

Perception och acceptans för integritetskränkande säkerhetsåtgärder

Björn Sildemark

Department of Fire Safety Engineering and Systems Safety
Lund University, Sweden

Brandteknik och Riskhantering
Lunds tekniska högskola
Lunds universitet

Report 5362, Lund 2011

**Perception och acceptans för integritetskränkande
säkerhetsåtgärder**

Björn Sildemark

Lund 2011

Perception and acceptance of privacy-invasive security measures
Perception och acceptans för integritetskränkande säkerhetsåtgärder

Björn Sildemark

Report 5362

ISSN: 1402-3504

ISRN: LUTVDG/TVBB--5362--SE

Number of pages: 77

Keywords

Privacy, security technology, acceptance, risk perception.

Sökord

Personlig integritet, säkerhetsteknik, acceptans, riskperception.

Abstract

This is a thesis report for the Master's program in Risk Management and Safety Engineering at Lund University. It is also a part of the research project *Assessing acceptance of privacy-invasive ICT Solutions* at the Royal Institute of Technology. Its aim is to examine how the perception and acceptance of privacy-invasive technology is determined by demographics, context and cognitive factors. The main focus of the report is on public risk management with the use of technical security measures. First, an extensive literature review on the areas of privacy and risk perception is made in order to obtain a comprehensive and objective picture of the current state of research. This knowledge is then used to formulate hypotheses that are used to analyze the data from an already completed survey. The analyses are performed by the use of statistical methods in the computer software SPSS Statistics. These tests provide support for a connection between whether respondents have children or not, and how acceptable they find the security technologies to be. It's not possible to observe any differences between the sexes, and there is a weak, albeit not statistically significant, correlation with age. Furthermore, it is clear that the cognitive factors studied shows strong correlation with acceptance and perception of privacy-invasive security measures. Finally, the design of the survey and the results are discussed. Overall, it is noted that it is difficult to draw any conclusions from the results until further studies have been carried out.

© Copyright: Brandteknik och Riskhantering, Lunds tekniska högskola, Lunds universitet, Lund 2011.

Brandteknik och Riskhantering
Lunds tekniska högskola
Lunds universitet
Box 118
221 00 Lund

brand@brand.lth.se
<http://www.brand.lth.se>

Telefon: 046 - 222 73 60
Telefax: 046 - 222 46 12

Department of Fire Safety Engineering
and Systems Safety
Lund University
P.O. Box 118
SE-221 00 Lund
Sweden

brand@brand.lth.se
<http://www.brand.lth.se/english>

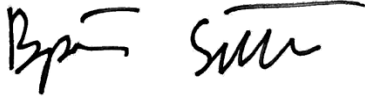
Telephone: +46 46 222 73 60
Fax: +46 46 222 46 12

FÖRORD

För deras hjälp vid tillkomsten av den här rapporten riktar jag tack till:

Misse Wester, min bonushandledare, som gav mig möjlighet att avsluta min utbildning med att genomföra examensarbetet inom ett område som verkligen engagerar mig!

Marcus Abrahamsson, min handledare, som bidragit med värdefull återkoppling.

A handwritten signature in black ink, consisting of the first name 'Björn' and the last name 'Sildemark' written in a cursive style.

Björn Sildemark
Lund, 17 februari 2011

TERMINOLOGILISTA

<i>Avslöjad preferens</i>	Metod där man studerar konsumentmönster för att avgöra vilka preferenser som människor har i praktiken (Varian, 2006).
<i>Demografi</i>	Vetenskap som studerar befolkningens storlek, sammansättning och geografiska fördelning samt förändringar i befolkningsstrukturen förorsakade av demografiska händelser. Centrala indelningsvariabler är ålder, kön, civilstånd, boenderegion och etnisk tillhörighet (Nationalencyklopedin 4).
<i>F. ö.</i>	Författarens översättning.
<i>Kognitiv</i>	Som avser kognition (tankefunktioner med vilkas hjälp information och kunskap hanteras), kunskap, förstånd eller information (Nationalencyklopedin 5).
<i>Kontext</i>	Det språkliga sammanhang som ett ord eller ett yttrande ingår i, utvidgat även gällande social situation (Nationalencyklopedin 6).
<i>Riskperception</i>	Hur individer upplever och bedömer olika risker (Riskkollegiet, 1993).
<i>Risk denial</i>	Ett fenomen som innebär att individer genomgående bedömer den egna risken som mindre än övriga befolkningens (Sjöberg, 2000).
<i>RFID</i>	Radio Frequency IDentification. Samlingsbegrepp för flera metoder att identifiera personer eller ting med hjälp av radioteknik (Nationalencyklopedin 7).
<i>SPSS</i>	Ett statistiskt programpaket för att hantera data och tillämpa statistiska metoder (SPSS).
<i>Uttalad preferens</i>	Metod där man explicit ställer frågor om vilka preferenser respondenterna har (Kroes & Sheldon, 1988).
Scenarier	
<i>CCTV</i>	Övervakningskameror (scenario 2-1 respektive 2-2).
<i>DNA</i>	DNA-lagring (6-1 respektive 6-2).
<i>Mejl</i>	Mejlfilter (4-1 respektive 4-2).
<i>Mobpos</i>	Mobiltelefonpositionering (3-1 respektive 3-2).
<i>Retina</i>	Näthinnefotografering (1-1 respektive 1-2).
<i>RFID</i>	5-1 respektive 5-2.

SAMMANFATTNING

Denna rapport utgör examensarbete på Riskhanteringsprogrammet vid LTH, och ingår dessutom i forskningsprojektet *Assessing acceptance of privacy-invasive ICT solutions* vid Kungliga tekniska högskolan.

Rapporten syftar till att undersöka hur perception och acceptans för integritetskränkande teknik beror på demografi, kontext och kognitiva faktorer. Fokus ligger på offentlig riskhantering med hjälp av tekniska säkerhetsåtgärder.

Först utförs en omfattande litteraturstudie på områdena personlig integritet och riskperception för att erhålla en heltäckande och i största möjliga utsträckning objektiv bild av nuvarande forskningsläge. Denna kunskap används sedan för att formulera hypoteser som används för att analysera data från en inom projektet redan genomförd enkätstudie. Analyserna sker med hjälp av statistiska metoder i datorprogrammet SPSS.

Resultaten av analyserna visar att det går att finna stöd för ett samband mellan huruvida respondenterna har barn och vilken acceptans de uppger för teknologierna. Det går inte att fastställa några skillnader mellan kön, och det föreligger ett svagt samband med ålder som dock inte är statistiskt signifikant. Vidare kan det konstateras att de kognitiva faktorer som studeras uppvisar ett starkt samband med acceptans och perception för integritetskränkande säkerhetsåtgärder. Slutligen diskuteras studiens utformning och erhållna resultat. Sammantaget konstateras det att det är svårt att dra några slutsatser utifrån resultaten förrän vidare studier har genomförts.

