Uppsala universitet
Inst. för informatik och media

Ljudövervakningssystem för smarta städer
Designriktlinjer i enlighet med svensk lagstiftning

Tobias Näslund Eriksson och Martin Skiöld

UPPSALA
UNIVERSITET

Kurs: Examensarbete
Nivå: C
Termin: VT-16
Datum: 160616

Abstract:

This paper investigates how audio monitoring systems should be designed, in the context of smart cities and in accordance with Swedish legislation. Audio monitoring for smart cities is promising and have previously shown great potential. However its opportunities are still relatively unexplored. ShotSpotter is one of several examples of audio monitoring in the context of smart cities. In the US only, the system has successfully been used to alert and locate shootings in over 90 cities. However, the technology is surrounded by controversies and there has been debate whether audio monitoring systems are compatible with law. Compatibility is critical since incompatibility could result in severe sanctions. Research related to this paper has been conducted according to the Design Science research strategy. The research resulted in design guidelines for audio monitoring systems, for law enforcement purposes, in accordance with Swedish law. The design guidelines are based upon existing audio monitoring systems, previous research and empirical data. The empirical data consists of 12 interviews with experts in law, phonetics and digital forensics. Additionally, the design guidelines have been evaluated by an expert in a criteria-based evaluation interview. Results of the research shows that it is, in fact, possible to design audio monitoring systems, in the context of smart cities, in accordance with Swedish legislation. The design guidelines can be applied in the development of audio monitoring systems with law enforcement purposes. With some modification, they can also be used for audio monitoring systems with other purposes.

Keywords:

Audio Monitoring Systems, Intelligent Acoustics, Acoustic Sensing, Smart Cities, Internet of Things, Privacy by Design, Design Guidelines, ShotSpotter, EAR-IT, IT law, Legal Conditions, Legal Compliance

Sammanfattning:

Uppsatsen syftar till att undersöka hur ljudövervakningssystem inom ramen för smarta städer-konceptet bör utformas i enlighet med svensk lagstiftning. Ljudövervakning för smarta städer har visat på stor potential och ännu är dess möjligheter outforskade. ShotSpotter är ett av flera exempel på ljudövervakning inom ramen för smarta städer. Systemet har med framgång använts för att uppmärksamma och lokalisera skottlossningar i över 90 amerikanska städer. Det råder dock debatt huruvida ljudövervakningssystemet är kompatibelt med lagstiftning. Denna kompatibilitet är kritisk då det motsatta kan resultera i stränga påföljder och därmed utgöra direkta hinder för implementation. Forskning i relation till uppsatsen har genomförts inom ramen för forskningsstrategin Design Science. Forskningsprocessen har mynnat ut i designriktlinjer för hur ett ljudövervakningssystem med brottsbekämpande syfte bör utformas i enlighet med svensk lagstiftning. Designriktlinjerna baseras på befintliga ljudövervakningssystem, tidigare forskning och omfattande empiriskt underlag. Det empiriska underlaget utgörs av 12 intervjuer med olika typer av experter inom juridik, fonetik och IT-forensik. Designriktlinjerna har med framgång utvärderats i en kriteriebaserad expertintervju. Av forskningsresultatet att döma är det möjligt att utforma ljudövervakningssystem för smarta städer i enlighet med svensk lagstiftning. De framtagna designriktlinjerna kan användas vid utveckling av ljudövervakningssystem med brottsbekämpande syfte. Med viss modifikation kan de även användas för ljudövervakningssystem med andra syften.

Nyckelord:

Ljudövervakningssystem, Intelligent Acoustics, Acoustic Sensing, Smarta Städer, Internet of Things, Inbyggd Integritet, Privacy by design, Designriktlinjer, ShotSpotter, EAR-IT, IT-rätt, Juridiska förutsättningar, Legal Compliance

Innehållsförteckning

Begreppslista

Nedan definieras relevanta begrepp som används i uppsatsen.

Smarta städer

Det finns många olika definitioner av begreppet smarta städer. Ordet "smart" byts i vissa definitioner ut mot "intelligent" eller "digital". Detta i kombination med att termerna inte alltid används konsekvent resulterar i att begreppet "smarta städer" kan uppfattas som diffust. (Albino, Berardi & Dangelico, 2015) I denna uppsats avser begreppet "smart stad" en högteknologisk stad som förenar människor, information och stadselement med hjälp av ny teknologi i syfte att bidra till, bland annat, förbättrad livskvalitet. (Bakici Almirall & Wareham, 2013)

Personlig integritet

Begreppet personlig integritet saknar i svensk rätt en allmängiltig definition vilket resulterar i att begreppet beskrivs på olika sätt i olika sammanhang. Ett sätt att rama in innebörden av begreppet är att utgå ifrån de handlingar som utgör kränkning av den personliga integriteten. Genom att anpassa sig efter dessa kan kränkning av den personliga integriteten undvikas. (SOU 2015:31) Det finns dock beskrivningar av begreppet personlig integritet som kan ses som definitioner. I en utredning från Statens offentliga utredningar har integritetsbegreppet varit att "anses som liktydigt med den enskildes anspråk att information om hans privata angelägenheter inte skall vara tillgänglig för eller få begagnas av utomstående utan hans vilja". (SOU 1970:85) Därutöver kan den personliga integriteten delas upp i två delar. Den personliga integriteten i fysisk mening, det vill säga skyddet för den personliga friheten och rörelsefriheten, och den personliga integriteten i ideell mening, det vill säga skyddet för privatlivet och personligheten. Framöver, i uppsatsen, avser begreppet personlig integritet den personliga integriteten i ideell mening. (SOU 2015:31)

Privatliv

Begreppet privatliv har liksom personlig integritet inte en allmängiltig definition men det har gjorts försök att konkretisera begreppets innebörd. Rätten till privatliv kan ses som individens rätt till en tillvaro i avskildhet och anonymitet (Helmius, 2000, s. 99). Ett intrång i privatlivet är enligt Winfield (citerad av Helmius, 2000, s. 100) "the unauthorised interference with anothers' seclusion of himself, his family or his property from the public". Som det går att utläsa ovan talas det om privatliv som en rättighet, en rätt till ett liv utan otillåten inblandning i avskildhet och tillvaro.

Internet of Things

Begreppet och konceptet Internet of Things, IoT, är under utveckling och har således inte heller en definitiv definition. Kevin Ashton var den första som föreslog konceptet Internet of Things och beskrev det som unikt identifierbara och samverkande anslutna objekt med teknik för radiofrekvensidentifiering, RFID. (Li, Xu, & Zhao, 2014) Internet of Things kan även

beskrivas som en vision om framtidens internet där anslutna fysiska saker utgör en aktiv del av internet och utbyter information om sig själva och sin omgivning. Detta ger direkt tillgång till information om den fysiska världen och dess objekt som leder till innovativa tjänster samt ökad effektivitet och produktivitet. (Bandyopadhyay & Sen, 2011)

Inbyggd integritet

Begreppet inbyggd integritet, på engelska "privacy by design", innebär att integritetsaspekter tas i beaktande i samtliga faser av ett systems livscykel, det vill säga från förstudie, kravställning, design och utveckling till användning och avveckling. Vid användning av principer för inbyggd integritet låter man således integritetsfrågor påverka systemets hela livscykel. (Datainspektionen, u.å.-a)

Offentlig plats och allmän plats

Enligt nationalencyklopedin är offentlig plats en plats som är upplåten och tillgänglig för allmänheten. Sådana exempel är allmän väg, gata, torg och park. Offentlig plats kan även avse utrymmen inomhus och platser avsedda för allmän trafik och gångtrafik. (NE, u.å.)

I uppsatsen används begreppen offentlig plats och allmän plats synonymt.

Ljudövervakningssystem

Ett konventionellt begrepp saknas för det vi beskriver som ljudövervakningssystem i uppsatsen. Ståhlbröst, Padyab, Sällström och Hollos (2015) beskriver ett sådant system i ord som "audio monitoring", "intelligent acoustics", "acoustic sensing" och "smart city solution". Dessa ord används även av projektkoordinatorn för det forskningsprojekt som Ståhlbröst et al. (2015) deltar i (Maló, 2014, 29 oktober). Ljudövervakningssystem kommer framöver, i uppsatsen, att avse ett informationssystem som syftar till att övervaka och uppmärksamma anmärkningsvärda ljud på allmänna platser inom ramen för smarta städer-konceptet.

Fonetik

Vetenskap där människans tal studeras. Inom fonetik analyseras talljud antingen med hjälp av hörsel eller instrument. (Lindblom, u.å.)

IT-forensik

Kortfattat innebär IT-forensik att eftersöka och säkra bevis ur digitala källor genom att undersöka och/eller återskapa digital information. (Carrier, 2003)

1. Inledning

I detta avsnitt presenteras bakgrund till forskningsarbetet. Forskningsarbetets aktualitet och relevans redogörs för. Detta följs av en problemformulering och det syfte som ligger till grund för forskningsarbetet. Därefter presenteras forskningsarbetets avgränsningar. Avslutningsvis redogörs för uppsatsens kunskapsintressenter och disposition.

1.1 Bakgrund

Runt om i världen ökar urbaniseringen i hög takt. Det hävdas numera att hälften av världens befolkning lever i städer. Ökningen ställer högre krav på städer när det kommer till områden som energiförsörjning, avfallshantering, transport, miljöfrågor och säkerhet. Den här uppsatsen fokuserar på IT-lösningar relaterat till det sistnämnda. För att möta de nya krav som ställs på städer har ett koncept känt som smarta städer utvecklats. (Ståhlbröst et. al, 2015) Ett gemensamt drag för smarta städer är att de använder sig av olika typer av IT-lösningar för att höja medborgarnas livskvalitet (Ståhlbröst, Sällström & Hollosi, 2014).

Två exempel på IT-lösningar som syftar till att höja medborgarnas livskvalitet är ShotSpotter (avsnitt 3.2.1) och experiment i forskningsprojektet EAR-IT (avsnitt 3.2.2). Dessa är även exempel på hur övervakning av ljud kan användas inom ramen för smarta städer.

EAR-IT var ett EU-finansierat forskningsprojekt som genomfördes mellan 2012 och 2014. I forskningsprojektet användes en kombination av ljudövervakning och Internet of Things-teknologi, i både inomhus- och utomhusmiljöer, för att utföra storskaliga experiment i verkliga situationer. (Ståhlbröst et al., 2015) Experiment i utemiljöer fokuserade på tillämpningsområden såsom trafikuppskattning och detektering av anmärkningsvärda händelser i städer, exempelvis sirener och olyckor. Projektkoordinatorn för EAR-IT menar att ljudrelaterade lösningar är lovande och har stor potential. (Maló, 2014, 29 oktober) Ytterligare potentiella tillämpningsområden är uppmärksammande av nödsituationer, exempelvis skrik och skottlossningar. (European Commission, 2015)

En IT-lösning med sådan tillämpning har sedan en längre tid tillbaka använts i USA. IT-lösningen går under namnet ShotSpotter och kan liknas vid ett ljudövervakningssystem med brottsbekämpande syfte, inom ramen för smarta städer-konceptet. ShotSpotter lanserades som ett pilotprojekt redan 1997 i Redwood City, USA, och har sedan dess vuxit stadigt. Numera finns systemet installerat i mer än 90 amerikanska städer, däribland New York, Miami, Boston och San Francisco. (ShotSpotter, u.å.-a, ShotSpotter, 2015, ShotSpotter, u.å.-c) ShotSpotter är återkommande uppmärksammat i media, där det visat sig att det finns en debatt huruvida systemet verkligen respekterar de bestämmelser och rättigheter som återfinns i amerikansk lagstiftning. (Gold, 2015, 17 juli, Goode, 2012, 28 Maj, CBS Denver, 2016)

Frågan angående ShotSpotters juridiska kompatibilitet är således högaktuell och samma problematik skulle även kunna gälla för liknande ljudövervakningssystem inom ramen för smarta städer i Sverige.

1.2 Problemformulering och kunskapsbehov

Enligt Ståhlbröst et al. (2014) är forskning angående ljudövervakning ännu i sin linda. En av de utmaningar som kan identifieras är hur teknologin bör utformas för att vara kompatibel med lagstiftning. Massey, Otto, Hayward och Antón (2010) menar att det är en utmaning att ta fram systemkrav som är kompatibla med lagar och att bristande kunskap för juridiska aspekter kan resultera i kompatibilitetsproblem. Kompatibilitet med lagstiftning är i sin tur kritisk för system då inkompatibilitet kan medföra finansiella och straffrättsliga påföljder (Otto & Antón, 2007).

Ziegler (2014) påstår att ljudövervakning, ämnad för smarta städer, kan göra intrång i de rättigheter som tillhandahålls av lagar som syftar till att skydda privatlivet. Stor vikt måste därför läggas vid att motverka sådana intrång. Detta påstående stöds även av Finch och Tene (2015) som menar att ny teknologi inom konceptet smarta städer kan leda till nya risker när det kommer till människors privatliv.

Little, Briggs och Coventry (2005) menar att skydd för privatlivet är en viktig aspekt och bör utgöra en central del i designprocessen. För att beakta privatliv i designprocessen har Ståhlbröst et al. (2015) föreslagit designprinciper för system ämnade för smarta städer. Dessa designprinciper är enbart konstruerade utifrån ett moraliskt perspektiv och tar således inte hänsyn till juridiska förutsättningar. Ståhlbröst et al. (2015) hävdar därutöver att det tidigare gjorts försök att ta fram principer för inbyggd integritet, både utifrån ett moraliskt och juridiskt perspektiv. Exempel på ett sådant försök, som inte nämns av Ståhlbröst et al. (2015), är Datainspektionens checklista för inbyggd integritet i IT-projekt. Checklistan syftar till att förbättra möjligheterna till juridisk kompatibilitet genom inbyggd integritet (Datainspektionen, u.å.-a). Ståhlbröst et al. (2015) hävdar dock att sådana typer av traditionella principer för inbyggd integritet inte är tillämpliga för smarta städer. Detta motiveras med att designprinciperna inte kan appliceras på lösningar där människor inte använder teknologin utan endast utsätts för den.

Följaktligen framgår det av tidigare forskning och vägledande dokument att skydd för privatliv ofta är i fokus när det kommer till juridisk kompatibel design. (Ziegler, 2014, Datainspektionen, u.å.-a) Med anledning av detta anser vi att det finns ett kunskapsbehov för hur ljudövervakningssystem för smarta städer bör utformas i enlighet med lagstiftning, och då inte enbart i enlighet med lagstiftning som syftar till att skydda privatlivet utan även med lagstiftning inom andra rättsområden. Detta för att undvika oönskade påföljder liknande de som beskrivits tidigare i delavsnittet.

1.3 Syfte och forskningsfråga

Det bakomliggande motivet till forskningsarbetet är att ge upphov till vägledande information som kan vara till nytta vid utveckling av ljudövervakningssystem genom att skapa förståelse för de juridiska förutsättningar som gäller för sådana system i Sverige.

Syftet med forskningsarbetet är att ta fram riktlinjer för hur man bör utforma ljudövervakningssystem så att de är kompatibla med rådande svensk lagstiftning.

Den frågeställning som legat till grund för forskningsarbetet är:

- Hur bör ljudövervakningssystem, ämnade för allmänna platser, utformas för att vara i enlighet med rådande svensk lagstiftning?

1.4 Avgränsningar

Forskningsarbetet avgränsas till rådande svensk lagstiftning. Lagstiftning som i nuläget inte tillämpas i Sverige kommer således inte tas i beaktande. Exempel på sådan lagstiftning är de nya regler för personuppgiftsbehandling som träder i kraft 2018, i och med EU:s nya dataskyddsförordning (Datainspektionen, 2016). Utöver avgränsning till rådande svensk lagstiftning avgränsas forskningsarbetet till undersökning av sådana ljudövervakningssystem som endast är ämnade för allmänna platser och har brottsbekämpande syfte.

1.5 Kunskapsintressenter

Denna uppsats riktar sig till framtida utvecklare av ljudövervakningssystem. Den preskriptiva kunskap som förmedlas kan vara av intresse för de som är intresserade för hur integritetsfrågor kan tas i beaktande vid utformning av ljudövervakningssystem. De som vill bedriva vidare forskning eller experiment inom området bör undersöka de juridiska förutsättningar som förmedlas i uppsatsen. Avslutningsvis är uppsatsen intressant för de som undrar hur designriktlinjer kan tas fram och utvärderas på ett metodiskt sätt utifrån tidigare forskning.

1.6 Disposition

Denna uppsats är indelad i sju avsnitt. Inledning (1), Metod (2), Kunskapsinventering (3), Identifiering av juridiska förutsättningar (4), Designriktlinjer (5), Utvärdering och diskussion (6) och Slutsats och reflektion (7). Därutöver återfinns fyra bilagor. Bilagorna innehåller hypotetiska designalternativ för ljudövervakningssystem (bilaga 1), intervjuguide (bilaga 2), temaindelning (bilaga 3) och utvärderingsplan (bilaga 4). Nedan beskrivs uppsatsens sju avsnitt kortfattat:

1. I det inledande avsnittet behandlas bakgrund, problem, syfte, avgränsningar och kunskapsintressenter till ämnesområdet.

2. I det andra avsnittet behandlas forskningsprocessens metodik. Forskningsstrategi, forskningsparadigm och metoder för datainsamling, dataanalys, framställning och utvärdering av designriktlinjer redogörs för.

3. I det tredje avsnittet presenteras en kunskapsinventering på ämnesområdet. Kunskapsinventeringen ligger till grund för de resonemang som framförs vid analys av det empiriska underlaget och vid motivering och diskussion av de framtagna designriktlinjerna.

