterna anonymiseras så snart som möjligt efter att de registrerats. I de allra flesta fall innebär det att personuppgifter lagras eller behandlas i sekunder eller kortare tid än sekunder.

Åtgärder som stärker registrerades rättigheter

Enskildas rättigheter till tillgång, rättelse, radering och att göra invändningar ska säkerställas. Med tanke på den mycket korta lagringstiden av icke-anonymiserade personuppgifter kommer rätten till tillgång till personuppgifterna sällan att kunna utövas. Det kommer inte heller inträffa att felaktig registrering av personuppgifter görs då multisensorn gör en bildupptagning av vad som registreras på platsen. Denna bildupptagning kommer i personuppgiftshänseende alltid att vara korrekt utifrån det upptagningsområde som multisensorn registrerar, om inte obehörig manipulering skett. I alla avseenden kommer personuppgifterna i de flesta fall vara gallrade genom anonymisering innan dessa rättigheter kan aktualiseras. Icke desto mindre måste den personuppgiftsansvarige ha en organisation och förmåga att ta emot och behandla begäranden och invändningar från enskilda.

Internationella överföringar

All personuppgiftsbehandling av multisensorerna ska ske i Sverige. Inga personuppgifter ska överföras till eller behandlas i något land utanför EU eller EES. Tekniska skyddsåtgärder ska implementeras så att detta inte sker.

Åtgärder för anonymisering

Det är av central betydelse för användningen av multisensorer att de personuppgifter som behandlas av multisensorerna omgående anonymiseras så att de uppgifter som behövs för att uppnå ändamålen kan användas utan risk för integritetsintrång för enskilda. När personuppgifterna har anonymiserats är det kvarstående uppgifterna inte längre att betrakta som personuppgifter.

Ett avidentifierat dataset kan dock fortfarande innebära kvarstående risker för de registrerade. Avidentifiering och re-identifiering är aktiva forskningsområden och nya upptäckter offentliggörs regelbundet, men även avidentifierade uppgifter, som t.ex. statistik, kan användas för att utöka enskilda personers befintliga profiler och därigenom skapa nya problem beträffande skyddet av personuppgifter.

Avidentifiering är därför inte en engångsåtgärd, och personuppgiftsansvariga ska regelbundet ompröva riskerna med behandlingen och inte lagra anonymiserade uppgifter längre än vad som behövs för att uppfylla ändamålen.

Riskanalys

Riskanalysen identifierar nio övergripande hot och sårbarheter som måste hanteras i varierande utsträckning: Kapning av kommunikationsprotokoll, avlyssning av kommunikation, tillgänglighetsattacker, skadlig kod eller kod som utnyttjar svagheter, obehörig fysisk modifiering, fel i system, konfiguration eller handhavande,

naturhändelser, avbrott i nätverk, anonymisering inte längre funktionell, och omfattande lagring av anonymiserade uppgifter.

Riskanalysen definierar vidare frekvensen för hur ofta dessa hot bedöms realiseras och vilka konsekvenser för enskildas fri- och rättigheter som kan uppstå samt bedömer en nivå av riskacceptans.

Riskerna kan därefter definieras genom en preciserad riskformulering baserad på hot, frekvens och konsekvens. Riskformuleringen konverteras därefter till en målformulering som anger vad som ska uppnås för att hantera risken på en övergripande nivå.

Det som bedömningar som presenteras i referenskonsekvensbedömningen är uppskattningar och den som använder underlaget för sin verksamhet och för en ansökan om kamerabevakningstillstånd är ansvarig för att bedöma om de gjorda bedömningarna är korrekta i förhållande till den aktuella verksamheten och måste göra de nödvändiga justeringar eller anpassningar som behövs för just den användning som användaren planerar.

Riskhantering

Referenskonsekvensbedömningen är inte en konsekvensbedömning för ett visst specifikt system från en viss specifik leverantör därför innehåller den inga detaljerade åtgärder för att hantera risker i förhållande till specifik utrustning utan riskerna hanteras på ett mer generellt plan.

Referenskonsekvensbedömningen identifierar nio övergripande målsättningar som multisensorsystemet ska uppnå och kan användas som stöd för att identifiera möjliga och riskreducerande åtgärder.

1. Multisensorsystemet har implementerat säkerhetsåtgärder för att snabbt upptäcka och skydda mot dataläckor och avlyssning eller avlyssningsförsök.
2. Multissensorsystemet ska vara robust mot tillgänglighetsattacker och personuppgiftsansvarig har rutiner för att snabbt återställa funktionalitet för driften av sensorsystemet.
3. Multisensorsystemet har kontinuerligt uppdaterat skydd mot skadlig kod samt kan upptäcka och spåra obehörig tillgång till och ändring av uppgifter. Informationsägaren uppdaterar omgående multisensorsystemet när säkerhetsuppdateringar ges ut. Krav ställs på att leverantören vid behov uppdaterar multisensorsystemet under hela dess förväntade livslängd.
4. Rutiner och regelbundna kontroller finns för att kontrollera multisensorernas upptagningsområde varje vardag. Rutinerna och kontrollerna säkerställer avstängning av sensorer som har felaktigt upptagningsområde till dess sensorn korrigerats.
5. Handhavandet av multisensorerna leder inte till att uppgifter hanteras eller lagras längre än vad som behövs för att lösa uppgifterna. Rutiner och

regelbundna kontroller säkerställer att informationsägaren snabbt upptäcker bildströmmar som inte anonymiserats som de ska och säkerställer att de omedelbart åtgärdas.