INNEHÅLLSFÖRTECKNING

1	Inledning	1
1.1	Bakgrund	1
1.2	Syfte och mål.....	1
1.3	Frågeställningar	2
1.4	Avgränsningar	2
1.5	Begränsningar	2
2	Metod.....	3
2.1	Litteraturstudie	3
2.2	Hypotesformulering	3
2.3	Enkätstudie.....	4
2.4	Statistiska metoder och verktyg	4
2.4.1	Mann-Whitneys U-test	4
2.4.2	Kruskal Wallis test	5
2.4.3	IBM SPSS Statistics 19	5
3	Litteraturstudie.....	7
3.1	Integritet.....	7
3.1.1	Definition av integritet.....	8
3.1.2	Värdet av integritet	10
3.1.3	Integritet och autonomi.....	11
3.2	Riskperception.....	11
3.2.1	Vad riskperception är.....	12
3.2.2	Faktorer i riskperception.....	13
3.2.3	Riskperceptionens dimensioner.....	15
4	Hypotesformulering.....	17
4.1	Demografiska faktorer	17
4.2	Kontextuella faktorer.....	17
4.3	Kognitiva faktorer	18
5	Enkätstudie	19
5.1	Scenarier.....	19
5.1.1	Näthinnefotografering (Retina)	19
5.1.2	Övervakningskameror (CCTV)	19
5.1.3	Mobiltelefonpositionering (Mobpos)	20
5.1.4	Mejlfilter (mejl)	20
5.1.5	RFID.....	20

5.1.6	DNA-lagring (DNA)	21
5.2	Resultat	22
5.2.1	Acceptans	22
5.2.2	Efterfrågan	31
5.2.3	Frivillighet	38
5.2.4	Fördelar/nackdelar	46
5.2.5	Tillit/missbruk	53
6	Analys	61
6.1	Demografiska faktorer	61
6.1.1	Kön	62
6.1.2	Föräldraskap	63
6.1.3	Ålder	65
6.2	Kontextuella faktorer	66
6.3	Kognitiva faktorer	67
7	Diskussion	71
7.1	Utförande	71
7.2	Förslag	72
8	Slutsatser	73
9	Källförteckning	75
	Bilaga A – Enkätfrågor	i
	Bilaga B – Statistiska metoder	iii
	Icke-parametriska test	iii
	Mann-Whitneys U-test	iii
	Kruskal-Wallis test	iii

1 INLEDNING

Denna rapport ingår i kursen Examensarbete i riskhantering (VBR920) som utgör avslutningen på civilingenjörsprogrammet i riskhantering vid Lunds tekniska högskola. Kursen omfattar 30 högskolepoäng vilket motsvarar 20 veckors heltidsstudier.

1.1 BAKGRUND

Människor är i stor utsträckning beroende av tjänster som baseras på informationsteknik. För att kunna använda dessa måste man ofta uppge personuppgifter såsom ålder, kön, inkomst, medborgarskap, personnummer och så vidare. I vissa fall krävs dessutom biometrisk data såsom fingeravtryck eller näthinnefotografering. Att övervaka och lagra information om individer är inte något nytt fenomen. Två saker har dock förändrats markant på senare tid: För det första lagras det betydligt mycket mer information nuförtiden och för det andra analyseras informationen i allt större utsträckning istället för att endast lagras (Lyon, 2007). Det verkar troligt att de här trenderna kommer öka i framtiden i och med den ökande användningen av informationsteknik i allmänhet och användningen för säkerhetsändamål, såsom bekämpning av terrorism och epidemier, i synnerhet.

Tekniken kan ge stora fördelar då det bland annat kan underlätta för hälsovårdsmyndigheter att minska spridningen av farliga sjukdomar, möjliggöra snabb åtkomst till passagerarlistor vid haverier för att underlätta eftersök och identifiering samt ge snabb informationsspridning till en stor mängd människor efter katastrofhändelser.

Det finns dock en oro bland allmänheten för användningen - särskilt vad gäller säkerheten kring den lagrade informationen. Farhågorna rör allt från att konsumentmönster avslöjas till tredje part, till att känslig eller direkt skadlig information offentliggörs. Många människor är oroliga för att personlig information kan överföras till obehöriga genom exempelvis stöld, felaktig användning, datorintrång eller olyckshändelser (Culnan & Armstrong, Organization Science). Informationssäkerhet är alltså av stor betydelse för allmänhetens perception och acceptans för ny informationsteknik. Det är dock inte känt i vilken utsträckning allmänheten är medveten om hoten mot informationssäkerhet. Det är tänkbart att människor undervärderar likväl som övervärderar dessa. Framför allt ter det sig troligt att attityderna till tekniken kan bero på demografiska faktorer så som ålder och kön.

Därför anses det intressant, ur både medborgarnas och myndigheternas perspektiv, att klarlägga hur acceptansen och perceptionen för sådana integritetskränkande, eller potentiellt integritetskränkande, åtgärder skiljer sig utifrån demografi och kontext. I en demokrati som Sverige är det viktigt att myndigheter och politiker tar beslut som baseras på en riktig uppfattning om hur allmänhetens inställning ser ut. I och med att det ofta kan vara svårt eller praktiskt omöjligt att välja alternativa tekniker kan inte användningen av en teknik likställas med acceptans för densamma.

Förutom att utgöra examensarbete för Riskhanteringsprogrammet vid LTH ingår denna rapport som en del i forskningsprojektet *Assessing acceptance of privacy-invasive ICT solutions* som genomförs vid Kungliga tekniska högskolan (KTH) i Stockholm, med hjälp av finansiering från dåvarande Krisberedskapsmyndigheten (KBM), nuvarande Myndigheten för samhällsskydd och beredskap (MSB).

1.2 SYFTE OCH MÅL

Syftet med examensarbetet är att studenten skall utveckla och visa sådan kunskap och förmåga som krävs för att självständigt arbeta som civilingenjör. Särskilt ska studenten visa förmåga att tillämpa och sammanställa kunskaper och färdigheter förvärvade inom olika centrala och kvalificerade kurser inom det aktuella

utbildningsprogrammet. Särskilt syftar detta examensarbete till att bidra med kunskaper till forskningsprojektet inom vilket det ingår och bidra med rekommendationer för vidare studier på området.

Målet med detta examensarbete är att kartlägga och presentera allmänhetens uppfattning om och acceptans för olika typer av informations- och kommunikationsteknik som kan anses vara integritetskränkande. Särskilt ämnar det att undersöka om vedertagna modeller och iakttaganden gällande riskperception skulle kunna gå att överföra på integritetsforskning genom att analysera data från en genomförd enkätundersökning.

1.3 FRÅGESTÄLLNINGAR

Målet konkretiseras i ett antal frågeställningar:

- Hur ser allmänhetens inställning till olika typer av integritetskränkande teknik ut?
- Finns det demografiska skillnader i acceptans och perception för integritetskränkande teknik?
- Vilka situationsspecifika omständigheter kan sägas ha betydande inverkan på acceptans och perception för integritetskränkande teknik?
- Går det att dra paralleller mellan den så kallade psykometriska modellen för riskperception och allmänhetens inställning till integritetskränkande teknik?

I slutändan är det dessa frågeställningar som rapporten ska besvara.

1.4 AVGRÄNSNINGAR

Rapporten riktar in sig på offentlig riskhantering med hjälp av säkerhetsteknik och därmed ligger fokus på ett myndighetsperspektiv.

1.5 BEGRÄNSNINGAR

Arbetet genomförs med ett redan befintligt dataunderlag varför författaren inte har haft möjlighet att vara involverad i framtagningen av detta.