4. I det fjärde avsnittet presenteras och motiveras de juridiska förutsättningar som ställer krav på utformningen av ett ljudövervakningssystem och som ligger till grund för designriktlinjernas rekommendationer. I avsnittet presenteras även det empiriska underlag, som ligger till grund för de identifierade juridiska förutsättningarna, och vilka informanter som deltagit i datainsamlingen.

5. I det femte avsnittet presenteras och motiveras de slutgiltiga designriktlinjerna som syftar till att tillfredsställa de juridiska förutsättningar som identifierats.

6. I det sjätte avsnittet presenteras resultatet av utvärderingen. I avsnittet diskuteras även de slutgiltiga designriktlinjerna i förhållande till tidigare forskning.

7. I det sjunde avsnittet återkopplas forskningsarbetets resultat med den frågeställning som legat till grund för forskningsarbetet. Därutöver förs en diskussion och reflektion av forskningsprocessen samt förslag på framtida forskning.

2. Metod

I detta avsnitt presenteras forskningsansats, forskningsstrategi, forskningsparadigm och ingående beskrivning av metodval och tillvägagångssätt.

2.1 Forskningsansats

Forskning i relation till uppsatsen har bedrivits i enlighet med forskningsstrategin Design & Creation i Oates (2006, s. 108), traditionellt benämnt Design Science. Val av forskningsstrategi motiveras med att frågeställningen lämpligast besvaras genom utveckling av en IT-artefakt. IT-artefakten utgörs i vårt fall av designriktlinjer. Designriktlinjer kan klassificeras som en *modell* i enlighet med Hevners, Marchs, Parks och Rams (2004) beskrivning av IT-artefakter. De utgör preskriptiv kunskap som möjliggör för utvecklare att förstå och åtgärda vissa typer av problem som infinner sig vid utformning av ljudövervakningssystem i framtiden (Hevner et al., 2004).

Forskningsarbetet har genomförts inom ramen för det interpretivistiska forskningsparadigmet. Det är i forskningsarbetet svårt att bevisa eller motbevisa en hypotes, varför ett positivistiskt synsätt inte är lämpligt. Det interpretivistiska synsättet är lämpligare då lagstiftning och lagtolkning spelar en betydande roll för hur ljudövervakningssystem kan utformas. Subjektiviteten vid lagtolkning kräver ett interpretivistiskt synsätt då ingen utgång kan förutsägas med definitiv säkerhet. Detta innebär att de slutgiltiga riktlinjerna ska ses som en potentiell och ej definitiv lösning på problematiken ur vår synvinkel, baserat på det empiriska material och expertis vi haft tillgång till. Det är viktigt att poängtera att rättsläget och designriktlinjernas juridiska kompatibilitet kan bedömas på olika sätt av olika personer. För att interpretivistisk forskning ska betraktas som värdefull krävs att god kvalitet eftersträvas i forskningsprocessen. Vi har därför tagit i beaktande kvalitetsaspekter såsom trovärdighet, spårbarhet och vidareförbarhet. Trovärdighet har eftersträvats genom utförlig och noggrann datainsamling tillsammans med koppling mellan framtagna designriktlinjer och tidigare forskning. Spårbarhet har eftersträvats genom att tydliggöra kopplingen mellan designriktlinjer och det empiriska och teoretiska underlaget. Vidareförbarhet har eftersträvats genom att tydliggöra designriktlinjernas relevans och generaliserbarhet. För att göra riktlinjerna generaliserbara har utförlig bakgrundsinformation lagts till i varje riktlinje. På så sätt kan designriktlinjerna anpassas till andra situationer i och med att det är möjligt att förstå och förutsäga effekterna av en förändring i sammanhanget eller efterföljandet av designriktlinjerna. (Oates, 2006)

Forskningsarbetet har utförts i samtliga typiska steg för Design & Creation (Oates, 2006, s. 111). Hur dessa steg efterföljts i forskningsprocessen sammanfattas i följande lista och i figur 1.

1. *Awareness*
   Hevner et al. (2004) anser att det för forskningsarbete inom ramen för Design Science är viktigt att utveckla IT-artefakter som faktiskt löser relevanta problem. I detta steg undersöktes därför olika tillämpningsområden för ljudövervakningssystem och huruvida dessa är lösningar på relevanta problem. Därutöver undersöktes ifall det finns ett behov av designriktlinjer för ljudövervakningssystem i enlighet med lagstiftning. Ovanstående undersöktes genom att studera nyhetsartiklar och tidigare forskning på ämnet. (Avsnitt 1.1 och 1.2)

I detta steg undersöktes även de juridiska förutsättningar som ställer krav på utformningen av ljudövervakningssystem. Vi identifierade de juridiska förutsättningarna genom scenariobaserade intervjuer där scenarion utgjordes av olika hypotetiska designalternativ för ljudövervakningssystem. Awareness-steget resulterade således i större delar av forskningsarbetets empiriska underlag (avsnitt 4.2).

2. *Suggestion*
   Detta steg utfördes iterativt ihop med awareness-steget. Intervjuguiden (bilaga 2) förfinades och de hypotetiska designalternativen för ljudövervakningssystem, som i intervjuerna användes för att extrahera juridiska förutsättningar och skiljelinjer, togs fram utifrån det som framkommit i samband med tidigare intervjuer och forskning (avsnitt 3). Genom att låta jurister bedöma olika designalternativ blev gränsen för vad som är lagligt och olagligt tydliggjort. Designalternativen dokumenterades i journal och presenteras i bilaga 1.

3. *Development*
   I detta steg utgick vi ifrån de juridiska förutsättningar som erhållits i föregående steg. De juridiska förutsättningarna tillsammans med empiriskt och teoretiskt underlag låg till grund för de rekommendationer som togs fram (avsnitt 5.3). Sammanställningen av de juridiska förutsättningarna och rekommendationerna resulterade avslutningsvis i designriktlinjer (avsnitt 5.2).

4. *Evaluation*
   I detta steg planerades och utfördes en utvärdering av designriktlinjerna. Utvärderingen genomfördes som en kriteriebaserad utvärderingsintervju med en ämnesexpert. Resultatet från utvärderingen kompletterade det ursprungliga empiriska underlaget och innebar ett par mindre anmärkningsvärda åtgärder (avsnitt 6.1).

5. *Conclusion*
   I det sista steget drogs slutsatser utifrån de slutgiltiga designriktlinjerna, utvärderingen och insikter som framkommit under forskningsprocessen (avsnitt 6.2 och 6.3).

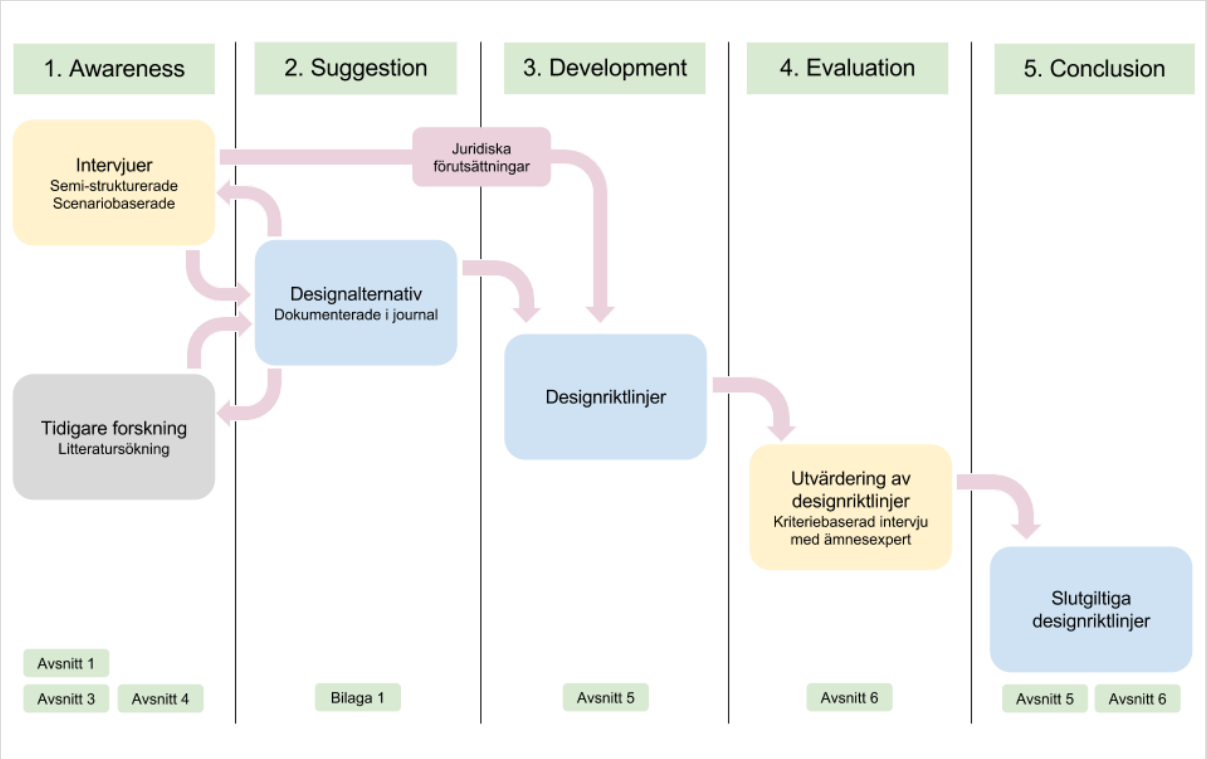

Fig 1. Illustrerad forskningsprocess. Forskningsprocessen beskrivs i ovanstående lista.

2.2 Metodik för datainsamling

Inom Design & Creation ingår oftast någon eller några av följande fyra datainsamlingsmetoder: Intervjuer, observationer, dokumentanalys och/eller enkäter (Oates, 2006 s. 117). Den datainsamlingsmetod som varit aktuell för detta forskningsarbete är intervjuer.

Intervjuer har använts som datainsamlingsmetod för att erhålla en djupare förståelse för de juridiska aspekter som påverkar utformningen av ett ljudövervakningssystem. Det är otillräckligt att enbart läsa lagar, inom ramen för dokumentanalys, eftersom juridiska problem är svåra att avgöra med definitiv säkerhet utifrån lagtext. Bristande förkunskaper inom svensk lagstiftning har inneburit att datainsamlingen varit av explorativ natur. Intervjuerna har, på förhand, varit bestämda enligt en intervjuguide. Intervjuguidens innehåll har i och med intervjuprocessens explorativa karaktär förändrats inför de flesta intervjuer, i takt med att nya intressanta frågor och rättsområden dykt upp. Gemensamt för de olika versionerna av intervjuguiden är att de innehållit en beskrivning av premisserna för intervjun, en introduktion till ämnet, de hypotetiska designalternativen och relaterade juridiska frågor. De hypotetiska designalternativen (bilaga 1) har i intervjuerna presenterats som scenarion. Intervjuerna har därmed varit scenariobaserade eftersom detta hjälpt att identifiera de juridiska skiljelinjerna för olika designalternativ. Det bidrog även med att vi kunde ställa konkreta frågor och måla upp en konkret bild av något så diffust som ljudövervakningssystem. För att ytterligare öka intervjuobjektens förståelse av ljudövervakningssystem skickades i förväg en avskalad variant av intervjuguiden till intervjuobjekten. (Oates, 2006)

Vid val av intervjutyp vägdes behovet av flexibilitet mot behovet av att frågorna, som är relaterade till de hypotetiska designalternativen, beskrivs och besvaras i rätt ordning. Detta resulterade i att semi-strukturerade intervjuer valdes. (Oates, 2006, s. 188)

Vi har vid val av intervjuobjekt eftersträvat stor spridning gällande expertis. Intervjuerna har främst genomförts med personer med god kännedom inom juridik, men även med personer med god kännedom inom röstidentifikation och ljud i övrigt. Intervjuerna har vid möjlighet genomförts på plats och i annat fall via telefon och mejl. För att kunna lägga fokus på samtalet i intervjuerna spelades intervjuerna in. Detta medförde att vi under intervjuerna kunde fokusera på att ställa givande följdfrågor snarare än att anteckna.

2.3 Metodik för dataanalys

I forskningsarbetet har den insamlade datan analyserats kvalitativt eftersom en kvalitativ dataanalys ansågs lämpligare än en kvantitativ dataanalys, då djup förståelse och kunskap om befintliga regelverk eftersträvats. Datan har därutöver analyserats induktivt då dataanalysen inte tagit utgångspunkt i en förbestämd teori. (Oates, 2006, s. 269)

Inför dataanalysen förbereddes den insamlade datan till en form lämplig för dataanalys. Detta genom att transkribera de intervjuer som genomförts på plats och via telefon så att all insamlad data återfanns i textform. För dataanalysen användes den metod för kvalitativ dataanalys som framförts av Oates (2006 s. 268). Inledningsvis lästes samtlig data för att få ett helhetsintryck. Därefter segmenterades datan i tre olika typer av segment:

1. Segment som inte är relaterade till forskningssyftet, och därmed inte behövs.
2. Segment som innehåller data som kan hjälpa till att beskriva forskningskontexten för läsarna. Exempelvis data som beskriver historia, befattning, bakgrund och företag.
3. Segment som är relevanta för forskningsfrågeställningen.

En tematisk kodning genomfördes på segmenten i den tredje punkten. Gemensamma nämnare i datan eftersöktes och beskrevs kort och koncist som teman. De teman som växt fram under analysen presenteras i bilaga 3. Genom den tematiska kodningen kunde text som hörde ihop med varandra, inom och mellan olika intervjuer, identifieras och jämföras.

För att öka dataanalysens trovärdighet och minska dataanalysens subjektivitet utfördes den inledningsvis separat av var forskare för sig. Därefter sammanställdes de resulterande två analyserna och tvetydigheter och oklarheter diskuterades.

Slutligen sammanställdes all data, per tema, i ett dokument. Det framgick i detta dokument vilken informant som sagt vad, inom varje tema. Detta dokument gav en god inblick i de olika informanternas synsätt, samt vilka problem de ansåg var relevanta.

2.4 Metodik för utvärdering

Venable, Pries-Heje och Baskerville (2014) har utvecklat, tydliggjort och framfört bevis för ett ramverk för utvärdering inom Design Science. Ramverket handlar i stort om att vägleda forskare inom Design Science att ta fram en strategi för utvärdering av de artefakter som skapas av forskningen. Denna strategi tar följande faktorer i beaktande: varför, när, hur och vad som bör utvärderas.

Utifrån Venables et al. (2014) ramverk valdes en utvärderingsstrategi. Den valda utvärderingsstrategin kretsade kring formativa och summativa artificiella utvärderingar. Artificiella utvärderingar karaktäriseras av att artefakten utvärderas utan att instansieras. Denna typ av utvärdering anses oftast vara enklast och minst kostsam, men samtidigt orealistisk eftersom den inte tar hänsyn till de riktiga användarna och problemen.

Utvärdering har i forskningsarbetet skett med fokus på två egenskaper hos artefakten: tillförlitlighet och fullständighet. Anledningen till att vi valt tillförlitlighet som egenskap för utvärdering är att Nowack (1997, s. 48) påpekar dess relevans i förhållande till designriktlinjer. Det framkommer att det är viktigt för en designer att känna till tillförlitligheten av ett förväntat utfall då kunskap, i vårt fall designriktlinjerna, konsumeras. Annars finns risken att design blir felaktig. Det är alltså viktigt att se till att konsumtion av designriktlinjerna faktiskt leder till en design som är kompatibel med svensk lagstiftning. Utöver tillförlitlighet menar Nowack (1997, s. 47) att kunskap kan vara subjektiv och härstamma från personliga erfarenheter. Ur detta härleder Nowack (1997) att kunskap kan leda till att viktiga problem förbises. Det är därför viktigt att kunskapen är fullständig och täcker all problematik (Nowack, 1997).

I utvärderingsstrategin begränsades antalet utvärderingsepisoder till en, med tanke på forskningsarbetets korta tidsram. Detta kan anses vara mindre pålitligt, då artefakten inte utsätts för flera utvärderingar. Därmed bör läsare ha i åtanke att utvärderingens pålitlighet kan ifrågasättas.

Den valda utvärderingsstrategin innebär att artificiella utvärderingar bör genomföras. Venable et al. (2014) menar att dessa kan genomföras som en kriteriebaserad utvärdering. Cronholm och Goldkuhl (2003) beskriver vidare hur en sådan bör genomföras. Vi har i utvärderingen följt Cronholms et al. (2003) metod för kriteriebaserad utvärdering av IT-artefakter. Detta har inneburit att utvärderingen planerats och mynnat ut i en utvärderingsplan (bilaga 4). I utvärderingsplanen beskrivs utvärderingens tillvägagångssätt samt vilka kriterier som är föremål för utvärderingen. Utvärderingens tillvägagångssätt, kriteriebaserad utvärderingsintervju med ämnesexpert, ligger i linje med Cronholm et al. (2003) uppräkning av möjliga tillvägagångssätt för kritieriebaserade utvärderingar. Att utvärderingen genomförts som en intervju innebar att fokus i intervjun lagts på vissa av artefaktens kvaliteter. Den slutgiltiga utvärderingsintervjun utformades så att ämnesexperten höll sig till de två utvärderingskriterierna tillförlitlighet och fullständighet. Vi beskrev i utvärderingsplanen indikationer på tillförlitlighet och fullständighet. Detta användes senare i utvärderingsintervjun för att ta ställning till ifall artefakten uppfyller kriterierna eller inte.