6. Multisensorsytemet har rimlig redundans i förhållande till risken för avbrott i elförsörjning eller kommunikation.
7. Rutiner och regelbundna kontroller finns för att kontrollera multisensorernas upptagningsområde varje vardag. Rutinen säkerställer avstängning av sensorer som har felaktigt upptagningsområde till dess sensorn korrigerats.
8. Multisensorsystemet säkerställer anonymisering av bildströmmar och andra uppgifter som produceras av systemet under hela dess livslängd. Gallringsrutiner för anonymiserade uppgifter finns.
9. Anonymiserade uppgifter lagras inte längre än vad som behövs för verksamhetens behov.

Riskreducerande åtgärder implementeras i detalj i samband med kravställning inför upphandling och användning av multisensorer för de ändamål som anges i detta dokument. Exempel på detaljerade åtgärder för att minska riskerna som anges i riskanalysen kan delas in i tre huvudkategorier.

1. Säkerhetspolicy, säkerhetspolicyn ska syfta till att göra arbetet mer konkret och åtgärderna mer robusta.
2. Organisation, personal och processmätvärden, den personuppgiftsansvariga ska ha organisatoriska kriterier för hantering av informationssäkerhet och dataskydd. Personalrutiner ska främja god säkerhet.
3. Tekniska åtgärder. För att minska sårbarheten i ett multisensorsystem ska säkerhetsåtgärder och god praxis implementeras och omfatta systemets tekniska element under hela dess livslängd.

Kvarstående risker och kontinuitetsplanering

Det går inte att bortse från att användning av multisensorer kan innebära en mycket omfattande kamerabevakning av ett stort antal allmänna platser inom tätbebyggt område och på landsbygden inom en kommun. Även om multisensorsystemet fungerar precis som det är tänkt, det vill säga inom mycket kort tid anonymiserar de uppgifter som behövs för ändamålet och information om detta finns tillgänglig för alla på ett öppet, fullständigt och transparant sätt i omedelbar och medelbar anslutning till multisensorerna. Så kan det ändå inte uteslutas att enbart förekomsten av en stor mängd kameror i den offentliga miljön kan skapa en känsla hos enskilda av att vara övervakad även om det inte orsakar någon reell eller objektiv skada.

Därför är det viktigt att användning av multisensorer för dessa ändamål endast används i enlighet med tillstånd från Integritetsskyddsmyndigheten, att den personuppgiftsansvarig är transparent, kontinuerligt ser över verksamheten samt kontrollerar att den följer de tillstånd och villkor som Integritetsskyddsmyndigheten meddelar och ser till att verksamheten kan granskas utan allvarliga anmärkningar.

Etiska överväganden

I snabbrörliga processer som kännetecknas av stark innovation, som till exempel samhällets digitalisering, är det inte sällan så att utredningar ställer frågor för första gången. Etik är en levande fråga som behöver diskuteras och analyseras som en del av utvecklingsprocesser, och framför allt, aldrig förmodas vara ”färdigutredd” – det som inte var en uppenbar etisk problematik när man formulerade ett system kan vid närmare påseende, när systemet har använts ett tag, bli framstå som ett uppenbart problem.

Om en användare avviker från det angivna ändamålet i referenskonsekvensbedömningen är det viktigt att göra en förnyad avvägning av de etiska riskerna i relation till det allmänna intresset för dessa ytterligare ändamål. Den verksamhet som en kommunal myndighet bedriver är av allmänt intresse, men ur en etisk synvinkel är det alltid önskvärt att kommunen gör en avvägning av de etiska riskerna i relation till det allmänna intresset i det enskilda fallet.

När ett multisensorsystem används och genererar data kan det leda till att nya tidigare oförutsedda användningsområden för den anonymiserade datan upptäcks och efterfrågas. Även om ett sådant nytt användningsområde principiellt inte skulle vara oförenligt med det ursprungliga ändamålet bör ändamålen med behandlingen ändå uppdateras med den nya användningen. På detta sätt beaktas dels principen om öppenhet, dels hanteras risken för ändamålsglidning.

Eftersom det finns uppenbara risker för enskildas fri- och rättigheter vid användning av multisensorer är det nödvändigt att tillämpa dataminimering, det vill säga att bara samla in, behandla, tillgängliggöra (internt och externt) samt lagra data i den mån detta tydligt behövs för att uppfylla ändamålet, och ta hänsyn till proportionalitetsprincipen. Att spara data, även om det är anonymiserat, innebär alltid en risk, som måste vägas mot värdet av att spara data. Anonymiserade videofilmer från kamerabevakning ska därför inte sparas längre än nödvändigt.

När en personuppgiftsansvarig behandlar komplex data som till exempel video (även anonymiserad video) finns en osäkerhet om vad som kan komma att utläsas ur datat. Förutsägelseanalyser ("predictive analytics") på komplext, mänskligt genererat data för att förutspå individbeteenden, framtida händelser och samhällstrender är ett växande område som kan ha implikationer för framtida demokrati och individers möjligheter att inte bli manipulerade eller ledda.

Det bör uppmärksammas om till exempel data samlas in i en viss stadsdel med vissa sociokulturella egenskaper, så måste detta faktum beaktas vid beslut baserade på denna data för en annan stadsdel som kan ha andra sociokulturella egenskaper.

Sårbara personer och grupper bör särskilt uppmärksammas och inkluderas i processen runt ändamål och metod. Detta hanteras bland annat genom tillståndsprocessen hos

Integritetsskyddsmyndigheten, där villkor och begränsningar i tillstånd också beaktar dessa aspekter.