2 METOD

Eftersom det finns vissa fastställda krav på examensarbetets form och på grund av att en redan genomförd enkätstudie ligger till grund för uppsatsen så faller sig metodvalet ganska naturligt. Arbetet delas in i ett antal olika moment:

- Inledningsvis genomförs en litteraturstudie.
- Utifrån kunskap inhämtad under litteraturstudien formuleras hypoteser som är till för att användas vid analysen av det statistiska materialet.
- Det råmaterial som finns från en enkätstudie sammanställs, presenteras och tolkas.
- De framtagna resultaten analyseras med hjälp av de hypoteser som tidigare formulerats.
- En omfattande diskussion förs med syfte att reflektera över resultat och valda metoder.
- Dokumentation sker löpande under arbetets gång.

Tack vare tillgången till en redan genomförd undersökning behöver ingen ny enkät utformas. Detta kan visserligen ses som en nackdel då studenten går miste om erfarenhet av detta moment, men det har vägts mot fördelen av att ha tillgång till data av både hög kvalitet och stor kvantitet. Sammantaget anses detta över-skugga eventuella nackdelar med upplägget. Därför läggs också stor vikt vid att kritiskt reflektera över huruvida den befintliga studiens utformning är lämplig eller om den kunde gjorts annorlunda.

2.1 LITTERATURSTUDIE

I syfte att teckna en bred och i största möjliga mån objektiv bild av ämnet genomförs en för examensarbetet obligatorisk och omfattande referenssökning och litteraturstudie. Litteraturgranskningsfasen fyller flera funktioner: Förutom tidigare nämnda generella orientering så visar den hur begrepp definieras, vilka metoder som är etablerade och som använts i tidigare undersökningar samt hur resultaten från dessa studier tolkats. Inte minst kan eventuella svagheter i tidigare forskning identifieras (Backman, 2010). Källor erhålls huvudsakligen på tre olika sätt:

- Undersökning av för projektet tidigare samlade artiklar och andra källor.
- Uppföljning av referenserna i relevanta och användbara källor.
- Genomsökning av vetenskapliga artikeldatabaser med hjälp av relevanta sökord.

Utifrån frågeställningarna kan två mål med litteraturstudien identifieras: För det första att få en bred och översiktlig bild av forskningsområdet för personlig integritet. För det andra att fördjupa sig i ämnet riskperception, och då särskilt forskning som rör den psykometriska förklaringsmodellen.

2.2 HYPOTESFORMULERING

Utifrån vad som framkommer under litteraturstudien konkretiseras frågeställningarna och hypoteser formuleras, vilka sedan prövas mot det studiematerial som finns tillgängligt. Syftet med dessa hypoteser är att undersöka hur attityder gällande integritetskränkande teknikanvändning förhåller sig till den psykometriska modellen för riskperception (Fischhoff, Slovic, Lichtenstein, Read, & Combs, 1978). En hypotes är, till skillnad från frågeställningen, formulerad som ett potentiellt och preliminärt svar på en fråga. Ytterligare en skillnad mot frågeställningen är att hypoteserna behöver ha någon sorts anknytning till tidigare forskning (Backman, 2010). Därför tas från litteraturen relevanta påståenden om riskperception ut. Dessa måste naturligtvis också vara praktiskt användbara på den genomförda undersökningen.

2.3 ENKÄTSTUDIE

En enkätstudie är exempel på ett arbetssätt som används inom kvantitativ metod, vilket betyder ett vetenskapligt arbetssätt i vilket man under systematiska former samlar in empiriska och kvantifierbara data, sammanställer dessa i statistisk form och sedan analyserar resultatet utifrån formulerade hypoteser. Arbetet är strikt formaliserat. Sådana metoder är i princip ett krav då stora populationer studeras, och objektiviteten anses öka då forskaren inte själv deltar i det som studeras (Nationalencyklopedin 1). Därför bedöms detta vara ett lämpligt förfaringssätt för att studera det valda ämnet.

Då studenten har tillgång till en omfattande och redan genomförd enkätundersökning inom projektets ramar så anses det rimligare att arbeta med detta material än att genomföra en egen studie. Materialet utgörs dock av rådata varför viss behandling är nödvändig. Efter sammanställningen presenteras och analyseras statistiken och hypoteserna prövas, därefter tolkas resultaten. Eftersom enkäten inte är utformad av studenten läggs stor vikt vid att ingående diskutera huruvida utformningen är lämplig eller om den hade kunnat förbättras på något vis. I detta läge är det snarast en fördel att studenten inte deltagit i dess framställning.

2.4 STATISTISKA METODER OCH VERKTYG

För att behålla eller förkasta hypoteserna räcker det inte med att jämföra medelvärden från stickprovsdata. Man måste då också ta hänsyn till variansen och antalet respondenter genom att beräkna statistisk signifikans. Även om medelvärdena skiljer sig åt kan skillnaden vara så liten att den kan tänkas bero på slumpmässig varians, varför den inte kan anses vara statistiskt säkerställd med hänsyn till antalet respondenter. Därför används statistiska metoder för hypotesprövning med syfte att kontrollera huruvida sådana signifikanta skillnader föreligger (Körner & Wahlgren, 2006).

Statistisk hypotesprövning utgör en metod där man använder olika typer av statistiska metoder för att empiriskt pröva hypoteser mot statistiska modeller. Eftersom slumpmässig varians kan ha en mer eller mindre utpräglad effekt på resultat görs slutsatser med ett visst mått av statistisk osäkerhet. Prövningen kan både undersöka om data passar en viss statistisk modell men också huruvida en parameter har ett specifikt värde. Den senare metoden används vid analysen av resultaten i denna rapport.

Signifikanstest avgör huruvida ett observerat utfall är sannolikt givet att en formulerad vetenskaplig hypotes stämmer. En signifikansnivå väljs på förhand, vanligtvis 0,05. Om det visar sig att sannolikheten för att erhålla det observerade utfallet (givet att hypotesen stämmer) understiger signifikansnivån innebär detta att hypotesen förkastas. Ju lägre signifikansnivå som väljs, desto större avvikelse krävs för att förkasta hypotesen (Nationalencyklopedin 2).

De olika statistiska metoder som har använts redovisas översiktligt nedan. Beskrivningar av hur de fungerar rent matematiskt redovisas i Bilaga B – Statistiska metoder.

2.4.1 MANN-WHITNEYS U-TEST

Även kallad Wilcoxons rangsummatest. Används då två oberoende stickprov analyseras, i praktiken exempelvis för att undersöka huruvida olika respondentgrupper svarat likvärdigt på en fråga. Nollhypotesen innebär att de båda populationerna ur vilka stickproven har tagits inte skiljer sig fördelningsmässigt. Mothypotesen innebär att det föreligger en sådan skillnad, och att det alltså är större sannolikhet att få högre värden ur den ena av populationerna än den andra. Detta test används i rapporten för att undersöka demografiska skillnader i form av kön och vid analys av kontextuella faktorer. I båda fallen jämförs svaren från två olika grupper av respondenter, varför stickproven räknas som oberoende (Körner & Wahlgren, 2006).