2.5 Metodik för framställning av riktlinjer

Det är i tidigare forskning dåligt belyst hur man bör gå tillväga för att ta fram riktlinjer. Det saknas således riktlinjer för att ta fram riktlinjer. Det finns däremot en samling definitioner att utgå ifrån som stöd. Fu, Yang och Wood (2015) har efter undersökning av diverse definitioner av designriktlinjer kommit fram till följande:

> *"A context-dependent directive, based on extensive experience and/or empirical evidence, which provides design process direction to increase the chance of reaching a successful solution."* (Fu et. al, 2015, s. 3)

En av de undersökta definitionerna är Nowacks (1997) definition av designriktlinjer. Nowack (1997) definierar designriktlinjer mer specifikt och beskriver däribland dess uppbyggnad. Nowack (1997, s. 62) beskriver designriktlinjer som preskriptiva rekommendationer för handlingar beroende av en viss kontext och som adresserar ett designproblem. En designriktlinje består av fyra delar:

1. Problem som adresseras
2. Samband med designkontext
3. Rekommendationer
4. Anledning

Utifrån ovanstående beskrivning tog vi fram en metod för hur designriktlinjer kan framställas. Initialt identifieras juridiska förutsättningar (avsnitt 4.3.2), i vårt fall utifrån intervjudata. Därefter eftersöks rekommendationer som tillfredsställer de identifierade juridiska förutsättningarna (avsnitt 5.3). Detta sammanställs sedan som riktlinjer (avsnitt 5.2) tillsammans med bakgrundsinformation. Bakgrundsinformation inkluderas i riktlinjerna för att öka riktlinjernas generaliserbarhet. På så sätt kan riktlinjerna anpassas till andra designsituationer och ett förändrat juridiskt landskap. Således framgår det vilka lagar som förbises om vissa riktlinjer inte efterföljs och vice versa. Den tillhörande bakgrundsinformationen gör det möjligt att spåra vilka bestämmelser som gäller för vilka riktlinjer och hur riktlinjerna förhåller sig till dessa. Anledningen till att vi explicerar kopplingen mellan riktlinjer och bestämmelser är att Becker, Heddier, Braeuer och Knackstedt (2014) föreslår detta i sin forskning om hur man bör integrera juridiska krav i informationssystemsdesign.

3. Kunskapsinventering

I detta avsnitt presenteras forskningsarbetets kunskapsinventering. Kunskapsinventeringen innehåller beskrivningar av befintliga ljudövervakningssystem samt principer för hur informationssystem ska utformas i enlighet med lagstiftning och som skyddar den personliga integriteten. Avslutningsvis presenteras den lagstiftning som berörts i forskningsarbetet.

3.1 Introduktion till kunskapsinventering

Tidigare forskning, beträffande ljudövervakningssystem, kretsar kring ett EU-finansierat forskningsprojekt, vid namn EAR-IT. Kortfattat berör forskningsprojektet ljudövervakning inom ramen för smarta städer. Utöver EAR-IT, finns på området ett befintligt ljudövervakningssystem kallat ShotSpotter. Dessa två ljudövervakningssystem har delvis inspirerat designriktlinjernas rekommendationer.

Tidigare forskning med avseende på hur man bör utforma informationssystem i överensstämmelse med lagstiftning omfattas, i stort, av principer och checklistor för hur man bör ta integritetsfrågor i beaktande under systemets livscykel, så kallad inbyggd integritet (Ståhlbröst et al., 2015). Förutom Ståhlbrösts et al. (2015) designprinciper återfinns i tidigare forskning ett flertal principer för inbyggd integritet. Dessa är dock inte avsedda för just ljudövervakning i smarta städer. Majoriteten av principerna är dessutom uppbyggda utifrån ett moraliskt perspektiv och tar således inte hänsyn till juridiska förutsättningar. I kommande delavsnitt kommer tre olika principer för inbyggd integritet presenteras. Två principer utifrån ett juridiskt perspektiv, Langheinrich (2001) och Datainspektionen (u.å.-a), samt en utifrån ett moraliskt perspektiv, Ståhlbröst et al. (2015). Speciellt Ståhlbröst et al. (2015) designprinciper har stor betydelse för framställandet av designriktlinjerna. Övriga två principer tas med i kunskapsinventeringen då brister i dessa identifierats i och med forskningsarbetets resultat (avsnitt 6.3).

3.2 Tidigare ljudövervakningssystem

Element hos tidigare ljudövervakningssystem har kommit att inspirera de riktlinjer som tagits fram. Nedan presenteras och beskrivs dessa två befintliga ljudövervakningssystem i detalj.

3.2.1 ShotSpotter

ShotSpotter påstår sig inneha teknologi som är först av sin sort. ShotSpotter är ett system skapat för att upptäcka, lokalisera, larma och analysera skottlossningar. Det är uppbyggt av geografiskt utspridda sensorer som tillsammans triangulerar och larmar brottsbekämpande organisationer i realtid när skottlossning pågår. ShotSpotter hävdar att deras sensorer endast avlöses vid explosiva och impulsiva ljud och att domstolar, i USA, tidigare kommit fram till att samtal som avlyssnas på allmänna platser inte räknas som ett integritetsintrång i juridisk mening. Detta då det inte går att förvänta sig sekretess i dessa miljöer. De påstår även att systemet är konstruerat så att realtidsavlyssning förhindras och att människoröster inte avlöser sensorerna. De hävdar att utav 3 miljoner incidenter har det endast rapporterats om 3 ljudklipp innehållandes mänskliga röster. De påstår även att någon privat konversation aldrig hörts. För att undvika att mänskliga röster samlas in av systemet har man placerat sensorerna på en höjd

mellan 6 till 30 meter från marken, oftast på hustak eller gatubelysning. (ShotSpotter, u.å.-c, ShotSpotter, u.å.-d, ShotSpotter, u.å.-e)

Om sensorerna avlöses av ett impulsivt ljud skickas sammanfattande data angående händelsen (t.ex. amplitud och position), men inte ljudupptagning i sig, till experter på en av ShotSpotters kontrollcentraler. Datan bedöms av experterna, vars uppgift är att validera larmet. Om fler än en sensor avlösts initierar systemet en triangulering där positionen för skottlossningen fastställs. Mottagen data lagras därefter i en centraliserad databas. På datan tillämpas artificiell intelligens och statistiska metoder för att identifiera vad för typ av ljud det är som mottagits. Om data för ljudets karaktär stämmer väl överens med ett skott skickar sensorerna en kort ljudinspelning till kontrollcentralen som därefter bedömer ljudet. Om denna korta ljudinspelning aldrig begärs från sensorn skrivs ljuddatan över i minnet och förloras permanent. I de fall där ljudet, av experter, bedömts vara en skottlossning larmas brottsbekämpande organisationer. Larm skickas då till den brottsbekämpande organisationens utryckningsenhet och larmen visas som en punkt på en karta tillsammans med ytterligare information. Data skickas till alla enheter som är kopplade till systemet. (ShotSpotter, u.å., ShotSpotter, u.å.-d, ShotSpotter, u.å.-e)

3.2.2 EAR-IT

EAR-IT var ett EU-finansierat forskningsprojekt som utfördes mellan 2012 och 2014. Projektet fokuserade på ljudövervakning i smarta städer. Projektet använde sig av Internet of Things-teknologi i både inomhus- och utomhusmiljöer för att utföra storskaliga experiment i verkliga situationer. (Ståhlbröst et al., 2015) Experiment i utemiljöer berörde tillämpningsområden såsom trafikuppskattning och detektering av anmärkningsvärda händelser i städer, exempelvis sirener och olyckor (European Commission, 2015). Experiment utfördes genom att placera ut så kallade "Audio Processing Units", APUs, kopplade till befintliga intelligenta sensorer från tidigare forskningsprojekt. Dessa APUs var konstruerade med inbyggda mikrofoner för att kontinuerligt kunna avlyssna sin omgivning. Inkommande ljud analyserades lokalt på enheten för att bestämma om ljudet var av intresse. (Ståhlbröst et al., 2015) Systemet var uppbyggt så att enheterna kunde samla in och vidarebefordra ljuddata på begäran av en kontrollcentral under mänsklig bevakning (Pham, Cousin & Carer, 2014).

3.3 Principer för inbyggd integritet

Principer för inbyggd integritet har kommit att visa sig vara essentiella vid framställning av designriktlinjerna (avsnitt 4.3.2 och 5.3). I de tre kommande delavsnitten presenteras tre olika principer för inbyggd integritet. Två principer härstammar utifrån ett juridiskt perspektiv, Langheinrich (2001) och Datainspektionen (u.å.-a), och en princip utifrån ett moraliskt perspektiv, Ståhlbröst et al. (2015). Speciellt Ståhlbröst et al. (2015) designprinciper har stor betydelse vid framställning av designriktlinjerna. Övriga två principer tas med i kunskapsinventeringen då brister i dessa identifierats, vilket diskuteras vidare i avsnitt 6.3.

3.3.1 Inbyggd integritet för Ubiquitous Computing

Langheinrich (2001) tar i sin artikel upp principer för inbyggd integritet för så kallad "Ubiquitous computing". Ubiquitous computing är ett koncept som innebär att alla möjliga informations- och kommunikationstjänster är tillgängliga varsomhelst, närsomhelst och i alla former. För att förtydliga begreppet går det att likställa Internet of Things med Ubiquitous computing ur ett kommunikationsperspektiv. (Datainspektionen, 2007)

Langheinrich (2001) presenterar i sin artikel ett inflytelserikt policydokument, vid namn Fair Information Practices. Policydokumentet har legat till grund för lagstiftning, gällande skydd för privatliv och personlig integritet, världen över. Utifrån principerna i Fair Information Practices tillsammans med ett inflytelserikt Europeiskt direktiv, som ligger till grund för bland annat Personuppgiftslagen (avsnitt 3.4.4), föreslår Langheinrich (2001) sex principer för inbyggd integritet:

- *Upplysning/Öppenhet*
  Om personlig data samlas in från en användare ska de vara medvetna om detta.

- *Val och samtycke*
  Användare ska ha valet att dela eller inte dela med sig av sin personliga information. De måste ge samtycke till insamling.

- *Närhet och plats*
  Närhet avser att datainsamling från en användares enhet ska ske endast när användaren är i närheten. Plats innebär att bearbetning och tillgång till data ska ske endast på platsen där datan blivit inhämtad.

- *Anonymitet och pseudonymitet*
  När en användares identitet inte behövs eller när användare inte givit samtycke, ska data behandlas anonymt eller pseudonymt.

- *Adekvat säkerhet*
  Det ska finnas säkerhetsmekanismer som ger ett adekvat skydd av insamlad data.

- *Tillgång*
  En användares data ska endast vara tillgängligt för behöriga personer.

3.3.2 Datainspektionens checklista för inbyggd integritet

Datainspektionen har tagit fram en checklista för inbyggd integritet i IT-projekt. Datainspektionen menar att efterlevnad av checklistan ökar chanserna att lagstiftning på området följs. (Datainspektionen, u.å.-a)

Datainspektionens checklista sammanfattas nedan:

- *Genomför riskanalys och kartlägg konsekvenser*
  En riskanalys bör genomföras där konsekvenserna för integritetsintrång kartläggs (Datainspektionen, u.å.-a).

- *Minimera mängden personuppgifter*
  Mängden personuppgifter som samlas in och hanteras bör begränsas i den grad det är möjligt. Endast de personuppgifter som krävs för ändamålet med insamlingen ska samlas in. (Datainspektionen, u.å.-a)

- *Begränsa åtkomst till personuppgifter*
  Systemet ska vara utformat så att endast behöriga personer kan få tillgång till personuppgifter (Datainspektionen, u.å.-a).

- *Skydda personuppgifter*
  Det ska finnas säkerhetsfunktioner som skyddar personuppgifter. Desto känsligare personuppgifter, desto grundligare måste dessa säkerhetsfunktioner vara. (Datainspektionen, u.å.-a)

- *Systemet ska styra användaren rätt*
  För att integritetssäkra ett system ska systemet utformas så att användarens arbetssätt styrs i en integritetssäker riktning på ett användarvänligt sätt. Systemet ska bland annat utformas så att den registrerade tydligt upplyses om hur uppgifterna behandlas samt ge stöd till att ge eller ta tillbaka samtycke till behandlingen. (Datainspektionen, u.å.-a)

3.3.3 Inbyggd integritet i samband med EAR-IT

Medlemmar i forskningsprojektet EAR-IT fann det viktigt att undersöka medborgarnas syn på integritet med koppling till ljudövervakningssystem för smarta städer, då de ansåg att den allt mer påträngande digitaliseringen av städer ökar risken för att den personliga integriteten inskränks. Deras forskningsarbete utgjordes av en studie som fokuserade på moraliska aspekter kring personlig integritet och EAR-IT systemets inverkan på detta. Studien mynnade ut i designprinciper för att stödja design av nya IT-lösningar för smarta städer som skyddar rätten till privatliv och personlig integritet.

Ståhlbröst et al. (2015) tar därutöver upp problematiken med att tidigare designprinciper (avsnitt 3.3.1 och 3.3.2) avser IT-lösningar där de som är föremål för datainsamling är användare av IT-lösningarna. Problemet när det kommer till inbyggd integritet för IT-lösningar för smarta städer är att de som är föremål för datainsamling inte alltid är användare av IT-lösningarna utan endast blir påverkade av dem. De designprinciper som Ståhlbröst et al. (2015) föreslår bemöter denna problematik och presenteras nedan:

- *Generell placering av sensorer*
  Placera sensorer på ett sätt så att endast generell data kan samlas in och som inte avslöjar någon personlig information.

- *Ingen personlig lagring*
  Lagra inte data som kan härledas till en individ, även om det inte direkt handlar om personlig data. Exempel på sådan data är röstdata och rörelsemönster.

- *Strömma data*
  Istället för att lagra data, låt data flöda genom systemet och ha avlösare som känner igen data som är värdefull för systemet. Fokusera på exempelvis anmärkningsvärda händelser.

- *Isolerat sensorsystem*
  Systemet ska ej kombineras med annan teknologi. Genom att kombinera data eller system kan information avslöjas om en individ, vilket leder till ökad risk för intrång i den personliga integriteten, även om personlig information inte samlas in individuellt i något av systemen.

3.4 Svensk lagstiftning

Nedan behandlas majoriteten av de lagar och paragrafer som berörts i forskningsarbetet. Laghänvisningar återkommer i såväl uppsatsens empiriska som analytiska avsnitt. Lagarna har använts som utgångspunkt för att verifiera det som framkommit i intervjuerna och som referensram när de juridiska förutsättningarna identifierats och designriktlinjerna formulerats och motiverats. De lagar som uppmärksammats i forskningsarbetet är: Europakonventionen, Regeringsformen, Brottsbalken, Rättegångsbalken, Personuppgiftslagen, Polisdatalagen, Polislagen, Ordningslagen och Upphovsrättslagen. Presentation av lagarna i kommande delavsnitt kompletteras med länkar till aktuella avsnitt i lagtexten.

3.4.1 Regeringsformen

Regeringsformen, förkortad RF, är en svensk grundlag och innehåller bland annat medborgares fri- och rättigheter samt regler för hur myndigheter får bedriva sin verksamhet. I 2 kap. 6 § Regeringsformen behandlas bland annat medborgares rätt att gentemot det allmänna, det vill säga statliga verksamhet, vara skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och kan anses innebära en övervakning eller kartläggning av en persons personliga förhållanden. (SFS 1974:152)

I 1 kap. 9 § Regeringsformen behandlas bland annat krav på att det allmänna ska utöva sin makt opartiskt och sakligt (SFS 1974:152).

Länk: 2 kap. 6 § Regeringsformen
Länk: 1 kap. 9 § Regeringsformen

3.4.2 Europakonventionen

Europakonventionen, förkortad EKMR, är en konvention om mänskliga rättigheter. EKMR är utfärdat av Europarådet och gäller som svensk lag. Åttonde artikeln i EKMR behandlar envars rätt till skydd för privat- och familjeliv samt skydd för hem och korrespondens. (Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, u.å., SFS 1994:1219)

Länk: Åttonde artikeln i Europakonventionen

3.4.3 Brottsbalken

Brottsbalken, förkortad BrB, berör den allmänna straffrätten i Sverige. I brottsbalken beskrivs vilka brott som existerar samt dess påföljder. I 4 kap. 9 a § Brottsbalken behandlas olovlig avlyssning. Olovlig avlyssning omfattar avlyssning eller upptagning av tal som görs i hemlighet och i utrymmen dit allmänheten inte äger tillträde och som sker med tekniskt hjälpmedel ämnat för återgivning av ljud. Vid fall då olovlig avlyssning gör sig gällande räknas det som ett straffrättsligt brott och påföljderna är maximalt 2 års fängelse. (SFS 1962:700)

Länk: 4 kap. 9 a § Brottsbalken

3.4.4 Personuppgiftslagen

Personuppgiftslagen, förkortad PUL, reglerar hur personuppgifter får hanteras och avser i huvudsak databehandling av sådana uppgifter. Lagen syftar till att skydda människor mot att deras personliga integritet kränks. Personuppgiftslagen kompletteras därutöver av förordningar och föreskrifter från Datainspektionen. Utöver detta regleras, som tidigare nämnt, den personliga integriteten i artikel 8 i EKMR. I 3 § Personuppgiftslagen framgår det att all typ av information som direkt eller indirekt kan hänföras till en person, i livet, är att anses som en personuppgift. Begreppet behandling omfattar i personuppgiftslagen, bland annat, insamling och bearbetning av personuppgifter. I 3 § Personuppgiftslagen framgår även att samtycke definieras som en frivillig och otvetydig viljeyttring där en person godkänner behandling av uppgifter relaterade till denne. Enligt 21 § Personuppgiftslagen är det förbjudet för andra än myndigheter att behandla personuppgifter som rör lagöverträdelser, exempelvis brott och domar. (SFS 1998:204)

Länk: 3 § Personuppgiftslagen
Länk: 21 § Personuppgiftslagen

3.4.5 Polisdatalagen

Polisdatalagen, förkortad PDL, syftar till att ge polisen möjlighet att, i sin brottsbekämpande verksamhet, behandla personuppgifter. Den reglerar hur polisen får bedriva personuppgiftsbehandling och ser till att skydda människor mot kränkning av dess personliga integritet gentemot polisens personuppgiftsbehandling. (SFS 2010:361)

Länk: Polisdatalagen

3.4.6 Polislagen

Polislagen, förkortad PL, styr hur Polisens verksamhet får bedrivas och beskriver bland annat vilka uppgifter och befogenheter Polisen har, samt vem som får bedriva polisiär verksamhet. I 1 § Polislagen och 2 § Polislagen framgår det att det är Polisen som ska upprätthålla allmän ordning och säkerhet. (SFS 1984:387)

Länk: Polislagen

3.4.7 Kameraövervakningslagen

Kameraövervakningslagen, förkortad KÖL, reglerar kameraövervakning i Sverige. Syftet med lagen är att se till att kameraövervakning endast förekommer när övervakningsintresset väger tyngre än integritetsintresset. Kameraövervakning ska därutöver bedrivas enligt lag och god sed. Vid kameraövervakning ska hänsyn tas till den personliga integriteten.
(Datainspektionen, u.å.-b) Enligt kameröverväkningslagen innebär kameraövervakning användning av övervakningsutrustning. Med övervakningsutrustning avses bland annat TV-kameror och andra typer av optisk-elektroniska instrument. Till övervakningsutrustning räknas även andra tekniska anordningar som behandlar bild- och ljudmaterial. (SFS 2013:460)

Länk: Kameraövervakningslagen

3.4.8 Upphovsrättslagen

Upphovsrättslagen, förkortad URL, reglerar upphovsrätten. Lagen är omfattande och svåröverskådlig. Upphovsrätten omfattar verk av litterärt och konstnärligt slag. Exempel på sådant är ett musikaliskt verk, en film och en beskrivande framställning i tal. Rättigheterna som utgör upphovsrätten är uppdelat i ekonomiska och ideella rättigheter. Den ekonomiska rättigheten ger upphovsrättsinnehavaren exklusiv rätt till framställning av verket. En framställning innebär varje direkt eller indirekt, tillfällig eller permanent framställning av exemplar av verket. Framställningens form är irrelevant. Den ekonomiska rättigheten ger upphovsmannen kontroll till utnyttjande av verket och rättigheten kan överlåtas. Den ideella rättigheten innebär att upphovsmannen ska anges i en omfattning som krävs av god sed och i samband med framställning av ett exemplar av verket. Den ideella rättigheten är ofrånkomlig och kan ej avtalas bort. (Valentin Rehncrona, 2012)

Upphovsrätten kan inskränkas på så sätt att verk kan utnyttjas fritt ifall framställning sker för privat bruk eller att verk framställs som citat. Citering får göras av ett offentliggjort verk enligt god sed och i omfattning som motiveras av ändamålet med citeringen. I övrigt kan delar av upphovsrätten, som tidigare nämnts, avtalas bort med ömsesidigt avtal mellan upphovsman och nyttjare eller i form av en tvångslicens. För tvångslicens krävs att vissa specifika förhållanden föreligger.

Därutöver finns en inskränkning i upphovsrätten, 2 kap. 11 a § Upphovsrättslagen, som tillåter framställning av tillfälliga exemplar av verk. Det är tillåtet att framställa tillfälliga former av verk om framställningen är en del av en teknisk process, där framställningen är av en underordnad betydelse i denna process och att det inte görs av ekonomisk anledning. Därtill måste något av följande villkor vara uppfyllda för att inskränkning ska vara möjlig: att framställning görs i en överföring i nät mellan tredje parter via mellanhand eller via laglig användning med tillstånd från upphovsman. (Valentin Rehncrona, 2012, SFS 1960:729)

Att bryta mot upphovsrättslagen kan resultera i böter eller fängelse i högst två år. Valentin Rehncrona (2012) påpekar dock att det är den som påstår ett intrång som måste bevisa intrånget för att det ska göras gällande. Att bryta mot upphovsrättslagen kan utöver böter eller fängelse även resultera i ersättning till upphovsman och återkallande, ändring och förstörelse av egendom. Lagöverträdelse kan också leda till ett informationsföreläggande, där ursprung och spridning av verket måste förklaras av den som utfört upphovsrättsintrånget. (Valentin Rehncrona, 2012)

Länk: 2 kap. 11 a § Upphovsrättslagen
Länk: Upphovsrättslagen

4. Identifiering av juridiska förutsättningar

I detta avsnitt presenteras och motiveras de juridiska förutsättningar som identifierats för ljudövervakningssystem. De juridiska förutsättningarna ställer krav på utformningen av ljudövervakningssystem och ligger till grund för de designriktlinjer som tagits fram i forskningsarbetet. I detta avsnitt presenteras inledningsvis det empiriska underlag som den kvalitativa dataanalysen tagit utgångspunkt i. Det totala empiriska underlaget härstammar från 7 mejlintervjuer, 4 telefonintervjuer och 2 personliga intervjuer med jurister, IT-forensiker och fonetiker med olika expertis. Den kvalitativa dataanalysen resulterade i fem identifierade juridiska förutsättningar (avsnitt 4.3.2) för ljudövervakningssystem. Beskrivning av de teman som den kvalitativa dataanalysen gett upphov till återfinns i bilaga 3.

4.1 Informanter

Beskrivning av de informanter som deltagit i datainsamlingen illustreras i tabell 1.

Informant	Beskrivning	Intervjutyp
Informant 1	Jurist på Datainspektionen.	Telefonintervju
Informant 2	Doktor i offentlig rätt. Avhandling om polisiära befogenheter.	Personlig intervju och utvärderingsintervju
Informant 3	Professor Emeritus i straffrätt.	Telefonintervju
Informant 4	Jurist på Polismyndighetens rättsavdelning.	Telefonintervju
Informant 5	Doktorand i rättsinformatik.	Telefonintervju
Informant 6	Enhetschef på Datainspektionen,	Mejlintervju
Informant 7	Professor i fonetik.	Mejlintervju
Informant 8	Universitetsadjunkt inom IT och IT-forensik.	Mejlintervju
Informant 9	Sektionschef informationstekniksektionen för Nationellt Forensiskt Centrum.	Mejlintervju
Informant 10	Forskare i fonetik inom området röstidentifikation.	Mejlintervju
Informant 11	Tidigare doktorand i lingvistik. Jobbar numera med rättsfonetik på ett företag som agerat sakkunnig i domstolsärenden och som är underleverantör åt Nationellt Forensiskt Centrum.	Mejlintervju
Informant 12	Professor i fonetik.	Mejlintervju

Tabell 1. Lista över informanter som deltagit i datainsamlingen.

4.2 Empiri

Nedan presenteras det empiriska material som legat till grund för identifiering av juridiska förutsättningar och det empiriska material som uteslutits på grund av irrelevans. Empiriskt material som härstammar från utvärderingen presenteras inte i detta avsnitt utan i avsnitt 6.

4.2.1 Regeringsformen

Regeringsformen (avsnitt 3.4.1) har behandlats i fyra intervjuer. Det har i intervjuerna visat sig att det råder delade meningar huruvida 2 kap. 6 § Regeringsformen har betydelse för ljudövervakning eller inte. En informant anser att 2 kap. 6 § Regeringsformen är helt irrelevant i frågan om systemets kompabilitet med lag. En informant anser att inspelning av ljud på allmänna platser inte inskränker de rättigheter som ges av 2 kap. 6 § Regeringsformen. En informant anser att 2 kap. 6 § Regeringsformen är högst relevant och skulle utgöra ett direkt hinder för ljudövervakning på allmänna platser. Denna informant anser dock att 2 kap. 6 § Regeringsformen inte behöver beaktas i större utsträckning eftersom EKMR (avsnitt 3.4.2) innebär ett starkare skydd. Slutligen återfinns en informant som är osäker i frågan, men anser att inspelningar på allmän plats kan vara problematiskt med tanke på 2 kap. 6 § Regeringsformen.

Samtliga är dock överens om att 2 kap. 6 § Regeringsformen handlar om ett generellt integritetsskydd. Det handlar om rätten att få vara ifred, om att förtroliga samtal inte ska avlyssnas, och att envar i grund och botten har rätt till privatliv. Det krävs ett betydande integritetsintrång och att personer övervakas eller kartläggs för att lagen ska utgöra ett hinder för ljudövervakningssystem. Ifall det är ett privat företag som ligger bakom ett integritetsintrång i strid med 2 kap. 6 § Regeringsformen är det staten som ställs till svars då det är statens skyldighet att ha specifika regleringar som förhindrar intrånget. Därför är 2 kap. 6 § Regeringsformen en viktig bestämmelse rent formellt sett.

Utöver 2 kap. 6 § Regeringsformen har det även framkommit att 1 kap. 9 § Regeringsformen kan påverka utformningen av ett ljudövervakningssystem. Bestämmelsen förutsätter att placering av sensorer sker på ett sakligt och opartiskt sätt.

4.2.2 Europakonventionen

Europakonventionens åttonde artikel (avsnitt 3.4.2) har behandlats i fyra intervjuer. Intervjusvaren angående EKMR är i stort sett identiska med dem för 2 kap. 6 § Regeringsformen, men att åttonde artikeln i EKMR saknar begränsningen angående kartläggning, övervakning och betydande integritetsintrång. Av informant 5 framkommer att bedömningar utifrån EKMR är svåra. Informant 2 menar att åttonde artikeln i EKMR omfattar kartläggning och övervakning precis som 2 kap. 6 § Regeringsformen, om man ser till Europadomstolens praxis. Där utläses även att privatlivet ska vara skyddat på allmänna platser. Informant 2 menar att åttonde artikeln i EKMR är det starkaste skyddet och innebär därmed ett starkare skydd än 2 kap. 6 § Regeringsformen eftersom den saknar begränsningar som 2 kap. 6 § Regeringsformen innehar.

4.2.3 Personuppgiftslagen

Personuppgiftslagen (avsnitt 3.4.4) har behandlats i samtliga fem intervjuer med jurister. Det råder viss osäkerhet huruvida ljudinspelningar på allmän plats kan anses vara personuppgifter. Alla informanter är däremot överens om att ifall en inspelning kan kopplas till en specifik individ, då är det fråga om personuppgifter och då är personuppgiftslagen tillämplig. Det framgår även att en ljudupptagning som inte kan identifiera en person direkt kan användas som hjälpmedel i kombination med annan information, exempelvis material från kameraövervakning, för att identifiera en person. Ifall personuppgiftslagen är tillämplig måste ljudövervakningssystem förhålla sig till ett ganska omfattande regelverk.

Det framkommer i en av intervjuerna med Datainspektionen att personuppgiftsbehandling angående lagöverträdelser är exklusivt för Polisen.

4.2.4 Polisdatalagen

Polisdatalagen (avsnitt 3.4.5) har behandlats i fyra intervjuer. Samtliga informanter menar att polisdatalagen gäller för personuppgiftsbehandling. Tre av informanterna utvecklar påståendet och menar att polisdatalagen gäller för behandling av personuppgifter inom brottsbekämpande verksamhet. Av en informant framgår att Polisen har ensamrätt på denna typ av verksamhet. Därutöver utvecklar samma informant det regelverk som återfinns i polisdatalagen och vilka begränsningar det medför för ljudövervakningssystem. Med hänsyn till regelverkets irrelevans, framöver i analysen, presenteras inte innebörden av polisdatalagens regelverk.

4.2.5 Röstidentifikation

Temat röstidentifikation förekommer i sex mejlintervjuer med olika typer av experter inom fonetik och IT-forensik. Det råder viss osäkerhet huruvida en ljudinspelning av en röst med säkerhet kan kopplas till en specifik person. Fyra informanter menar att det inte går att identifiera en person med absolut säkerhet utifrån en ljudinspelning. Ingen av de tillfrågade hävdar det motsatta, det vill säga att det med säkerhet går att identifiera en person utifrån en ljudinspelning. Det framkommer dock att personer kan känna igen andra personer genom ledtrådar i talljudet om det kan kopplas till en relativt begränsad domän av referenspersoner, det vill säga vänner eller andra, för personen, kända personer. Därutöver framkommer det att en ljudinspelning kan användas som bevisning i domstol om det finns en annan ljudinspelning att jämföra med.

4.2.6 Brottsbalken

Brottsbalken (avsnitt 3.4.3) har behandlats i fyra intervjuer. Tre informanter anser att bestämmelsen i brottsbalken angående olovlig avlyssning, 4 kap. 9 § a Brottsbalken, inte är tillämplig eftersom upptagning av ljud sker på allmän plats. En informant anser att bestämmelsen dock kan gälla även för upptagning av ljud på allmänna platser och att man då måste tänka på att upptagning inte sker i hemlighet, eller att upptagning inte innehåller samtal mellan personer.

4.2.7 Upphovsrättslagen

Upphovsrättslagen (avsnitt 3.4.8) har behandlats i intervjun med informant 5. Informanten kan inte med säkerhet säga att lagen är tillämplig, men att lagen skulle kunna utgöra ett problem. Ljudupptagningar får i så fall inte innehålla större delar av ett skyddat verk. Med skyddat verk avses i detta fall musik.

4.2.8 Rättsläge

Det generella rättsläget har behandlats av två informanter. Informant 2 menar att ifall regeringsformen och EKMR inte utgör ett hinder för systemets juridiska kompatibilitet, så utgör inga andra lagar hinder för systemet. Informanten anser att om ett förtroligt samtal upptas, då utgör detta en överträdelse i såväl åttonde artikeln i EKMR som 2 kap. 6 § Regeringsformen. Om det går att garantera att ljudövervakningssystemet inte hör vad någon säger eller spelar in samtal, då är det större chans att ljudövervakning är laglig. Informanten menar därutöver att den viktigaste knäckfrågan för ljudövervakningssystem handlar om huruvida data i systemet kan knytas till specifika personer.

Om man vill ha ryggen fri, gäller det att försäkra sig om att det aldrig blir fråga om en inskränkning av privatlivet. Det får inte finnas en möjlighet att avlyssna i realtid eftersom risken för missbrukning är stor, och att åklagare skulle kunna använda detta som argument för att få en fällande dom.

Informant 5 belyser att ett fall måste avgöras i domstol för att ge definitiva svar på vilka bestämmelser som är tillämpliga och inte. Om ljudövervakningssystem utgör en stor investering anser informanten att det krävs en större juridisk utredning. Men inte ens då skulle ett definitivt svar på juridisk kompatibilitet kunna erhållas.

4.2.9 Kameraövervakningslagen

Kameraövervakningslagen (avsnitt 3.4.7) har behandlats i fem intervjuer. Fyra informanter är tydliga med att kameraövervakningslagen inte är tillämplig, däribland två jurister från datainspektionen. En informant är osäker huruvida kameraövervakningslagen är tillämplig.

4.2.10 Sekretess

Sekretess inom ramen för systemets distribution av data har behandlats i intervjun med informant 2. Informanten menar att distribution av data myndigheter emellan och mellan myndigheter och privatpersoner påverkas av sekretess. Sekretess är enligt informanten knutet till personuppgifter. Om något är sekretessbelagt hos en myndighet får det inte flyttas till en annan myndighet eller person.

4.2.11 Ordningslagen

Ordningslagen har behandlats i intervjun med informant 2. Informanten nämner att kommuner utifrån ordningslagen kan utfärda ordningsföreskrifter för uppsättning av sensorer. Ordningslagen i sig utgör inte ett hinder för systemet. I nuläget hävdar informanten att sådana ordningsföreskrifter inte finns. Däremot kan implementation av ljudövervakningssystem starta debatt som resulterar i att kommuner, i framtiden, inför ordningsföreskrifter. Sådana ordningsföreskrifter skulle exempelvis kunna innebära krav på tillstånd för installation av sensorer.

4.3 Analys av empiri

I detta delavsnitt redogörs inledningsvis vilka lagar som kan uteslutas på grund av irrelevans eller otillämplighet. Därefter presenteras och motiveras de juridiska förutsättningarna som utifrån det empiriska underlaget identifierats.

4.3.1 Utesluten empiri

Det första vi konstaterar är att ljudövervakning inte omfattas av kameraövervakningslagen. Det råder, i princip, konsensus om att upptagning av ljud på allmänna platser inte kan räknas till kameraövervakning då ljudupptagning ej kombineras med bildupptagning (avsnitt 3.4.7 Kameraövervakningslagen och 4.2.9 Kameraövervakningslagen). Det är därför inte nödvändigt att gå in närmare på konsekvenserna av denna lag.

Av det empiriska underlaget (avsnitt 4.2.10 Sekretess) framgår att distribution av data kan begränsas av sekretess. Sekretess är dock irrelevant eftersom det är knutet till personuppgifter. Det framgår, i avsnitt 5.3, att alla juridiska begränsningar som är knutna till personuppgifter är irrelevanta eftersom det aldrig får vara fråga om behandling av personuppgifter. Därför tas dessa problem inte i vidare beaktande i uppsatsen.

Av det empiriska underlaget (avsnitt 4.2.11 Ordningslagen) framgår att ordningsföreskrifter kan innebära problem. Ordningsföreskrifter är dock ett framtida problem där kommuner, i ett hypotetiskt scenario, har möjlighet att kräva tillstånd för sensorer genom fastställande av nya ordningsföreskrifter. På grund av forskningsarbetets avgränsning till rådande lagstiftning tas detta inte i vidare beaktande.