2.4.2 KRUSKAL WALLIS TEST

Ensidig variansanalys med rangtal, som det också kallas, är en generalisering av rangsummatest av två oberoende stickprov. I likhet med rangsummatest av två stickprov är nollhypotesen att stickproven kommer från identiska populationer, med skillnaden att det istället handlar om k stickprov från k populationer. Mothypotesen innebär att det föreligger skillnader. Metoden används i den här rapporten för att undersöka huruvida det finns statistiskt signifikanta skillnader i svarsresultaten från olika åldersgrupper (Körner & Wahlgren, 2006).

2.4.3 IBM SPSS STATISTICS 19

De rådata som används är lagrad i ett format som är kompatibelt med programpaketet SPSS. Det är också detta statistikprogram som används vid framtagning av data och analys av resultaten, i form av bland annat de statistiska test som redovisas tidigare. Samtliga statistiska test i rapporten är alltså utförda med hjälp av SPSS.

Programnamnet SPSS stod ursprungligen för *Statistical Package for the Social Sciences* och utvecklades av tre doktorander vid Stanford University. Första versionen släpptes 1968 och året därpå flyttades utvecklingen till University of Chicago. Programmet blev snabbt populärt i den akademiska världen, och när det sedermera började spridas till organisationer och privata företag kommersialiserades programmet som ett fristående företag. Under en kort period hette programmet *PASW Statistics*, men i och med ett uppköp av IBM är det officiella namnet nu *IBM SPSS Statistics*. Det är ett integrerat mjukvarupaket med verktyg skapat främst för att analysera data inom samhällsvetenskaperna. Det erbjuder ett stort antal statistiska test och olika sätt att hantera statistisk data varför det blivit ett av de populäraste programmen för statistisk analys (SPSS).

3 LITTERATURSTUDIE

Denna rapport behandlar områdena personlig integritet och riskperception, varför litteraturstudien främst syftar till att introducera och beskriva dessa två begrepp på ett sätt som bidrar med både förståelse och bakgrund.

3.1 INTEGRITET

Människor kan delas upp i tre olika grupper beroende på sin inställning till den personliga integriteten: fundamentalister, obekymrade och pragmatiker. Fundamentalisterna är väldigt skeptiskt inställda till alla förändringar som medför integritetskränkningar oavsett vilka eventuella fördelar som kommer med dem. Personer i den obekymrade gruppen är tvärtom villiga att tillgängliggöra personlig information utan att detta behöver motiveras i någon större utsträckning. Slutligen finns gruppen pragmatiker som är villiga att uppge personlig information endast om de tycker att risken och fördelarna sammantaget motiverar detta. Fram till sekelskiftet utgjorde den pragmatiska gruppen 55 procent av befolkningen samtidigt som de andra grupperna utgjorde 25 (fundamentalister) respektive 20 procent (obekymrade). År 2000 skedde dock en större förändring då pragmatikerna visserligen låg kvar på ungefär samma nivå med 58 procent men där de obekymrade minskade till 8 procent samtidigt som fundamentalisterna ökade till 34 procent (Westin, 2003). Uppenbarligen har alltså något hänt som fått allmänheten att i högre grad ifrågasätta effekterna av det informationssamhälle som håller på att växa fram.

I och med en accelererande samhällsutveckling på området informations- och kommunikationsteknik har uttrycket integritet allt oftare hamnat i fokus på senare tid. IPRED-lagen, signalspaningslagen, EU:s datalagringsdirektiv och frågan om övervakningskameror i det offentliga rummet är några exempel på ämnen som skapat intensiv debatt på senare år (Datainspektionen, 2009). Tre aktuella samhällsomdaningar kan sägas driva den här utvecklingen:

Den aktuella debatten speglar bara toppen av isberget som digitaliseringen av samhället utgör. Under ytan pågår ett febrilt arbete bland svenska offentliga förvaltningar för att rationalisera och uppnå målet om *24-timmarsmyndigheten* som syftar till att ge medborgarna ständig tillgång till offentliga tjänster och kontakt med myndigheter. Eftersom detta ofta bygger på användandet av informationsteknologi ställs allt högre krav på informationssäkerhet då det involverar ökade risker i form av bland annat identitetsstöld, bedrägeri och *data mining* – datautvinning (Palm & Wester, 2010).

Samtidigt har kriget mot terrorismen medfört en diskurs som tillåter urholkning av medborgerliga rättigheter till förmån för säkerhetsåtgärder som syftar till att bekämpa terrorism men också grövre konventionell brottslighet (European Parliamentary Technology Assessment, 2006). Krig innebär kristillstånd, och kristillstånd innebär att särskilda åtgärder kan motiveras. Vad som kunnat skönjas på senare tid är således framväxandet av en säkerhetsstat där kristillståndet har övergått till vardag och övervakningen alltmer syftar till att verka förebyggande (Lyon, 2007). Underrättelseverksamhetens premierande av stora volymer information för att ingenting viktigt ska förbli oupptäckt kommenteras av Gary T. Marx (författarens översättning): *”Underrättelserollen kan definieras på ett sätt som skapar en omätlig aptit på information, samtidigt som åtgärder baserade på den insamlade informationen begränsas”* (1988). Denna utveckling påvisades med all önskvärd tydlighet när den välrenommerade tidningen *The Washington Post* presenterade sin tvååriga kartläggning av den amerikanska underrättelseverksamheten som växt till oöverträffade proportioner de senaste nio åren. Granskningen sammanfattas med (f. ö.):

Den topphemliga värld som regeringen skapade som svar på terroristattacker den elfte september 2001 har blivit så stor, så tungrodd och så hemlig att ingen vet exakt hur mycket pengar den kostar, hur

många personer den sysselsätter, hur många program som existerar inom den eller exakt hur många organisationer som gör samma jobb. (The Washington Post)

Risken med denna utveckling är att stora mängder information samlas in i onödan och att informationen sedan istället används i andra syften än vad den var menad för från början, dels genom praktiskt taget oundvikliga misstag men även på grund av ändamålsglidning och missbruk. Ett aktuellt exempel på detta är FRA:s signalspaningsverksamhet som kritiserats för att förmedla vidare uppgifter om svenska medborgares kommunikation till främmande staters underrättelsetjänster, trots försäkringar om att detta inte skulle ske (Dagens Nyheter, 2010).

Slutligen har företagen alltmer börjat se personlig data, exempelvis i form av konsumtionsmönster, som en ekonomisk tillgång vilken kan användas för att generera vinst och bidra till att ge affärsmässigt övertag gentemot konkurrenter. Detta innebär att allt större datavolymer med insamlade personliga uppgifter i växande grad används och sprids än tidigare. För användaren är det i princip praktiskt omöjligt att kontrollera den här spridningen (European Parliamentary Technology Assessment, 2006).

Sammantaget kan det sägas att det är viktigt att den här utvecklingen diskuteras och problematiseras då den kan innebära oönskade inskränkningar i den personliga integriteten om inte adekvata åtgärder för att skydda denna vidtas. Oavsett om detta ligger i linje med den allmänna viljan eller inte så bör sådana förändringar genomsyras av öppenhet och debatt.

3.1.1 DEFINITION AV INTEGRITET

I Nationalencyklopedin definieras integritet dels som "*rätt att ha (visst) eget område som är skyddat mot intrång mest betr. abstrakta områden som önskas skyddade mot åtgärder el. insyn, särsk. från myndighet*" och dels som "*förmåga att handla helt efter eget samvete och utan att vara bunden av ovidkommande yttre hänsyn*" (Nationalencyklopedin 3). En normativ, praktiskt användbar definition av begreppet personlig integritet bör därför lyckas omfatta hela betydelsen utan att bli för specifik. Till att börja med är det därför lämpligt att fastställa vad integriteten syftar till att skydda.