4.3.2 Identifiering av juridiska förutsättningar

Vid analys av det empiriska underlaget har fem juridiska förutsättningar identifierats för ljudövervakningssystem. I tabell 2 presenteras en sammanställning av dessa. De juridiska förutsättningarna motiveras var för sig i kommande delavsnitt.

Förutsättning nr.	Förutsättning
1	Ljud innehållandes större delar av skyddat verk, exempelvis musik, får ej framställas. Empiristöd: Avsnitt 4.2.7 Upphovsrättslagen.
2	Ljudövervakning i syfte att upprätthålla allmän ordning och säkerhet får endast bedrivas av Polismyndigheten. Empiristöd: Avsnitt 4.2.3 Personuppgiftslagen.
3	Ljudövervakning får inte anses vara en inskränkning av den personliga integriteten, privatlivet, familjelivet, dess hem eller korrespondens. Empiristöd: Avsnitt 4.2.1 Regeringsformen och 4.2.2 EKMR.
4	Placering av sensorer måste vara baserat på opartiska och sakliga grunder. Empiristöd: Avsnitt 4.2.1 Regeringsformen.
5	Tal får inte avlyssnas eller upptas, i enrum eller på platser dit allmänheten inte äger tillträde. Empiristöd: Avsnitt 4.2.6 Brottsbalken.

Tabell 2. Sammanställning av identifierade juridiska förutsättningar.

I följande motiveringar är det av intresse att veta ifall det som samlas in av ljudövervakningssystem är att anses som personuppgifter eller inte. I våra kontakter med experter inom fonetik och IT-forensik diskuterades huruvida ljudupptagningar kan knytas till specifika personer rent tekniskt (avsnitt 4.2.5 Röstidentifikation). Det framgick att ljudupptagningar kan användas som forensisk bevisning i domstol. Detta är en tydlig indikation på att det är möjligt att knyta ljudupptagningar till specifika personer. Samtliga experter är osäkra huruvida det, med säkerhet, går att identifiera personer via ljudupptagningar. De menar dock att det är möjligt att knyta ljud till specifika personer om domänen av referenspersoner är tillräckligt liten. Utifrån ovanstående information utgår vi framöver från att ljud kan kopplas till specifika personer eftersom det finns en möjlighet till detta om domänen av referenspersoner är tillräckligt liten.

Osäkerheten beträffande huruvida en inspelning kan kopplas till en specifik person avspeglar sig även i juristernas svar i intervjuerna (avsnitt 4.2.3). Det finns de som anser att en inspelning kan kopplas till specifika personer och det finns de som anser det motsatta. En av juristerna menar att även en ljudupptagning som inte direkt kan kopplas till en person, möjligtvis ändå kan ses som personuppgift om upptagningen kombineras med annan information, exempelvis med material från kameraövervakning. Därutöver finns en annan jurist, från Datainspektionen, som menar att så länge det finns en möjlighet att en ljudupptagning kan kopplas till en specifik person, så är det fråga om en personuppgift.

Av det empiriska underlaget framgår att ifall ljudupptagningar räknas som personuppgifter så är personuppgiftslagen (avsnitt 4.2.3 Personuppgiftslagen) och/eller polisdatalagen (avsnitt

4.2.4 Polisdatalagen) tillämpliga. Det finns då en rad juridiska förutsättningar som ett ljudövervakningssystem måste förhålla sig till. Eftersom det inte går att utesluta att en inspelning kan kopplas till en specifik person, varken av experter inom fonetik, IT-forensik eller juridik, så utgår vi, framöver, från att ett ljudövervakningssystem behandlar personuppgifter om det vid datainsamlingen spelar in ljud där röster förekommer.

Motivering till den första juridiska förutsättningen
Den första juridiska förutsättningen presenteras nedan, i tabell 3.

Förutsättning nr.	Förutsättning
1	Ljud innehållandes större delar av skyddat verk, exempelvis musik, får ej framställas. Empiristöd: Avsnitt 4.2.7 Upphovsrättslagen.

Tabell 3. Förutsättning nr. 1, utdrag från Tabell 2.

En av informanterna har belyst problemet kring ljudupptagningar där skyddat verk, till exempel musik, framkommer (avsnitt 4.2.7 Upphovsrättslagen). I upphovsrättslagen framgår att intrång i upphovsrätten kan resultera i flera stränga påföljder. Det är därför viktigt att undvika intrång i upphovsrätten. Intrånget sker då upphovsmannens rättigheter missbrukas i strid med upphovsrättslagen. Bland upphovsmannens rättigheter återfinns bland annat den ekonomiska rättigheten. Den ekonomiska rättigheten innebär exklusiv rätt till framställning av verk. Detta innebär att sådan framställning av verk aldrig får ske. Det framgår dock i upphovsrättslagen ett flertal tillåtna inskränkningar av upphovsrätten. Dessa inskränkningar tycks dock inte vara tillämpliga för ljudövervakningssystem. Inskränkningen angående tillfällig framställning av exemplar ser i första anblick ut att vara tillämplig. Vi menar dock att inte alla förutsättningar föreligger för att en sådan inskränkning skulle vara möjlig, eftersom framställning då måste syfta till "överföring i ett nät mellan tredje parter via en mellanhand" (SFS 1960:729) eller att "användning sker med tillstånd av upphovsman" (SFS 1960:729). Ingen av dessa förutsättningar föreligger och ur vår synvinkel går det därför inte att inskränka upphovsrätten. Därmed måste problemet med ljudupptagningar innehållandes skyddade verk tas i beaktande. Det går dock att ifrågasätta ifall det bör läggas fokus vid detta problem eftersom det i det teoretiska underlaget (avsnitt 3.4.8 Upphovsrättslagen) framgår att bevisbördan ligger på den som påstår ett intrång. Att bevisa intrång kan vara problematiskt om man inte lyckas komma över bevis på att intrånget faktiskt skett. Avslutningsvis anser vi att den juridiska förutsättningen som följer av ovanstående problem är att ljud innehållandes större delar av skyddat verk inte får framställas.

Motivering till den andra juridiska förutsättningen
Den andra juridiska förutsättningen presenteras nedan, i tabell 4.

Förutsättning nr.	Förutsättning
2	Ljudövervakning i syfte att upprätthålla allmän ordning och säkerhet får endast bedrivas av Polismyndigheten.

	Empiristöd: Avsnitt 4.2.3 Personuppgiftslagen.

Tabell 4. Förutsättning nr. 2, utdrag från Tabell 2.

Vi konstaterar utifrån det empiriska (avsnitt 4.2.3 Personuppgiftslagen) och teoretiska underlaget (avsnitt 3.4.4 Personuppgiftslagen och 3.4.6 Polislagen) att endast Polismyndigheten får behandla data i brottsbekämpande syfte. I 21 § Personuppgiftslagen står skrivet att uppgifter angående lagöverträdelser endast får behandlas av myndigheter. Detta har tagits upp av en informant. Enligt informanten är det inte säkert om 21 § Personuppgiftslagen är tillämplig eftersom det inte med säkerhet går att säga att ett ljudövervakningssystem nödvändigtvis samlar in uppgifter om lagöverträdelser. Informanten som anser detta är själv jurist på Polisens rättsavdelning och säger bland annat följande i intervjun:

> *"Och då ligger det på polisen ändå så det känns som en... det faller inte kanske på just tjugoförsta paragrafen i PUL utan det faller i så fall snarare på att det är polisen som ska ta hand om allmän ordning och säkerhet."* (personlig kommunikation, 21 april 2016)

Följaktligen anser informanten att det är Polismyndigheten som ska behandla data om lagöverträdelser oavsett om 21 § Personuppgiftslagen är tillämplig eller inte, eftersom det är Polismyndighetens uppgift att upprätthålla allmän ordning och säkerhet. Stöd för detta framgår av lagtext i 1 § Polislagen och 2 § Polislagen (avsnitt 3.4.6 Polislagen).

Motivering till den tredje juridiska förutsättningen
Den tredje juridiska förutsättningen presenteras nedan, i tabell 5.

Förutsättning nr.	Förutsättning
3	Ljudövervakning får inte anses vara en inskränkning av den personliga integriteten, privatlivet, familjelivet, dess hem eller korrespondens. Empiristöd: Avsnitt 4.2.1 Regeringsformen och 4.2.2 EKMR.

Tabell 5. Förutsättning nr. 3, utdrag från Tabell 2.

Eftersom det konstaterats att ljudövervakningssystem med brottsbekämpande syfte måste bedrivas av Polismyndigheten krävs det att ljudövervakningssystem respekterar de rättigheter som omfattas av åttonde artikeln i EKMR (avsnitt 3.4.2 EKMR) och 2 kap. 6 § Regeringsformen (avsnitt 3.4.1 Regeringsformen) som gäller för myndigheters verksamhet gentemot enskilda. Det råder dock viss osäkerhet huruvida dessa lagar behöver tas i beaktande. Hälften av informanterna anser att bestämmelserna är irrelevanta och hälften anser att de är högst relevanta och utgör direkta hinder för ljudupptagning på allmän plats. Bestämmelserna är väldigt vaga, vilket ger ett stort utrymme för olika tolkningar och olika avgöranden i domstol. Vi anser att det därför är bäst att vara förberedd på värsta möjliga scenario, i och med att det råder osäkerhet gällande tillämpligheten av 2 kap. 6 § Regeringsformen och åttonde artikeln i EKMR. Följaktligen utgår vi framöver från att lagarna är tillämpliga.

Eftersom det krävs lagstöd för att inskränka rättigheterna i 2 kap. 6 § Regeringsformen och åttonde artikeln i EKMR, och sådant lagstöd ej finns, måste ljudövervakningssystem utformas så att de ej kränker de rättigheter som framgår av lagarna. Ljudövervakning får därför ej

innebära ett intrång i den personliga integriteten, privatlivet, familjelivet, dess hem eller korrespondens.

Motivering till den fjärde juridiska förutsättningen
Den fjärde juridiska förutsättningen presenteras nedan, i tabell 6.

Förutsättning nr.	Förutsättning
4	Placering av sensorer måste vara baserat på opartiska och sakliga grunder. Empiristöd: Avsnitt 4.2.1 Regeringsformen.

Tabell 6. Förutsättning nr. 4, utdrag från Tabell 2.

Av det empiriska underlaget (avsnitt 4.2.1 Regeringsformen) framgår att 1 kap. 9 § Regeringsformen kan utgöra problem när det kommer till hur man väljer att placera sensorer. Av lagen framgår (avsnitt 3.4.1 Regeringsformen) att all makt som utövas av myndigheter gentemot enskilda måste vara opartisk och saklig. Detta innebär att placering av sensorer måste vara baserat på opartiska och sakliga grunder såvida ljudövervakning bedrivs av myndigheter.

Den fjärde juridiska förutsättningen föreligger eftersom vi tidigare (avsnitt 4.3.2 Motivering till den andra juridiska förutsättningen) konstaterat att ljudövervakning i brottsbekämpande syfte måste bedrivas av Polismyndigheten och därmed är 1 kap. 9 § Regeringsformen tillämplig.

Motivering till den femte juridiska förutsättningen
Den femte juridiska förutsättningen presenteras nedan, i tabell 7.

Förutsättning nr.	Förutsättning
5	Tal får inte avlyssnas eller upptas, i enrum eller på platser dit allmänheten inte äger tillträde. Empiristöd: Avsnitt 4.2.6 Brottsbalken.

Tabell 7. Förutsättning nr. 5, utdrag från Tabell 2.

Det framgår av det empiriska underlaget (avsnitt 4.2.6 Brottsbalken) att det är kriminaliserat att i hemlighet avlyssna eller uppta tal i enrum eller på platser dit allmänheten inte äger tillträde. Detta räknas i enlighet med 4 kap. 9 a § Brottsbalken (avsnitt 3.4.3 Brottsbalken) som olovlig avlyssning.

Med hänsyn till detta är det viktigt att ljudövervakningssystem inte avlyssnar eller upptar tal i enrum eller på platser dit allmänheten inte äger tillträde. Vi väljer att inkludera denna juridiska förutsättning trots att den strider mot uppsatsens avgränsning då 4 kap. 9 a § Brottsbalken påföljder är oerhört stränga och informanterna lagt stor vikt vid bestämmelsen i intervjuerna.

5. Designriktlinjer

I detta avsnitt presenteras (avsnitt 5.2) och motiveras (avsnitt 5.3) designriktlinjer som syftar till att tillfredsställa de juridiska förutsättningarna som identifierats i föregående avsnitt (avsnitt 4.3.2).

5.1 Designriktlinjernas uppbyggnad

Riktlinjerna är uppbyggda enligt Nowacks (1997) definition av designriktlinjer. Varje designriktlinje korresponderar till en juridisk förutsättning och innehåller delarna:

- *Riktlinje*
  En kortfattad sammanfattning av riktlinjen.

- *Problem*
  Beskriver det problem riktlinjen syftar till att avhjälpa. Denna del beskriver således den bakomliggande problematiken som härstammar från den korresponderande juridiska förutsättningen.

- *Berörda lagar*
  Beskriver vilka lagar som berörs ifall riktlinjen förbises eller förändras. För vissa riktlinjer tydliggörs på vilket sätt rättsläget förändras om riktlinjen förbises eller förändras.

- *Designkontext*
  Beskriver vilken av ljudövervakningssystemets funktioner som påverkas av riktlinjen. Ett ljudövervakningssystem har ur ett informatiskt perspektiv fyra funktioner: Insamling, bearbetning, lagring och distribution av data (Laudon & Laudon, 2011).

- *Rekommendationer*
  Beskriver rekommendationer för att avhjälpa problemet som presenterats i riktlinjen. I vissa designriktlinjer återfinns även konkretiserade rekommendationer som i större grad är praktiskt användbara för framtida utvecklare.

5.2 Designriktlinjer

De designriktlinjer som presenteras, i figur 2, är slutgiltiga och åtgärdade utifrån den återkoppling som framkommit i utvärderingen (avsnitt 6.1). Notera att designriktlinjerna inte presenteras i den ordning som de juridiska förutsättningarna presenterats i tabell 2. Ordningen i tabell 2 var nödvändig för att på ett begripligt sätt förklara de juridiska förutsättningarna, men är innehållsmässigt suboptimal, varför designriktlinjerna presenteras i en annan ordning i detta delavsnitt.

Riktlinje 1
Ljudövervakningssystem ska utformas på sådant sätt att insamlad data inte kan härledas till en specifik person, varken direkt eller indirekt. Insamlad data ska inte heller innehålla röster eller samtal.

Problem: Insamlad data som kan kopplas till en specifik person, direkt eller indirekt, kan anses vara ett intrång i de rättigheter som återfinns i 8 art. EKMR och 2 kap. 6 § RF. (Ziegler, 2014) (Avsnitt 4.2.8)

Berörda lagar: 8 art. EKMR och 2 kap. 6 § RF. Ifall data inte kan kopplas till en specifik person är PUL och PDL inte tillämpliga. Kan data kopplas till en specifik person är PUL och PDL tillämpliga, och dess regelverk måste tas i beaktande. (Avsnitt 4.2.1, 4.2.2, 4.2.3, 4.2.4)

Designkontext: Insamling, bearbetning, lagring och distribution av data. Riktlinjen är kritisk vid insamling av data.

Rekommendationer:

- Insamlad data får inte kunna kopplas till specifika personer. (Avsnitt 3.3.3 och 4.2.8)
- Insamlad data får inte innehålla röster eller samtal. (Avsnitt 3.3.3 och 4.2.8)
- Insamlad, bearbetad, lagrad eller distribuerad data får inte kombineras med annan information och/eller teknologi som inte är en del av systemet. (Ziegler, 2014) (Avsnitt 3.3.3 och 4.2.3)

Konkretiserade rekommendationer:

- Alternativ 1)
  Utforma systemets datainsamling på sådant sätt att data, istället för att lagras, flödar genom systemet. Endast data relaterad till anmärkningsvärda händelser behandlas i vidare utsträckning. Ljud samlas varken in eller lagras. (Avsnitt 3.3.3)

- Alternativ 2)
  Utforma systemet så att data samlas in via ljudupptagningar på sådant sätt att sensorers placering garanterar en inspelning där röster och samtal inte kan urskiljas pga. avstånd till ljudets källa. (Avsnitt 3.3.3 och 3.2.1)

Riktlinje 2
Ljudövervakningssystem ska utformas på sådant sätt att insamlad data inte kan innehålla större delar av skyddade verk, ex. musik.

Problem: Insamlad data som innehåller större delar av skyddat verk kan strida mot URL. (Avsnitt 3.4.8 och 4.2.7)

Berörda lagar: URL.

Designkontext: Insamling av data.

Rekommendationer:

- Insamlad data får inte innehålla större delar av skyddade verk. (Avsnitt 4.2.7)

Konkretiserade rekommendationer:

- Alternativ 1)
  Utforma systemets datainsamling på sådant sätt att data, istället för att lagras, flödar genom systemet. Endast data relaterad till anmärkningsvärda händelser behandlas i vidare utsträckning. Ljud samlas varken in eller lagras.

- Alternativ 2)
  Utforma systemet så att data samlas in via ljudupptagningar på sådant sätt att sensorers placering garanterar en inspelning där skyddade verk inte kan urskiljas pga. avstånd till ljudets källa.

Riktlinje 3
Ljudövervakningssystem får endast övervaka allmänna platser.

Problem: Att i hemlighet avlyssna eller uppta tal i enrum eller platser dit allmänheten inte äger tillträde är kriminaliserat och räknas i enlighet med 4 kap. 9a § BrB som olovlig avlyssning. (Avsnitt 3.4.3 och 4.2.6)

Berörda lagar: 4 kap. 9a § BrB.

Designkontext: Insamling av data.

Rekommendation:

- Placera och konstruera sensorer på sådant sätt att de endast kan uppta ljud på allmänna platser. (Avsnitt 3.4.3 och 4.2.6)

Riktlinje 4
Ljudövervakningssystem ska utformas på sådant sätt att sensorer placeras med geografiskt regelbunden utspridning alternativt att sensorer placeras med geografiskt oregelbunden utspridning baserat på sakliga och opartiska grunder.

Problem: Placering av sensorer kan strida mot 1 kap. 9 § RF om de placeras på partiska och osakliga grunder. (Avsnitt 4.2.1 och 3.4.1)

Berörda lagar: 1 kap. 9 § RF. (Avsnitt 4.2.1 och 3.4.1)

Designkontext: Insamling av data.

Rekommendationer:

- Placera sensorer med geografiskt regelbunden utspridning, alternativt
- Placera sensorer med geografiskt oregelbunden utspridning. Detta ska då rättfärdigas med en saklig och opartisk motivering. (Galdon-Clavell, 2013) (Avsnitt 4.2.1)

Konkretiserad rekommendation:

- Om sensorer placeras i specifika områden ska detta kunna motiveras, exempelvis med att området tidigare varit speciellt utsatt för brottslighet. (Avsnitt 4.2.1)

Riktlinje 5
Ljudövervakningssystem som syftar till att upprätthålla allmän ordning och säkerhet får endast användas av Polismyndigheten.

Problem: Det är Polismyndigheten som ska upprätthålla allmän ordning och säkerhet enligt 1 § PL och 2 § PL. (Avsnitt 3.4.6 och 6.1)

Berörda lagar: 1 § PL och 2 § PL. Även 21 § PUL om det är fråga om personuppgiftsbehandling. (Avsnitt 3.4.6, 4.2.3 och 6.1)

Designkontext: Insamling, bearbetning, lagring och distribution av data.

Rekommendation:

- Endast Polismyndigheten får bedriva ljudövervakning i syfte att upprätthålla allmän ordning och säkerhet. (Avsnitt 3.4.6 och 6.1)

Fig 2. Framtagna riktlinjer.

5.3 Motivering till designriktlinjer

Nedan motiveras var och en av de presenterade riktlinjerna. Det redogörs för vilken juridisk förutsättning som tillfredsställs av riktlinjen och hur dess rekommendationer tagits fram.

5.3.1 Motivering till Riktlinje 1

Den första designriktlinjen syftar till att bemöta den tredje juridiska förutsättningen med tre rekommendationer som kan konkretiseras till två alternativa rekommendationer. Detta sammanfattas i tabell 8 och redogörs därefter.

Förutsättning nr.	Förutsättning	Rekommendationer
3	Ljudövervakning får inte anses vara en inskränkning av den personliga integriteten, privatlivet, familjelivet, dess hem eller korrespondens.	Insamlad data får inte kunna kopplas till specifika personer. Insamlad data får inte bestå av röster eller samtal. Insamlad data får ej kombineras med annan information då detta kan identifiera och avslöja information om en specifik individ.

Tabell 8. Förutsättning nr. 3 och dess korresponderande rekommendationer.

För att undvika att inskränka rättigheterna i 2 kap. 6 § Regeringsformen (avsnitt 3.4.1 Regeringsformen) och åttonde artikeln i EKMR (avsnitt 3.4.2 Europakonventionen) måste ljudövervakningssystem utformas på sådant sätt att de ej kränker de rättigheter som följer av de två lagarna. De informanter som anser att 2 kap. 6 § Regeringsformen och åttonde artikeln i EKMR utgör hinder för ljudövervakningssystem menar att ljudupptagningar är särskilt problematiskt. De menar att förtroliga samtal inte får spelas in och att ingen röst får vara urskiljbar. Det framgår av dessa informanter att ju längre man kommer ifrån att kunna identifiera personer utifrån insamlad data, desto större chans är det att rättigheterna i 2 kap. 6 § Regeringsformen och åttonde artikeln i EKMR respekteras. Om datainsamling sker utan att möjliggöra koppling till specifika personer är det inte fråga om personuppgifter och då är inte personuppgiftslagen eller polisdatalagen tillämpliga och troligtvis inte heller 2 kap. 6 § Regeringsformen och åttonde artikeln i EKMR. Det blir då fråga om ett oreglerat rättsområde. Ovanstående har sammanfattats i två rekommendationer.

1. Insamlad data får inte kunna kopplas till specifika personer. Empiristöd: Avsnitt 4.2.8 Rättsläge. Teoristöd: Avsnitt 3.3.3 Inbyggd integritet i samband med EAR-IT.

2. Insamlad data får inte bestå av röster eller samtal. Empiristöd: Avsnitt 4.2.8 Rättsläge. Teoristöd: Avsnitt 3.3.3 Inbyggd integritet i samband med EAR-IT.

Utöver de två ovanstående rekommendationerna framgår av empiriskt underlag att anonym data kan användas som hjälpmedel i kombination med annan information eller teknologi för

att identifiera en specifik individ. Därav har de två ovanstående rekommendationerna kompletterats med ytterligare en rekommendation.

3. Insamlad data får ej kombineras med annan information då detta kan identifiera och avslöja information om en specifik individ. Empiristöd: Avsnitt 4.2.3 Personuppgiftslagen. Teoristöd: Avsnitt 3.3.3 Inbyggd integritet i samband med EAR-IT och Ziegler (2014).

De tre ovanstående rekommendationerna har i huvudsak teoretiskt stöd i Ståhlbröst et al. (2015) designprinciper. Designprinciperna syftar till att försäkra att system för smarta städer utformas så att de värnar om privatlivet. Den första och andra rekommendationen har teoretiskt stöd i designprincipen "Ingen Personlig Lagring". Designprincipen innebär att man inte ska lagra data som kan härledas till en individ. Vi menar dock att betoning på lagring inte räcker eftersom regeringsformen, EKMR, personuppgiftslagen och polisdatalagen tillämpas så fort data samlas in. Den tredje rekommendationen har teoretiskt stöd i designprincipen "Isolerat sensorsystem", vilket innebär att smarta städer-system inte ska kombineras med annan teknologi eftersom det kan avslöja information om en person och bidra till integritetsintrång, även om ingen personuppgift samlas in individuellt i något av systemen. Vi anser därutöver med stöd av empiriskt material (avsnitt 4.2.3 Personuppgiftslagen) att det räcker att data kombineras med annan information, och inte endast teknologi, för att möjliggöra koppling till en specifik individ.

De tre rekommendationerna är diffusa och ger dålig vägledning för framtida utvecklare av ljudövervakningssystem. Därför har de konkretiserats till två alternativa och praktiskt användbara rekommendationer. Dessa presenteras nedan.

1. *Alternativ 1*
   Utforma systemets datainsamling på sådant sätt att data, istället för att lagras, flödar genom systemet. Endast data relaterad till anmärkningsvärda händelser behandlas i vidare utsträckning. Ljud samlas varken in eller lagras.

   Rekommendationen har teoretiskt stöd i designprincipen "Strömma data" (avsnitt 3.3.3 Inbyggd integritet i samband med EAR-IT).

2. *Alternativ 2*
   Utforma systemet så att data samlas in via ljudupptagningar på sådant sätt att sensorers placering garanterar en inspelning där röster och samtal inte kan urskiljas pga. avstånd till ljudets källa.

   Rekommendationen har teoretiskt stöd i avsnitt 3.3.3 Inbyggd integritet i samband med EAR-IT och avsnitt 3.2.1 ShotSpotter. Rekommendationen togs fram genom att konkretisera Ståhlbröst et al. (2015) designprincip "Generell placering av sensorer" med ShotSpotters lösning för att undvika att mänskliga samtal och konversationer tas upp av systemet. ShotSpotter löser problemet genom att placera sensorer med en viss höjd från marken så att ljud, innehållandes konversationer, försvagas så pass mycket på vägen till sensorn att ljudet ej längre kan urskiljas.

5.3.2 Motivering till Riktlinje 2

Den andra designriktlinjen syftar till att bemöta den första juridiska förutsättningen med en rekommendation som kan konkretiseras till två alternativa rekommendationer i likhet med Riktlinje 1. Detta sammanfattas i tabell 9 och redogörs därefter.

Förutsättning nr.	Förutsättning	Rekommendationer
1	Ljud innehållandes större delar av skyddat verk, exempelvis musik, får ej framställas.	Insamlad data får inte bestå av större delar av skyddat verk, ex musik.

Tabell 9. Förutsättning nr. 1 och dess korresponderande rekommendation.

Grundproblematiken kring den första förutsättningen är att undvika intrång i upphovsrätten. Intrånget sker då upphovsmannens rättigheter missbrukas, däribland den ekonomiska rättigheten. Den ekonomiska rättigheten innebär en exklusiv rätt till framställning av verk. Med framställning menas varje direkt, indirekt, tillfällig eller permanent framställning av ett exemplar av ett verk (avsnitt 3.4.8 Upphovsrättslagen).

Vår tolkning av framställningsbegreppet är att så fort ett verk lagras, tillfälligt eller permanent, exempelvis som en ljudupptagning, är det fråga om en framställning av ett exemplar av verket och då räknas det som en framställning av verket i enlighet med upphovsrättslagen. Då ett upphovsrättsskyddat verk, utan ömsesidig överenskommelse, inte får framställas, menar vi att en naturligt tillfredsställande rekommendation för förutsättningen är att skyddade verk aldrig får samlas in av ljudövervakningssystem. Rekommendationen kan dock anses vara abstrakt, varför rekommendationen konkretiserats till två praktiska och alternativa rekommendationer. Dessa presenteras nedan:

1. *Alternativ 1*
   Utforma systemets datainsamling på sådant sätt att data, istället för att lagras, flödar genom systemet. Endast data relaterad till anmärkningsvärda händelser behandlas i vidare utsträckning. Ljud samlas varken in eller lagras.

2. *Alternativ 2*
   Utforma systemet så att data samlas in via ljudupptagningar på sådant sätt att sensorers placering garanterar en inspelning där skyddade verk inte kan urskiljas pga. avstånd till ljudets källa.

5.3.3 Motivering till Riktlinje 3

Den tredje designriktlinjen syftar till att bemöta den femte juridiska förutsättningen med en rekommendation. Detta sammanfattas i tabell 10 och redogörs därefter.

Förutsättning nr.	Förutsättning	Rekommendationer
5	Tal får inte avlyssnas eller upptas, i enrum eller på platser dit allmänheten inte äger tillträde.	Placera och konstruera sensorer på sådant sätt att de endast kan uppta ljud på allmänna platser.

Tabell 10. Förutsättning nr. 5 och dess korresponderande rekommendation.

Det framgår av empiriskt (avsnitt 4.2.6 Brottsbalken) och teoretiskt underlag (avsnitt 3.4.3 Brottsbalken) att det är kriminaliserat att i hemlighet avlyssna eller uppta tal i enrum eller på platser dit allmänheten inte äger tillträde. Detta räknas i enlighet med 4 kap. 9 a § Brottsbalken som olovlig avlyssning. Därför är det viktigt att ett ljudövervakningssystem endast utför ljudövervakning på allmänna platser, och att sensorerna är placerade och konstruerade på sådant sätt att de endast kan uppta ljud på dessa platser.

5.3.4 Motivering till Riktlinje 4

Den fjärde designriktlinjen syftar till att bemöta den fjärde juridiska förutsättningen med två alternativa rekommendationer. Detta sammanfattas i tabell 11 och redogörs därefter.

Förutsättning nr.	Förutsättning	Rekommendationer
4	Placering av sensorer måste vara baserat på opartiska och sakliga grunder.	Placera sensorer med geografiskt regelbunden utspridning, alternativt placera sensorer med geografiskt oregelbunden utspridning och rättfärdiga med en saklig och opartisk motivering.

Tabell 11. Förutsättning nr. 4 och dess korresponderande rekommendationer.

I det empiriska underlaget (avsnitt 4.2.1 Regeringsformen) framgår att placering av sensorer måste vara opartisk och saklig. Om placering inte är opartisk och saklig, utan specificerad till specifika områden måste det finnas en saklig grund till varför man väljer att placera sensorer i vissa områden och inte andra.

5.3.5 Motivering till Riktlinje 5

Den femte designriktlinjen syftar till att bemöta den andra juridiska förutsättningen med en rekommendation. Detta sammanfattas i Tabell 12 och redogörs därefter.

Förutsättning nr.	Förutsättning	Rekommendationer
2	Ljudövervakning i syfte att upprätthålla allmän ordning och säkerhet får endast bedrivas av Polismyndigheten.	Endast Polismyndigheten får bedriva ljudövervakning i syfte att upprätthålla allmän ordning och säkerhet.

Tabell 12. Förutsättning nr. 2 och dess korresponderande rekommendation.

Rekommendationen till denna juridiska förutsättning härstammar naturligt från förutsättningen i sig. Vi ansåg att endast en omformulering av förutsättningen var nödvändig för att passa in som rekommendation.

6 Utvärdering och diskussion

I detta avsnitt behandlas resultatet av utvärderingen. Utvärderingen utgör en del av det empiriska underlaget till designriktlinjerna och genomfördes som en utvärderingsintervju med informant 2. Observera att det finns skillnader mellan de slutgiltiga riktlinjerna (avsnitt 5.2) och de som presenterats för utvärderaren. Denna skillnad består i huvudsak av att delar av Riktlinje 5 omformulerats. Omformuleringen innebär i stort att riktlinjens problembeskrivning och berörda lagar modifierats enligt anvisning.

6.1 Empiri

På fråga om riktlinjernas tillförlitlighet framkom att det fanns marginella anmärkningar. De åtgärder som föreslogs var att omformulera Riktlinje 5 till att avse "Polismyndigheten", alltså i bestämd form med stort P, istället för "polismyndigheter". Detta eftersom det inte längre finns flera polismyndigheter i Sverige.

Det framkom att 21 § Personuppgiftslagen i Riktlinje 5 inte är tillämplig eftersom Riktlinje 1 medför att det inte är fråga om personuppgiftsbehandling. 21 § Personuppgiftslagen i Riktlinje 5 borde därför inte anges som ett problem.

Utvärderaren såg därutöver att ingen hänvisning skett till lag när det påstås att endast Polismyndigheten får bedriva ljudövervakning i syfte att upprätthålla allmän ordning och säkerhet. Utvärderaren påpekade att man bör hänvisa till 1 § Polislagen och 2 § Polislagen. Där står det skrivet att det endast är polisen som ska upprätthålla allmän ordning och säkerhet.

Vid fråga om riktlinjernas fullständighet kom informanten fram till följande:

> *"Nej, jag tycker det var snyggt, vad ni har jobbat!"* (personlig kommunikation, 13 maj 2016)

Avslutningsvis sammanfattade informanten utvärderingen:

> *"Tillförlitlighet, absolut. Fullständighet, ja, vad jag kan bedöma."* (personlig kommunikation, 13 maj 2016)

6.2 Analys av utvärdering

Om man jämför det empiriska materialet, från utvärderingsintervjun, med de indikatorer som presenteras i utvärderingsplanen (bilaga 4), angående vad som bör anses vara en framgångsrik utvärdering, går det att konstatera att indikatorn för fullständighet är uppfylld men inte indikatorn för tillförlitlighet. Anmärkningarna gällande tillförlitligheten är dock försumbara och innebär endast en omformulering och en laghänvisning. Således påverkas inte de uppmanade handlingarna och designriktlinjernas innebörd. Efter att ha åtgärdat problemet med hur Riktlinje 5 formulerats menar vi att riktlinjerna både är tillförlitliga och fullständiga utifrån det som framkommit i utvärderingen. Det går dock att ifrågasätta huruvida riktlinjerna, trots detta resonemang, är tillförlitliga och fullständiga. Detta eftersom det går att ifrågasätta huruvida utvärderingen i sig är att betrakta som pålitlig. Detta diskuteras vidare i avsnitt 7.2.

6.3 Diskussion

Våra designriktlinjer överensstämmer dåligt med tidigare designprinciper. Exempel på sådana principer är Datainspektionens (u.å.-a) checklista för inbyggd integritet och Langheinrichs (2001) principer för inbyggd integritet. De sistnämnda principerna behandlar bland annat "Upplysning/Öppenhet", "Val och samtycke", "Närhet och Plats", "Anonymitet och pseudonymitet". Vi menar dock att Langheinrichs (2001) principer är otillräckliga för att försäkra juridisk kompatibilitet gällande personlig integritet, i fallet för ljudövervakningssystem. Langheinrich (2001) påstår att ifall samtycke inte kan tas ska systemet behandla data anonymt eller pseudonymt. Detta räcker dock inte då systemet kan anses vara olagligt redan vid insamling av personlig data då det eventuellt strider mot 2 kap. 6 § Regeringsformen (avsnitt 4.2.1 Regeringsformen, 3.4.1 Regeringsformen) och åttonde artikeln i EKMR (avsnitt 4.2.2 EKMR, 3.4.2 EKMR) oavsett om data behandlas anonymt eller pseudonymt. Därutöver är principerna "Adekvat säkerhet" och "Tillgång" helt irrelevanta ur juridisk synpunkt i fråga om ljudövervakningssystem, så länge personuppgiftslagen och/eller polisdatalagen inte är tillämpliga. Vi konstaterar att ingen av Langheinrich (2001) designprinciper löser de identifierade juridiska förutsättningarna (avsnitt 4.3.2). De är följaktligen otillräckliga för att skydda den personliga integriteten, när det kommer till ljudövervakningssystem, med hänsyn till 2 kap. 6 § Regeringsformen och åttonde artikeln i EKMR.