På engelska är orden *privacy* (personlig integritet) och *private* (privat) närbesläktade, och integritet kan sägas handla just om att skydda det som anses privat. Det finns föga överraskande ett flertal definitioner av vad som är privat och vad integritet därmed innebär. Enligt Rössler (2005) kan dessa i huvudsak delas in i fem kategorier:

- Den klassiska definitionen av privat är att det utgörs av vad som naturligt faller inom sfären hushåll, reproduktion och biologiska nödvändigheter. Allt som faller utanför hushållet är sedermera offentligt. Uppenbarligen är definitionen väldigt smal och begränsad eftersom den knappast går utanför den rumsliga aspekten av integritet, och misslyckas med att inkludera mycket av det som intuitivt ses som privat - särskilt i dagens moderna informationsamhälle.
- Att integritet innebär "*rätten att bli lämnad ifred*" myntades av de amerikanska domarna Warren och Brandeis (Warren & Brandeis, 1890). Detta är istället en väldigt allmänt hållen definition som är tveksam lämplig för praktiskt bruk, bland annat för att den inte möjliggör någon åtskillnad mellan rätten till frihet och rätten till integritet.
- Integritet är ett mått på personlig otillgänglighet och en individ upplever fullständig integritet först då den är totalt otillgänglig för andra människor. Grundinställningen lyckas vara precis och generell på samma gång, men misslyckas dock att ta hänsyn till huruvida otillgängligheten är självvald eller inte. En människa som är utsatt för ofrivillig isolering kan inte gärna anses åtnjuta integritet, trots att den är fullständigt otillgänglig för andra.

- Definitioner som utgår från integritet som kontroll av information. Westin uttrycker det exempelvis som (f. ö.): *"Integritet är anspråk från individer, grupper eller institutioner att själva avgöra när, hur och i vilken utsträckning information om dem själva kommuniceras"* (Gavison, 1980). Dessa missar dock många aspekter av integritet då de endast tar upp integritet med hänsyn till information och i form av skydd från allmänhetens granskning, vilket gör den begränsad. Integritet kan uppenbarligen röra sådant som inte är att betrakta som information och behöver nödvändigtvis inte gälla för allmänhetens insyn, utan även för vänner och bekanta. Någon som får sina telefonsamtal avlyssnade får också uppenbarligen sin integritet kränkt, oavsett om information från dessa sprids eller inte.
- Den sista kategorin syftar till att definiera integritet på ett sätt som ger både en generell betydelse och en specifik definition av termen. Enligt Sissela Boks definition (f. ö.): *"Tillståndet då man är skyddad från oönskad åtkomst från andra – antingen fysisk åtkomst, personlig information eller uppmärksamhet. Anspråk på integritet är anspråk på att kontrollera åtkomst."* (1984)

För att erhålla en definition av privat och integritet som kan fungera normativt utgår Rössler från den sistnämnda definitionen och föreslår följande definition (f. ö.): *"Det kan sägas att någonting är privat om man själv kan och/eller bör kontrollera åtkomsten till detta ting"*. Med detta menas både fysisk tillgänglighet, som för exempelvis ett privat utrymme, och metaforisk tillgänglighet, exempelvis persondata. Integritet blir då följaktligen (f. ö.): *"Skyddet av privata ting mot oönskad åtkomst av andra människor"* (Rössler, 2005). Det bör förtydligas att någonting privat inte nödvändigtvis behöver vara hemligt och att något hemligt inte behöver vara privat. Statshemligheter är inte privata, på samma sätt som att ens val av religiös bekännelse inte behöver vara hemlig trots att den i högsta grad är privat.

Vidare identifierar Rössler utifrån tidigare definitioner tre olika sorters privata ting, och därmed tre olika typer av integritet. För att få en heltäckande bild av vad integritet innebär kan begreppet därför delas in i tre olika dimensioner:

- Privata handlingar som skyddas av beslutsmässig integritet (*decisional privacy*). Denna syftar på rätten till självständiga beslut och handlingar utan inblandning från andra personer och påverkan från yttre förhållanden. Exempel på sådana handlingar kan vara att gå i kyrkan, klä sig på ett visst sätt eller hur man uppfostrar sina barn.
- Privat kunskap eller kännedom som skyddas av informationsmässig integritet (*informational privacy*). Rätten att kontrollera åtkomsten till personlig information rörande en själv, som till exempel patientjournaler, brottsregister och finansiell information.
- Fysiska, privata rum som skyddas av rumslig integritet (*locational privacy*). Den traditionella, icke-metaforiska betydelsen där man syftar på rätten att neka tillträde till privata platser eller rum.

De tre dimensionerna representerar vitt skilda egenskaper av begreppet. Följaktligen kan integritetskränkningar ske på tre olika sätt: olovlig inblandning i handlingar, olovlig övervakning eller olovligt intrång i utrymmen eller bostad

Men begreppet personlig integritet måste också ständigt omvärderas på grund av förändringsprocesser i samhället. Särskilt tre förändringar kan enligt Rössler (2005) sägas driva denna pågående revidering:

- Det som förut ansågs intimt och privat har nu tagit sig in i det offentliga rummet.
- Relationerna mellan könen har förändrats med åtföljande förändring av den privata sfären.
- Utvecklingen av informationsteknologi. Digitaliseringen av samhället, internets utbredning och användningen av allt mer avancerad mobil teknik har lett till oöverträffade möjligheter till automatiserad övervakning.

Den sista punkten är central för varför integritet har blivit ett alltmer aktuellt begrepp. Övervakningsdystopin förutsåg tidigare ett samhälle där medborgarnas fysiska handlingar bevakades av en väldig övervakningsapparat, vilket i praktiken skulle vara resurskrävande och ändå bidra med begränsad information på individnivå. Dagens hot går istället att finna i den veritabla massövervakning av medborgarnas datorvanor som både myndigheter och företag har möjlighet till. Det har alltså växt fram ett samhälle där individernas digitala, snarare än fysiska, aktiviteter förhållandevis enkelt och resurssnålt kan kartläggas - så kallad *dataveillance*.

3.1.2 VÄRDET AV INTEGRITET

Även om det finns vitt skilda åsikter om i vilken utsträckning integriteten behöver skyddas så kan man utgå från att det intuitivt finns ett behov av att ha åtminstone någon form av integritetsskydd. Det finns en uttalad rätt till skydd mot inskränkningar i privat- och familjeliv i både FN:s *deklaration om de mänskliga rättigheterna* och i artikel åtta i *Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna* (United Nations; Council of Europe). En rätt till skydd av den personliga integriteten finns inte explicit uttalad i USA:s konstitution, men Högsta domstolen har fastställt att ett sådant skydd mot statliga inskränkningar i den personliga integriteten implicit går att uttolka från andra garanterade rättigheter. Det första sådana prejudikatet kom i fallet *Griswold mot Connecticut* 1965, vilket gällde en delstatslag som förbjöd användningen av preventivmedel inom äktenskapet. Domstolen konstaterade att lagen inte var förenlig med konstitutionen med argumentet att den bröt mot en rätt till personlig integritet som går att uttolka från denna (Beaney, 1966). Åsikten att den personliga integritetens värnande är viktig, för att inte säga fundamental, kan alltså konstateras vara väl spridd.