Samma problematik återfinns även mellan våra designriktlinjer och Datainspektionens (u.å.-a) checklista för inbyggd integritet. Checklistan innehåller dock ett avsnitt som inte är helt irrelevant, nämligen "Genomför riskanalys och kartlägg konsekvenser". Avsnittet är dock inte vägledande gällande hur ett ljudövervakningssystem ska utformas utan vägleder snarare utvecklingsprocessen. Därav har avsnittets innehåll inte inkluderats i designriktlinjerna. Resterande punkter i checklistan tillfredsställer inte de identifierade juridiska förutsättningarna, varför vi anser att datainspektionens checklista inte skyddar den personliga integriteten i tillräckligt hög grad, när det kommer till ljudövervakningssystem, med hänsyn till 2 kap. 6 § Regeringsformen och åttonde artikeln i EKMR.

Ett exempel på en ren motsägelse mellan våra designriktlinjer och traditionella principer för inbyggd integritet som ges av Datainspektionen (u.å.-a) och Langheinrich (2001) är att användare ska kunna ge samtycke till behandling i syfte att skydda den personliga integriteten. Våra designriktlinjer saknar samtyckeskrav eftersom vi har svårt att se hur detta är möjligt vid ljudövervakning av allmänna platser. Vi menar dock ändå att det är möjligt att utforma ljudövervakningssystem som respekterar den personliga integriteten och rätten till privatliv, utifrån ett juridiskt perspektiv. Det finns andra sätt att gå tillväga för att skydda den personliga integriteten vid design av ljudövervakningssystem. Det framgår av forskningsresultatet att det går att skydda den personliga integriteten och rätten till privatliv, ur ett juridiskt perspektiv, genom att undvika att samla in personliga uppgifter från början. Vi spekulerar i det som Ståhlbröst et al. (2015) diskuterar i sin artikel, nämligen att det krävs nya principer för inbyggd integritet för smarta städer-system, eftersom tidigare principer endast avser system där de som utsätts för systemet faktiskt är användare av systemet. Vid jämförelse mellan våra riktlinjer och de designprinciper som föreslås av Ståhlbröst et al. (2015) kan vi konstatera att det finns stora likheter. Samtliga av Ståhlbröst et al. (2015) designprinciper är till stor hjälp, även ur ett juridiskt perspektiv, men ej heltäckande. De täcker exempelvis inte designriktlinjerna 3, 4 och 5. Detta har en logisk förklaring: Riktlinje 3, 4 och 5 berör inte den personliga integriteten och bör därför inte inkluderas i principer för inbyggd integritet.

Avslutningsvis, om man jämför våra designriktlinjer med det befintliga ljudövervakningssystemet ShotSpotter går det att konstatera att ShotSpotter inte är kompatibelt med svensk lagstiftning. ShotSpotter drivs av ett privat företag och strider därför mot Riktlinje 5 (avsnitt 5.2) och således mot 1 § Polislagen och 2 § Polislagen. Utöver detta är det osäkert ifall sensorernas placering, på hustak och på gatubelysning, räcker för att garantera att röster, samtal och skyddade verk inte samlas in av systemet och att detta argument faktiskt håller i en svensk domstolsprövning. Detta medför att det är svårt att avgöra om ShotSpotter strider mot Riktlinje 1 och 2 (avsnitt 5.2), 2 kap. 6 § Regeringsformen, åttonde artikeln i EKMR och upphovsrättslagen. Dessutom finns det en risk att systemet strider mot Riktlinje 4 (avsnitt 5.2), 1 kap. 9 § Regeringsformen om det inte finns en skälig grund till att sensorer placeras i vissa områden.

I kontrast till ShotSpotters tydliga inkompatibilitet med svensk lagstiftning är det svårare att resonera om detsamma för EAR-IT. Den otillräckliga dokumentation som finns att tillgå angående systemets uppbyggnad gör det svårt att avgöra ifall systemets datainsamling är legal eller illegal. Ljudövervakningssystemet ligger dessutom utanför forskningsarbetets avgränsning då systemet inte tillämpas i brottsbekämpande syfte. För EAR-IT måste inte ljudövervakning bedrivas av Polismyndigheten eller någon annan myndighet och då råder ett helt annat rättsläge. Detta förklaras i större detalj i avsnitt 7.3.

7. Slutsats och reflektion

I detta avsnitt återkopplas forskningsarbetets resultat med den frågeställning som angavs i syftet. Därutöver förs diskussion och reflektion kring forskningsprocessen och dess resultat. Avslutningsvis presenteras möjliga förbättringsområden och förslag på framtida forskning.

7.1 Slutsats

Forskningsprocessen har mynnat ut i designriktlinjer beträffande hur man bör utforma ljudövervakningssystem i enlighet med rådande svensk lagstiftning. Designriktlinjerna har utvärderats förhållandevis framgångsrikt och åtgärdats därefter. Vi konstaterar att forskningen framgångsrikt besvarat frågeställningen gällande hur ett ljudövervakningssystem bör utformas i enlighet med rådande svensk lagstiftning. Till viss förvåning kan vi också konstatera att det troligtvis är möjligt att utforma ett ljudövervakningssystem utan att strida mot lagstiftning, men att de restriktiva juridiska förutsättningarna bidrar till många begränsningar. Dessa begränsningar resulterar i sin tur i mindre praktiska lösningar. De praktiska lösningarna har identifierats utifrån tidigare forskning, däribland Ståhlbröst et al. (2015), Ziegler (2014) och Galdon-Clavell (2013), och av det befintliga ljudövervakningssystemet ShotSpotter (avsnitt 3.2.1 ShotSpotter).

Det kan hävdas att forskningsarbetets avgränsning till ljudövervakningssystem för brottsbekämpande syften bidrar till riktlinjer med dålig generaliserbarhet. Generaliserbarhet har dock ständigt eftersträvats vilket bidragit till att riktlinjerna utformats omfattande och med tillhörande bakgrundsinformation som tydligt beskriver bakomliggande problem och riktlinjernas koppling till lagar och bestämmelser. På så vis förenklas processen med att spåra vilka designriktlinjer som påverkas av vilka lagar och det blir enklare att förutsäga effekterna av förändrade eller förbisedda designriktlinjer. Dessutom kan designriktlinjerna även användas vid utveckling av ljudövervakningssystem för andra syften än brottsbekämpande, men då finns risken att riktlinjerna är onödigt restriktiva. För ljudövervakning i andra syften än att upprätthålla allmän ordning och säkerhet kan Riktlinje 5 förbises. Om ljudövervakning inte bedrivs av myndighet kan även Riktlinje 4 förbises.

7.2 Forskningsprocessen

I forskningsarbetet har vi genomfört alla de steg som Oates (2006, s. 111) beskriver som typiska för Design Science. Därutöver har vi haft i åtanke och följt de riktlinjer som föreslås av Hevner et al. (2004) för forskning inom Design Science. Vi har tagit fram en artefakt, dokumenterat problemrelevans i uppsatsen (avsnitt 1.1 och 1.2), utvärderat artefakten i enlighet med konventionella utvärderingsmetoder för Design Science-artefakter (avsnitt 2.4) och betonat noggrannhet vad gäller val och användande av metoder i design- och utvecklingsfaserna (avsnitt 2.5). Det går dock att ifrågasätta iterativiteten av forskningsarbetet då endast en iteration av Oates (2006) samtliga steg för Design Science genomförts.

Vi har i forskningsarbetet avlagt betydande tid åt intervjuer. Med hänsyn till uppsatsens dignitet bedömer vi att en god empirisk grund erhållits. Vi har eftersträvat en god spridning och trovärdighet gällande val av informanter. Flera informanter som deltagit i datainsamlingen innehar tung expertis inom sitt rättsområde och informanterna har valts så att deras expertis kompletteras med andra informanters expertis. Ingen informant innehar expertis inom samma

rättsområde som någon annan. Därutöver har data samlats in från experter inom fonetik och IT-forensik för att komplettera juristernas marginella kunskaper om röstidentifikation med kunskap från sakkunniga. Överlag bedöms således intervjuprocessen som rigorös. Dock ska det noteras att intervjuprocessen är bristfällig vad gäller mättnad. Det är definitivt möjligt att nå en högre mättnadsgrad i intervjumaterialet, då det framkommit nya juridiska problem även i den sista intervjun innan utvärderingen.

Den svagaste länken i forskningsarbetet är utvärderingen. På grund av forskningsarbetets knappa tidsram fanns det endast möjlighet till en formativ utvärdering. Det hade varit önskvärt att även genomföra en summativ utvärdering, så att åtgärder i riktlinjerna kunnat valideras. Det hade därutöver varit eftersträvansvärt att låta fler experter utvärdera riktlinjerna för att förbättra utvärderingens trovärdighet. I nuläget är trovärdigheten av utvärderingen låg eftersom endast en expert varit föremål för intervju. Detta innebär att även fast utvärderingen visat på tillförlitliga och fullständiga riktlinjer så kan kvalitetsegenskaperna långt ifrån garanteras; utvärderingen i sig kan ses som opålitlig. Visserligen valdes utvärderingsexperten med bakgrund av att denne bedömts som mest kunnig på rättsområdet utifrån tidigare intervjusvar och avhandling. Valet baserades också på att det funnits indikationer på att utvärderingsexperten initialt varit mest kritisk till övervakning. Detta är en försiktighetsåtgärd som eventuellt kan resultera i onödigt restriktiva designriktlinjer. Vi menar dock att det är bättre att låta en kritisk expert utvärdera riktlinjerna än tvärtom, då det motsatta löper större risk att resultera i designriktlinjer som har en falsk-positiv tillförlitlighet och fullständighet.

Det ska sägas att erhållna intervjusvar visat på väsentliga skillnader mellan olika informanters åsikter om lagars tillämplighet. I slutändan går det dock inte att säkerställa ett rättsläge förrän ljudövervakningssystem prövats i svensk domstol. Detta kommer inte ske om ljudövervakningssystem aldrig introduceras i Sverige eller Europa, eller om ingen har för avsikt att sätta stopp för sådana system. Resultatet av vårt forskningsarbete har dock visat att det högst troligt går att utforma lagliga ljudövervakningssystem för svensk marknad. Detta till vissa experters förvåning. Ett exempel är informant 2 som under intervjuprocessen ändrat åsikt om chanserna att utforma ljudövervakningssystem i enlighet med svensk lagstiftning. I första kontakt med informanten över mejl sades följande:

> *"Min spontana kommentar är att det inte kommer att funka rättsligt, hur ni än designar programmet."* (personlig kommunikation, 4 april 2016)

Samma informant hade i takt med att vi presenterat våra designalternativ och våra designriktlinjer fundamentalt ändrat åsikt.

Vårt forskningsarbete har därutöver tydliggjort att det finns intressanta tillämpningsområden och möjligheter med ljudövervakningssystem. Vi väntar nu spänt på vilka innovationer som uppträder på området i framtiden och hoppas att teknologin når Sverige inom snar framtid.

7.3 Förslag på vidare forskning

Om ljudövervakningssystem inte används i brottsbekämpande syfte och dessutom av privata företag blir rättsläget drastiskt förändrat. Då kan eventuellt den mest kritiska riktlinjen, Riktlinje 1, och även Riktlinje 4 och 5 bortses. Detta innebär att 1 kap. 9 § Regeringsformen, 2 kap. 6 § Regeringsformen och åttonde artikeln i EKMR kan bortses. Detta medför att det eventuellt är fullt möjligt att spela in ljud på allmänna platser, innehållandes urskiljbara röster

och samtal, om det ligger i linje med det regelverk som återfinns i personuppgiftslagen. Anpassning måste då göras utifrån personuppgiftslagen. Detta innebär att ytterligare undersökning av juridiska förutsättningar måste genomföras. Vi uppmanar därför att i framtida forskning genomföra sådan typ av undersökning. En stor problematik som uppstår handlar om att ljudövervakningssystem måste kunna informera och/eller ge möjlighet till samtycke, eller att motsvarande inskränkningar återfinns i personuppgiftslagen.

Utöver att i framtida forskning undersöka denna typ av anpassning, kommer det inom snar framtid vara nödvändigt att beakta EU:s nya dataskyddsförordning som träder i kraft år 2018. Förordningen innebär en rad förändringar i förhållande till personuppgiftslagens nuvarande regelverk och dessa förändringar kan komma att påverka de framtagna designriktlinjerna om definitionen av personuppgift ändras. (Datainspektionen, 2016)

Källförteckning

Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart Cities: Definitions, Dimensions, Performance, and Initiatives. Journal of Urban Technology, 22(1), 3-21. doi: 10.1080/10630732.2014.942092

Bakici, T., Almirall, E., & Wareham, J. (2013). A Smart City Initiative: the Case of Barcelona. Journal of the Knowledge Economy, 4(2), 135-148. doi: 10.1007/s13132-012-0084-9

Bandyopadhyay, D. & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. Wireless personal communications, 58(1), 49-69. doi:10.1007/s11277-011-0288-5

Becker, J., Heddier, M., Braeuer, S., & Knackstedt, R. (2014). Integrating Regulatory Requirements into Information Systems Design and Implementation. Thirty Fifth International Conference on Information Systems. doi:10.1.1.685.9651

Carrier, B. (2003). Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers. International Journal of Digital Evidence, 1(4), 1-12.

CBS Denver. (2016). Denver Police Fire Shots To Test Wildly Successful 'ShotSpotter' System. Hämtad 2016-04-27, från http://denver.cbslocal.com/2016/04/23/denver-police-department-shotspotter-system/

Clavel, C., Ehrette, T., & Richard, G. (2005). EVENTS DETECTION FOR AN AUDIO-BASED SURVEILLANCE SYSTEM. 2005 IEEE International Conference on Multimedia and Expo, 1306-1309. doi: 10.1109/ICME.2005.1521669

Cronholm, S. & Goldkuhl, G. (2003). Strategies for Information Systems Evaluation Six Generic Types. Electronic Journal of Information Systems Evaluation, 6(2).

Datainspektionen. (2007). Ubiquitous Computing - en vision som kan bli verklighet. Hämtad 2016-04-27, från http://www.datainspektionen.se/Documents/rapport-ubiq-computing.pdf

Datainspektionen. (2016). EU:s dataskyddsreform. Hämtad 2016-04-20, från http://www.datainspektionen.se/lagar-och-regler/eus-dataskyddsreform/

Datainspektionen. (u.å. a). Inbyggd integritet. Hämtad 2016-04-28, från http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/inbyggd-integritet-privacy-by-design/

Datainspektionen. (u.å. b). Inbyggd integritet. Hämtad 2016-05-02, från http://www.datainspektionen.se/lagar-och-regler/kameraovervakningslagen/

European Commission. (2015). In the smart city of Santander the walls have ears. Hämtad 2016-04-12, från http://ec.europa.eu/research/infocentre/article_en.cfm?id=/research/star/index_en.cfm?p=sf-20150219-wallshaveears&calledby=infocentre&item=Infocentre&artid=33997

Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. (u.å.). Hämtad 2016-05-02, från http://www.manskligarattigheter.se/dm3/file_archive/020521/bb9e3648d3ba4bc99876ca6c6485a221/europa_501104.pdf

Finch, K., & Tene, O. (2015). Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town. Fordham Urban Law Journal, 41(5), 1581-1615.

Fu, K. K., Yang, M. C., & Wood, K. L. (2015). DESIGN PRINCIPLES: THE FOUNDATION OF DESIGN. 27th International Conference on Design Theory and Methodology.
doi:10.1115/DETC2015-46157

Galdon-Clavell, G. (2013). (Not so) smart cities?: The drivers, impact and risks of surveillanceenabled smart environments. Science and Public Policy, 40(6), 717-723.
doi: 10.1093/scipol/sct070

Gold, H. (2015, 17 Juli). ShotSpotter: gunshot detection system raises privacy concerns on campuses. The Guardian. Hämtad 2016-04-25, från http://www.theguardian.com/law/2015/jul/17/shotspotter-gunshot-detection-schools-campuses-privacy

Goode, E. (2012, 28 Maj). Shots Fired, Pinpointed and Argued Over. The New York Times. Hämtad 2016-04-25, från http://www.nytimes.com/2012/05/29/us/shots-heard-pinpointed-and-argued-over.html?_r=3&pagewanted=all

Helmius, I. (2000). Polisens rättsliga befogenheter vid spaning (Doktorsavhandling). Uppsala: Iustus Förlag.

Hevner, A. R., March, S. T., Park, J., & and Ram, S. (2004). Design Science in Information Systems Research. MIS Quarterly, 28(1), 75-105.

Karat, J., Karat, C., & Brodie, C. (2005). Why HCI research in privacy and security is critical now. International journal of human-computer studies, 63(1), 1–4.
doi:10.1016/j.ijhcs.2005.04.016

Langheinrich, M. (2001). Privacy by design - principles of privacy-aware ubiquitous systems. Lecture notes in computer science, 2201, 273 - 291.

Laudon, K. C., & Laudon J. P. (2011). Management information systems: managing the digital firm. New Jersey: Prentice Hall.

Li, S., Xu, L. D., & Zhao, S. (2014). The internet of things: A survey. Information systems frontiers, 17(2), 243-259.
doi:10.1007/s10796-014-9492-7

Lindblom, B. Nationalencyklopedin [NE]. (u.å.). Fonetik. Tillgänglig:
http://www.ne.se.ezproxy.its.uu.se/uppslagsverk/encyklopedi/l%C3%A5ng/fonetik

Little, L., Briggs, P., & Coventry, L. (2005). Public space systems: Designing for privacy?. International journal of human-computer studies, 63(1-2), 254–268.
doi:10.1016/j.ijhcs.2005.04.018

Maló, P. (2014, 29 oktober). Acoustic technologies: A niche of future European research and innovation [Blogginlägg]. Hämtad från https://ec.europa.eu/digital-single-market/blog/acoustic-technologies-niche-future-european-research-and-innovation

Malhotra, A., Gosain, S., & El Sawy, O. A. (2007). Leveraging Standard Electronic Business Interfaces to Enable Adaptive Supply Chain Partnerships. Information Systems Research, 18(3), 260-279.

Massey, A. K., Otto, P. N., Hayward, L. J., & Antón, A. .I (2010). Evaluating existing security and privacy requirements for legal compliance. Requirements engineering, 15(1), 119-137.
doi:10.1007/s00766-009-0089-5

Nationalencyklopedin [NE]. (u.å.). Offentlig plats. Tillgänglig:
http://www.ne.se.ezproxy.its.uu.se/uppslagsverk/encyklopedi/l%C3%A5ng/offentlig-plats

Nowack, M. L. (1997). DESIGN GUIDELINE SUPPORT FOR MANUFACTURABILITY. (Doktorsavhandling) Camerbridge: Department of Engineering.
Tillgänglig: https://www.repository.cam.ac.uk/handle/1810/251628

Ntalampiras, S., Potamitis, I., & Fakotakis, N. (2009). On acoustic surveillance of hazardous situations. 2009 IEEE International Conference on Acoustics, Speech and Signal Processing, 165-168.
doi: 10.1109/ICASSP.2009.4959546

Oates, B. J. (2006). Researching Information Systems and Computing.
London: SAGE Publications Ltd.

Otto, P. N., & Antón, A. I. (2007). Addressing legal requirements in requirements engineering. 15th IEEE International Requirements Engineering Conference (RE 2007), 5 - 14.
doi:10.1109/RE.2007.65

Pham, C., Cousin, P., & Carer A. (2014). Real-time On-Demand Multi-Hop Audio Streaming with Low-Resource Sensor Motes. Local Computer Networks Workshops (LCN Workshops), 2014 IEEE 39th Conference, 539 - 543.
doi: 10.1109/LCNW.2014.6927700

SFS 1960:729. Upphovsrättslagen. Stockholm: Justitiedepartementet.

SFS 1962:700. Brottsbalk. Stockholm: Justitiedepartementet.

SFS 1974:152. Kungörelse (1974:152) om beslutad ny regeringsform. Stockholm: Justitiedepartementet.

SFS 1984:387. Polislagen. Stockholm: Justitiedepartementet.

SFS 1994:1219. Lag (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna. Stockholm: Justitiedepartementet.

SFS 1998:204. Personuppgiftslag. Stockholm: Justitiedepartementet.

SFS 2007:978. Lag (2007:978) om hemlig rumsavlyssning. Stockholm: Justitiedepartementet.

SFS 2010:361. Polisdatalag. Stockholm: Justitiedepartementet.

SFS 2013:460. Kameraövervakningslag. Stockholm: Justitiedepartementet.

ShotSpotter. (2015). Los Altos scientist named Inventor of the Year. Hämtad 2016-04-14, från http://www.shotspotter.com/news/article/los-altos-scientist-named-inventor-of-the-year

ShotSpotter. (u.å.-a). Law enforcement. Hämtad 2016-04-14, från http://www.shotspotter.com/law-enforcement

ShotSpotter. (u.å.-b). History. Hämtad 2016-04-14, från http://www.shotspotter.com/company#history

ShotSpotter. (u.å.-c). ShotSpotter Flex Datasheet. Hämtad 2016-04-16, från http://www.shotspotter.com/system/content-uploads/ShotSpotter-Flex-Datasheet.pdf

ShotSpotter. (u.å.-d). SST, Inc. Privacy Policy. Hämtad 2016-04-16, från http://www.shotspotter.com/privacy-policy

ShotSpotter. (u.å.-e). Company Overview. Hämtad 2016-04-16, från http://www.shotspotter.com/company

SOU 2015:31. Datalagring och integritet: Betänkande av Datalagringsutredningen. Stockholm: Fritzes Offentliga Publikationer.

SOU 1970:85. Fotografering och integritet: Betänkande av integritetsskyddskommittén Stockholm: LiberTryck.

Ståhlbröst, A., Padyab, A., Sällström, A., & Hollosi, D. (2015). DESIGN OF SMART CITY SYSTEMS FROM A PRIVACY PERSPECTIVE. IADIS International Journal on WWW/Internet, 13(1), 1-16.

Ståhlbröst, A., Sällström, A., & Hollosi, D. (2014). AUDIO MONITORING IN SMART CITIES - AN INFORMATION PRIVACY PERSPECTIVE. 12th International Conference e-Society 2014.

Valentin Rehncrona, P. (2012). Immaterialrättens Grunder. Lund: Studentlitteratur AB.

Valenzise, G., Gerosa, L., Tagliasacchi, M., Antonacci, F., & Sarti, A. (2007). Scream and Gunshot Detection and Localization for Audio-Surveillance Systems. 2007 IEEE Conference on Advanced Video and Signal Based Surveillance, 21-26.
doi: 10.1109/AVSS.2007.4425280

Venable, J., Pries-Heje, J., & Baskerville, R. (2014). FEDS: a Framework for Evaluation in Design Science Research. European Journal of Information Systems, 25(1), 77–89.
doi:10.1057/ejis.2014.36

Ziegler, S. (2014). Privacy risk area assessment tool for audio monitoring - from legal complexity to practical applications. Journal of international commercial law and technology, 9(3), 138-147.

Bilagor

Bilaga 1: Hypotetiska designalternativ för ljudövervakningssystem

Första designalternativet

Det första designalternativet innebär att ljudövervakningssystemet aldrig spelar in ljud kontinuerligt, utan istället mäter ljudet på sådant sätt att ljud aldrig kan återgivas. Det är mätningarna som kring misstänksamma ljudepisoder skickas och lagras permanent.

Det första designalternativets inspirationskälla är Ståhlbröst et al. (2015) designprincip "Strömma data". Designprincipen innebär bland annat att inget ljud ska spelas in. Endast data relaterad till anmärkningsvärda händelser lagras.

Andra designalternativet

Det andra designalternativet innebär att ljudövervakningssystemet, i likhet med ShotSpotter, kontinuerligt spelar in ljud med en mikrofon. Ljudinspelningen lagras temporärt på sensorenheten och vid en misstänksam händelse skickas den aktuella ljudsekvensen till en kontrollcentral för permanent lagring.

Inspirationen till detta designalternativ kommer från ShotSpotters integritetspolicy. Genom att granska detta dokument förstod vi hur deras övervakningssystem fungerade på ett ytligt plan. (ShotSpotter, u.å.-d)

Tredje designalternativet

Det tredje designalternativet innebär att ljudövervakningssystemet kontinuerligt spelar in korta ljudsekvenser, alltså mindre än en sekund till maximalt några sekunder. Dessa sekvenser analyseras sedan temporärt i sensorn och jämförs mot en samling referensljud som också lagras på sensorn. I samband med analysen kategoriseras ljudet till olika typer av ljud, exempelvis skrik, skottlossning, oljud och så vidare. Därefter tas ljudet bort genom att ljudet snabbt skrivs över i minnet av nya ljudanalyser. Det som därefter behandlas av systemet är inga ljud utan endast kategorier.

Inspiration till detta designalternativ grundar sig i att vi ansåg att det fanns dåligt om praktiska lösningar för det första designalternativet och det andra designalternativet hade i intervjuerna bemötts med skepticism. Detta resulterade i att vi började leta efter en design där ljud kan kategoriseras utan att systemet spelar in ljud kontinuerligt, eller åtminstone minska intrånget på den personliga integriteten. Vi hittade ett antal lämpliga artiklar: Ntalampiras, Potamitis och Fakotakis (2009), Valenzise, Gerosa, Tagliasacchi, Antonacci och Sarti (2007) och Clavel, Ehrette och Richard (2005). Dessa artiklar testade eller föreslog olika metoder för att kategorisera ljud, exempelvis skott, genom att spela in korta ljudklipp som därefter analyseras och kategoriseras.

Bilaga 2: Exempel på använd intervjuguide

Inledning

Introduktion och kort bakgrund

Vi pluggar systemvetenskap på Uppsala Universitet och genomför just nu vårt examensarbete inom ämnesområdet Informatik. Informatik är ett vetenskapligt ämnesområde där användning, utformning och tillämpning av IT studeras. Vi ska designa och utveckla ett informationssystem för övervakning av ljud på allmänna platser som följer svensk lagstiftning. Informationssystemet fungerar på så sätt att misstänksamma ljud uppmärksammas och visualiseras på en karta, tillsammans med övrig information om händelsen.

Premisser

Vi vill påminna att deltagande i den här intervjun är frivilligt och intervjun kan avbrytas när som helst. Resultatet av intervjun behandlas på sådant sätt att du inte nämns vid namn. Syftet med våra intervjuer är att ta reda på vilka lagar och paragrafer som kan vara aktuella för det system vi utvecklar och hur dessa kan tolkas. Intervjuerna kommer transkriberas och sammanfattas. Det som slutligen publiceras i uppsatsen är sammanfattningar och citat från intervjuerna. Utifrån resultaten av våra intervjuer sammanställer vi de juridiska förutsättningar som finns för informationssystemet och anpassar vår systemdesign utifrån dessa förutsättningar.

- Är dessa premisser okej?
- Är det okej att vi spelar in intervjun?

Inledande frågor

- Vad har du för befattning?
- Kan du berätta lite om din bakgrund inom juridik?
- (Om ej besvarad: Är du specialiserad inom vissa områden? Om ja, vilka?)

Översikt

Vi har strukturerat intervjun i fyra delar. De tre första delarna gäller juridiska förutsättningar för tre olika scenarion. Dessa tre scenarion omfattar tre skilt utformade informationssystem för ljudövervakning.

I den fjärde delen tar vi upp övriga frågor.

Vi kommer läsa frågorna exakt som de är skrivna så det finns risk för att det kan bli lite monotont. Vi har en hel del frågor så vi fortsätter så länge tiden räcker.

Del 1 - Scenario 1

Bakgrund

Vid svar på de kommande frågorna utgår vi ifrån att systemet kontinuerligt spelar in ljud med en mikrofon. Ljudinspelningen lagras temporärt på sensorenheten och vid en misstänksam händelse skickas den aktuella ljudsekvensen till hemsidan för permanent lagring. Denna ljudsekvens bedöms av övervakningspersonal, eller liknande.

- Har du frågor kring denna beskrivning?

Frågor

- Vårt system kommer alltså samla in data i form av ljudupptagningar på allmän plats. Vad gäller för denna insamling?

- Vårt system kommer efter insamling att bearbeta ljuddatan genom att analysera ifall ljudet är misstänksamt. Ifall det är misstänksamt skickas ljuddatan vidare till en webbserver, det vill säga en hemsida. Vad gäller för denna bearbetning?

- Vår hemsida kommer motta ljuddata från övervakningsplatserna och lagra datan i en databas. Det vill säga, man lagrar ljuddatan strukturerat. Vad gäller för den här typen av lagring?

- Vår hemsida kommer därefter distribuera datan till sina användare. Vad gäller för den här typen av distribution av data?

Om ej redan besvarade

- Kan en inspelning av någons röst i det här scenariot hänföras direkt eller indirekt till en person?
  - Om ja, spelar det någon roll hur lång inspelningen är? Exempelvis om den är 1 sekund eller 200 millisekunder etc.
  - Är det en personuppgift?
  - Om ja, ostrukturerat eller strukturerat material?

- Är 2 kap. 6§ Regeringsformen och åttonde artikeln i EKMR aktuella?

Del 2 - Scenario 2

Bakgrund

Vid svar på de kommande frågorna utgår vi ifrån att systemet kontinuerligt spelar in korta ljudsekvenser, alltså mindre än en sekund till maximalt några sekunder. Dessa sekvenser analyseras sedan temporärt i sensorn och jämförs mot en samling referensljud som också lagras på sensorn. I samband med analysen kategoriseras ljudet till olika typer av ljud, exempelvis skrik, skottlossning, oljud etc. och därefter tas ljudet bort. Ljudet skrivs snabbt över i minnet av nya ljudanalyser. Det som skickas till hemsidan är alltså inget ljud utan endast en kategorisering.

- Har du frågor kring denna beskrivning?

Frågor

- Vårt system kommer alltså samla in data i form av korta ljudinspelningar på allmän plats. Vad gäller för denna insamling?

- Vårt system kommer efter insamling att bearbeta datan genom att analysera och kategorisera ljudet. Ifall kategorin räknas som misstänksam skickas den tillsammans med tidpunkt och plats för avläsning vidare till en webbserver, det vill säga en hemsida. Alltså: Inget ljud skickas någonsin från sensorerna. Vad tror du gäller för denna bearbetning?

- Vid insamlingen lagras först korta ljudsekvenser temporärt på sensorn. Ljudsekvensen kategoriseras på sensorn och det är alltså själva kategorin som skickas och lagras permanent på hemsidan. Ljudsekvensen skrivs över (tas bort) så snart ljudet kategoriserats och nya ljudsekvenser spelas in. Vad tror du gäller för den här typen av lagring?

- Vår hemsida kommer därefter distribuera de mottagna misstänksamma avläsningarna (det vill säga kategori, plats och tidpunkt) till sina användare. Vad tror du gäller för den här typen av distribution av data?

Om ej redan besvarade

- Kan en inspelning av någons röst i det här scenariot hänföras direkt eller indirekt till en person?
  - Om ja, spelar det någon roll hur lång inspelningen är? Exempelvis om den är 1 sekund eller 200 millisekunder etc.
  - Är det en personuppgift?
  - Om ja, ostrukturerat eller strukturerat material?
  - Om ostrukturerat - Är polisdatalagen tillämplig?
  - Om ja, är det fortfarande en personuppgift när endast kategorierna lagras på hemsidan?

- Är 2 kap. 6§ Regeringsformen och åttonde artikeln i EKMR aktuella?

Del 3 - Scenario 3

Bakgrund

Vi tänker oss nu istället att vi utgår ifrån att informationssystemet aldrig spelar in ljud utan endast mäter ljudet på ett sådant sätt att det aldrig går att återgiva. Det är information om mätningen som, kring misstänksamma ljudepisoder, kommer skickas och lagras permanent på hemsidan.

- Har du frågor kring denna beskrivning?

Frågor

- Skiljer sig rättsläget något sen tidigare när det kommer till insamling, bearbetning, lagring och distribution av data?

Del 4 - Avslutning

- Har myndigheter särskilda lagar och regler inom vårt område?
  - Exempelvis personuppgiftsbehandling inom polisen.

- Om PUL är tillämplig, går det att kringgå kraven på upplysning och samtycke för personuppgiftsbehandling?

Sammanfatta intervjun ihop med intervjuobjekt

- Har du några övriga kommentarer eller frågor?

Bilaga 3: Beskrivning av teman

Tema (Förkortning)	Beskrivning
Europakonventionen (EKMR)	Avser data som kan relateras till bestämmelser i europakonventionen.
Regeringsformen (RF)	Avser data som kan relateras till bestämmelser i regeringsformen.
Personuppgiftslagen (PUL)	Avser data som kan relateras till bestämmelser i personuppgiftslagen. Avser även data som kan relateras till personuppgifter som nämns i samband med personuppgiftslagen.
Polisdatalagen (PDL)	Avser data som kan relateras till bestämmelser i polisdatalagen. Avser även som kan relateras till personuppgifter som nämns i samband med polisdatalagen.
Kameraövervakningslagen (KÖL)	Avser data som kan relateras till kameraövervakningslagen.
Upphovsrättslagen (URL)	Avser data som kan relateras till upphovsrättslagen.
Brottsbalken (BrB)	Avser data som kan relateras till bestämmelser i brottsbalken.
Rättegångsbalken (RB)	Avser data som kan relateras till rättegångsbalken.
Ordningslagen (OL)	Avser data som kan relateras till ordningslagen.
Röstidentifikation	Avser data som kan relateras till röstidentifikation. Det vill säga om personer kan identifieras utifrån röster.
Sekretess	Avser data som kan relateras till bestämmelser angående sekretess mellan myndigheter.
Rättsläge	Avser data som beskriver rättsläget ur en generell synvinkel och inte relaterad till en specifik lag.

Bilaga 4: Utvärderingsplan

Utvärderingstyp: Kriteriebaserad utvärdering.
Tillvägagångssätt: Intervju med ämnesexpert.
Ämnesexpert: Jurist med goda kunskaper inom aktuella rättsområden.
Kriterier för utvärdering: Tillförlitlighet och fullständighet. (Nowack, 1997)
Definition av kriterier:

- *Tillförlitlighet*
  Med tillförlitlighet avses hur troligt det är att uppnå ett förväntat resultat vid tillämpning av de framtagna riktlinjerna. Tillförlitligheten ska förhindra att design blir felaktig, det vill säga att tillämpade riktlinjer resulterar i ett system som strider mot rådande svensk lagstiftning.

  Indikation på tillförlitlighet:
  Riktlinjerna är att anses som tillförlitliga om utvärderingsexpert ej hittar brister i riktlinjerna.

- *Fullständighet*
  Med fullständighet avses ifall de framtagna riktlinjerna täcker alla möjliga juridiska problem. Genom att undersöka fullständighet minskas risken att viktiga problem, i vårt fall lagar, förbises.

  Indikation på fullständighet:
  Riktlinjerna är att anses som fullständiga ifall det inte framkommer nya lagar eller juridiska aspekter under utvärderingen.