Föga överraskande finns det även olika typer av uppfattningar om varför integriteten behöver skyddas. Övergripande delar Rössler (2005) in koncepten i två läger: De som anser att integriteten är betydelsefull endast på grund av att den kan reduceras till andra värden och de som inte anser detta. Vidare kan den senare gruppen delas in i ytterligare två grupper där den ena anser att integritet har ett rent intrinsiskt värde medan den andra gruppen visserligen inte tycker att integritetens betydelse kan reduceras, men som därmed inte ser något självändamål med integritet utan anser att den är värd att skyddas eftersom den fyller viktiga funktioner.

3.1.2.1 Intrinsiskt värde

Likt konceptet frihet finns det en skola som anser att den personliga integriteten intuitivt har ett rent intrinsiskt, inneboende, värde som därmed inte behöver motiveras vidare. Skyddet och upprätthållandet av den personliga integriteten finns alltså för att skydda ett egenvärde enligt detta synsätt. Dessa koncept kan vara svåra att urskilja från de som ser integritet ur ett funktionellt perspektiv, då det inte alltid tydligt framgår huruvida integriteten bör skyddas på grund av ett egenvärde eller de funktioner som den fyller.

3.1.2.2 Funktionellt värde

I Nationalencyklopedin står det bland annat så här om integritet: *"rätt att få sin personliga egenart och inre sfär respekterad och att inte utsättas för personligen störande ingrepp"* (Nationalencyklopedin 3). Den personliga egenarten förverkligas genom vad man inom filosofin brukar benämna autonomi. Ett funktionellt perspektiv är att skyddet av den personliga integriteten är en förutsättning för att kunna leva ett autonomt liv. Genom att tillskriva den personliga integriteten ett värde som grundas på dess skyddande av ett annat moraliskt koncept (snarare än ett egenvärde) säger man att den innehar ett funktionellt värde. Hur skyddet av integriteten funktionellt är en förutsättning för att leva autonomt, och vad detta innebär, behandlas mer utförligt senare.

3.1.2.3 Reducerande värde

De reducerande idéerna utgår ifrån att värderingen av personlig integritet i slutändan kan reduceras till andra intressen, rättigheter eller moraliska koncept. De kan även kallas för skeptiska idéer då de förhåller sig skeptiska både till det moraliska rättfärdigandet av integritetsskydd och till utsikterna för att ens kunna beskriva integritet på ett sätt som fångar in hela det heterogena konceptet.

3.1.3 INTEGRITET OCH AUTONOMI

En fri människa är inte nödvändigtvis en autonom människa. Någon som gör fria val men bygger sina beslut och handlingar på godtycklighet, utan att relatera dessa till sina egna värderingar och valmöjligheter kan betraktas som fri men knappast autonom. Med en autonom människa menas nämligen någon som ställer sig själv frågan hur man vill leva sitt liv och handlar därefter. Det underliggande antagandet är att endast autonomi kan leda till ett givande liv, även om det inte är en garanti för detta. Ett givande liv är här inte heller automatiskt lika med ett lyckligt liv (Rössler, 2005).

En autonom människa ska kunna identifiera sig med sina begär, mål och värderingar utan att processen påverkas på ett sådant sätt att identifieringsprocessen känns främmande. Handlingar som uppfyller detta kallas för autentiska handlingar. Vidare ska identifieringsprocessen vara utvärderande och inte bekräftande, val som görs utifrån konventioner och tidigare preferenser är alltså inte att anse som autonoma. Lindley har formulerat det som att: *"En person är autonom om hon förstår sig själv som upphovsman till en handling"* (1986). Men subjektiv autencitet är inte tillräckligt för att göra en handling autonom. Om självbilden är manipulerad av externa förhållanden, som till exempel kan vara fallet i patriarkala strukturer, kan falska begär, åsikter och värderingar formars. Detta leder till handlingar som för individen kan te sig autentiska men som trots detta inte är att anse som autonoma.

Om målet med frihet är att kunna leva ett autonomt liv så belyser villkoren för ett sådant liv att medborgerliga friheter i sig inte är tillräckliga för att skydda autonomi, utan att autonomi är beroende av att dessa friheter konkretiseras genom rättigheter till och anspråk på skydd av integriteten. En individ kan nämligen bli utsatt för handlingar som begränsar autonomi utan att detta strider mot medborgerliga friheter, varför skyddet av integriteten är nödvändig för att säkerställa autonomi. För att leva autonomt är det nämligen av stor vikt att individen själv har möjlighet att påverka bilden av sig själv gentemot andra, till stor del genom val av vilken personlig information man väljer att förmedla. Bryts exempelvis den informationsmässiga integriteten kommer individens antagande om hur och vad andra vet bygga på falska förespeglningar och möjligheten att kontrollera bilden av sin egen person minskar. I det fallet individen är medveten om eventuell övervakning kommer denna medvetenhet styra beteendet och leda till att autenciteten, och därigenom autonomi, förloaras. Att beteendet förändras vid övervakning kommer naturligt av tidigare nämnda behov av att kontrollera vilken bild av sig själv man förmedlar. Faktum är att vissa hävdar att personliga relationers karaktär bestäms av vilken och hur mycket information om ens identitet man delger, vilket skulle betyda att skyddandet av integriteten är en förutsättning för att överhuvudtaget kunna skapa nära relationer (Rachels, 1975).

3.2 RISKPERCEPTION

I allmänhet bedöms vi leva i ett samhälle som har mindre risker än någonsin tidigare, och statistik såsom ökad livslängd och minskad dödlighet i sjukdomar och olyckor stödjer detta. Samtidigt uppger medborgarna att de upplever sig leva i en miljö alltmer präglad av risk (Enander, 2005). Följaktligen finns det alltså en diskrepans mellan den definition av risk som är vedertagen bland experter som arbetar med riskhantering respektive lekmäns upplevelse av risk. Eftersom människor i slutändan agerar utefter hur de upplever risk har riskperception nu en central roll på den politiska agendan i många länder för att möjliggöra vidare teknologisk utveckling (Sjöberg, 2000).

3.2.1 VAD RISKPERCEPTION ÄR

Vid arbete med riskhantering brukar risk ofta definieras som en tripplett bestående av ett scenario med tillhörande sannolikhet och konsekvens, den så kallade risktripletten. Genom att utgå från ett tekniskt synsätt kan man beräkna ett förväntat värde och därmed jämföra olika risker. Detta ger något som kan kallas för objektiva riskmått eftersom det, åtminstone principiellt, inte involverar värderingar och åsikter (Enander, 2005). Beskrivningen av metoden som objektiv har dock kritiserats då exempelvis antaganden och modellval kan skilja sig beroende på vem som utför en analys samtidigt som konsekvenser kan presenteras på olika sätt, varför resultatet måste sägas vara ett resultat av vissa subjektiva bedömningar. Det faktum att förespråkare och kritiker av vissa aktiviteter och teknologier ofta kommer fram till helt olika riskvärderingar, exempelvis genom att sammanväga de negativa konsekvenserna olika och sedan presentera dessa konsekvenser annorlunda, påvisar detta. Vidare så påverkas riskuppfattningen av hur konsekvenserna formuleras, det har bland annat visats att olika beslut tas beroende på om konsekvenserna uttrycks i förlust istället för vinst – trots att utgången i praktiken är identisk (Slovic, 1999). Det får helt enkelt accepteras att det inte finns ett enda rationellt tillvägagångssätt utan att jämförelsemetoder skiljer sig beroende på vilka värderingar de utgår ifrån, varför det speglar frågor såsom etiska värderingar (Riskkollegiet, 1991).

Den riskbedömning som individen gör varje gång den ställs inför ett verkligt eller upplevt hot skiljer sig mycket från expertens. Denna skiljer sig naturligtvis också mellan olika individer då det är en subjektiv bedömning som ofta avviker från den tekniskt framräknade risken. Det var i början av 1970-talet som psykologer började intressera sig för hur människor uppfattar risker, vilket till stor del kan tillskrivas den kärnkraftsdebatt som förekom där många människor var skeptiska till den nya tekniken trots att de av experterna beräknade riskerna tycktes vara små. Ämnesområdet riskperception uppstod. Det förväntat-värdesmått som ingenjörerna använde sig av sågs av psykologerna som inadekvat för att beskriva individens uppfattning av risker och omfattande forskning inleddes för att klarlägga hur olika risker uppfattades och varför (Riskkollegiet, 1993).

Den upplevda risken ska främst ses som ett verktyg med vilket individen beslutar sig för hur den ska handla och inte som en beskrivning av hur verkligheten ser ut. Därför kan det vara svårt, om ens möjligt, att på samma sätt som för tekniska riskbedömningar rakt av jämföra olika risker utifrån detta perspektiv. Alltså är det ett misstag att tro att en risk som uppskattas vara mindre än någon annan därigenom är mer acceptabel (Riskkollegiet, 1991). Där tekniska bedömningar behöver ha väl definierade mått som kan jämföras och ett bestämt tillvägagångssätt så kan mänskliga bedömningar ta hänsyn till olika faktorer beroende på riskens natur och individens värderingar. Mänskliga bedömningar, eller riskperception, bygger helt enkelt på många fler faktorer tekniska dito kan ta hänsyn till. Medan tekniska riskbedömningar ofta använder antalet förlorade liv som enda måttstock tar mänskliga bedömningar förutom omfattningen även hänsyn till konsekvensens karaktär. Riskperceptionen behöver därför inte nödvändigtvis stå i motsats till det väntevärde som används utan kan ses som en mer sammansatt tillämpning av denna metod, och där värdesmättet inte behöver vara bestämt på förhand. Kostnaden och nyttan beräknas helt enkelt på ett annat sätt.

Genomgående är att människor lägger vikten på olika faktorer vid sina bedömningar om huruvida risker är acceptabla eller ej - även om två personer bedömer samma risk som lika stor kan de alltså komma fram till olika slutsatser vad gäller hur de ska bete sig med avseende på denna. Därför bör man inte utgå från att annorlunda riskuppfattningar grundar sig i olika bedömningar av riskens storlek. Exempelvis är det vanligt att teknikmotståndare fokuserar på konsekvensen av en risk, enligt devisen "*på lång sikt är det osannolika oundvikligt*", medan förespråkare talar om den (låga) sannolikheten att detta ska inträffa. Följaktligen kan de båda vara helt överens om giltigheten hos en objektiv riskbedömning, men vara oense om hur den ska tolkas och hanteras (Riskkollegiet, 1993). Vidare kan sannolikhetsgreppet vara svårt, likväl för lekmän som för

experter, när sannolikheterna är små. Därför får skillnader i konsekvens ofta större genomslag än motsvarande förändring av sannolikheten (Riskkollegiet, 1991).

Slovic (2001) ifrågasätter uppfattningen om att tekniska riskbedömningar kan utföras på ett objektivt sätt skilt från värderingar och åsikter. Han menar att alla analyser i är präglade av subjektiva värderingar rakt igenom: Bedömningar görs, modeller som bygger på vissa antaganden används och slutligen väljs det på vilket sätt resultatet ska presenteras. Kritiken att allmänhetens riskperception skulle vara irrationell och illa underbyggd tycker han förbiser det faktum att forskning visar att individens riskperception faktiskt bygger på modeller - modeller som dock skiljer sig från expertens tekniska dito och där resultatet av riskanalyser endast är en faktor vid individens samlade bedömning av risken.

En del anhängare av den rent objektiva metoden är dock kritiska mot den så kallade socialkonstruktivistiska skolan. Garrick (1998) ger sig på den stigmatisering av en del teknologi (främst kärnkraft) som han anser vara vetenskapligt ogrundad, och som intressegrupper och media i hans ögon är ansvariga för. Främst grundar sig kritiken i att opinionsbildare utan lämplig kompetens till stor del påverkar beslut i frågor om riskhantering utan att sedan behöva ansvara för eventuella konsekvenser. Detta resulterar i att samhällets resurser används till att reducera marginella risker på grund av att dessa stämplas som onda i allmänhetens ögon och att liv därmed går till spillo på grund av felaktig resursallokering. Många andra är också kritiska till allmänhetens riskperception vilken de anser vara subjektiv, irrationell, emotionell och orimlig (Slovic, 1999).

Garrick representerar åsikten att en diskrepans mellan objektiv risk och upplevd risk beror på okunskap, och att man därför kan påverka den upplevda risken genom att informera allmänheten bättre. Forskning har dock visat att riskperception är en sammansmältning av fakta och värderingar, varför endast upplysning troligtvis inte är tillräckligt för att påverka denna. Därför anses också media ha en mindre roll då det gäller att påverka individens fundamentala syn på olika risker. Men media kan fylla en annan roll genom att flytta fokus till vissa uppmärksammade riskkällor, vilket i sin tur leder till ökade krav på åtgärder för att minska just dessa risker. Dess inverkan på människors riskperception är dock fortfarande omdebatterad (Riskkollegiet, 1993; Sjöberg, 2000).

3.2.2 FAKTORER I RISKPERCEPTION

I slutet av 1960-talet genomförde Starr, med hjälp av historisk ekonomisk data, en undersökning enligt så kallad *avslöjad preferens*-metod för att se om människors acceptans av olika riskkällor berodde på mer än den så kallade objektiva risken. Denna visade att acceptabel risk inte bara påverkades av tekniska riskuppskattningar utan även subjektiva dimensioner, då det framgick att riskerna kunde delas in i två grupper: De fall där risken var frivillig och de där denna var påtvingad. Konsekvent bedömdes teknologier och aktiviteter i den senare gruppen vara mer acceptabla även när den objektivt bedömda risken inte skilde sig mellan riskkällorna, Starr angav en acceptansskillnad i storleksordningen faktor 1000. Vidare påverkades acceptansnivån direkt med teknologins eller aktivitetens upplevda fördelar och hur många individer som var exponerade, där färre exponerade innebar att högre risker accepterades (Starr, 1969). Dessa resultat var startskottet för forskningsområdet upplevd risk, eller riskperception, och samhällsvetenskapliga forskare började snart söka beskriva detta fenomen och hitta fler subjektiva faktorer som kunde hjälpa till att beskriva den upplevda risken. Frivillighet har därför senare fått kompletterats med en rad andra omständigheter som anses påverka riskperceptionen (Riskkollegiet, 1993; Sjöberg, 2000).

Fischhoff et al presenterade i slutet av 1970-talet en psykometrisk studie där man istället använde sig av *uttalad preferens*-metod. Bland annat kritiserade man Starr för att historiskt beteende inte behöver reflektera samtida preferenser samt för att han negligerade det faktum att det som är accepterat på marknaden inte behöver reflektera allmänhetens önsningar. Den av Starr valda metoden förutsätter nämligen att människor har fullständig kunskap om de val de gör, och att de kan använda den kunskapen på ett optimalt sätt utifrån

sina värderingar. Syftet med den psykometriska studien var att undersöka hur frivillighet och en rad andra faktorer inverkar på hur risker upplevdes och accepterades. Förutom frivillighet valdes faktorer som redan tidigare hade lagts fram som möjliga förklaringar av andra forskare men där tillgången till empirisk data varit sparsam: fördröjda konsekvenser, kunskap hos experter respektive allmänhet, kontrollerbarhet, nyhet, katastrofpotential, hemskhet och dödlighet. De teknologier och aktiviteter man valde att undersöka inkluderade de åtta som Starr hade använt sig av och kompletterades med ytterligare 22. Vad man upptäckte var dels att det oerhört starka samband som Starr noterade, att människor accepterar större risker för samma nytta om risken tas frivilligt, inte gick att påvisa i den psykometriska undersökningen. Dels upptäckte man att de nio föreslagna faktorerna uppvisade stark kovarians och egentligen kunde reduceras till två dimensioner; En skilde mellan låg- och högteknologiaktiviteter där den sistnämnda präglades av nya, ofrivilliga och illa kända aktiviteter med ofta fördröjda konsekvenser; Den andra avsåg sannolikheten att avlida givet att något önskat inträffar (dödlighet). Dessa två dimensioner, kombinerade med den upplevda nyttan av en aktivitet, visade sig kunna beskriva acceptansen väl. I allmänhet så bedömdes också många rådande risknivåer vara oacceptabelt stora, något som talar för att Starrs metodval kunde varit olämpligt (Fischhoff, Slovic, Lichtenstein, Read, & Combs, 1978).

Den psykometriska studien av Fischhoff et al har senare följts upp med flera andra, större undersökningar på området. De förklarande variablerna utökades från 9 till 18 och man fann att tre variabler förklarade en stor andel av variansen: nyhet, hemskhet och antalet exponerade (Sjöberg, 2000). Vidare beskriver Klinke och Renn (2002) den upplevda risken som beroende på två dimensioner: oro och missnöjdhet. Oro handlar om faktorer som fruktan och hur välbekant riskkällan är för individen, missnöjdhet rör om riskens konsekvenser anses vara orättvist fördelade och hur stort misstroende mot riskkällan som individen upplever.

Människor bedömer systematiskt att den subjektiva risken är mindre än den generella risken. En svensk studie visade att den egna och ens familjemedlemmars risk ansågs vara lägre än gemene mans för en given riskkälla. Vidare korrelerade medelvärden av differensen mellan subjektiv risk och generell risk (så kallad *risk denial*) väl med medelvärdet av den upplevda kontrollen över den aktuella risken. Detta visar att riskmålet (*risk target*) är en viktig faktor för den bedömda risken, något det ofta inte tas hänsyn till i liknande studier. Alltså går det att anta att det inte är den upplevta subjektiva risken som då mäts (Sjöberg, 2000).

Den enskilda faktor som korrelerar bäst med inställningen till experters riskbedömningar är dock graden av förtroende, vilken hör tätt ihop med kön, utbildningsbakgrund och sociokulturell bakgrund. Utsatta grupper uppvisar lägre förtroende än förfördelade, således uppger vita män störst förtroende för tekniska bedömningar (Slovic, 1999). Till dags dato har därför den forskning som utförts på ämne risk och säkerhet koncentrerats till hur man bygger upp förtroende och kommunicerar med allmänheten, särskilt med hänsyn till att förtroende är någonting som är betydligt lättare att förstöra än att bygga upp (Slovic, 1993). Speciellt socialt förtroende har antagits innebära en betydande inverkan på hur individer uppfattar och hanterar risker, varför tillit och säkerhet har setts som nödvändiga förutsättningar för den tekniska utvecklingens fortgång (Priest & Bonfadelli, 2003). Detta har dock inte stått oemotsagt utan ifrågasätts av andra undersökningar där tillit, istället för förtroende till institutioner och organisationer, snarare tolkas som en fråga om huruvida den vetenskapliga grunden som riskbedömningarna baseras på accepteras (Sjöberg & Wester-Herber, 2008). Andra har också framfört att det sociala förtroendet förmodligen endast inverkar i någon nämnvärd grad om det handlar om en betydande brist på förtroende (Priest & Bonfadelli, 2003; Slovic, 1993). Som Abraham Lincoln uttryckte det (f. ö.): "Har du en gång förverkat dina medborgares förtroende, kan du aldrig återfå deras respekt och aktning" (Slovic, 1999).

Det ska även sägas att det som kallas objektiv risk, alltså experters riskbedömningar, har visat sig inneha en viktig roll när det gäller allmänhetens riskbedömning trots att många författare väljer att tona ned den. Särskilt när det gäller så kallade normalrisker, där varken sannolikheten eller konsekvensen utmärker sig åt nå-

got håll, så har ett tydligt samband mellan uppskattat antal döda och den verkliga statistiken visats. Små risker överskattas dock generellt samtidigt som stora underskattas (Sjöberg, 2000). Men det är viktigt när man diskuterar riskperception att inte blanda ihop bedömningen av storleken på risken med acceptansen av denna. Lekmäns eventuella missbedömning av den förstnämnda kan sägas vara ett "problem" om det leder till oönskade konsekvenser, medan det senare endast är en fråga om värderingar varför det inte har några givna svar. Det kan alltså inte sägas finnas ett direkt samband mellan riskers bedömda storlek och acceptans (Riskkollegiet, 1993).

3.2.3 RISKPERCEPTIONENS DIMENSIONER

Sammanfattningsvis kan de faktorer som spelar in för riskupplevelsen enligt Riskkollegiet (1993) delas in i tre olika grupper: de som rör uppkomstmekanismerna, de som rör konsekvenserna och de som rör möjligheterna att hantera konsekvenserna. Naturligtvis är det inte alltid vattentäta skott mellan grupperna, men de fungerar för att ge en översiktlig bild av faktorernas dimensioner. Vidare kan några generella tendenser skönjas utifrån demografiska aspekter.

3.2.3.1 Uppkomstmekanismer

Som sagt inverkar det om riskkällan kan räknas som ny, och därför känd, eller gammal och okänd. Hur väl förtegen man är med riskkällan har nämligen visat sig spela en stor roll för den upplevda risken. Detta beror delvis på att risker upplevs olika beroende på hur man kan föreställa sig uppkomsten av eventuella incidenter, där riskkällor med ett fåtal tänkbara uppkomstscenarier upplevs som mindre riskfyllda. För välkända riskkällor finns ett begränsat antal av erfarenhet erhållna uppkomstscenarier medan det för nya, obekanta riskkällor blir mer avhängigt spekulationer.

I vilken utsträckning man har personlig erfarenhet av en riskkälla är även det en förklarande faktor, men inte entydigt åt endera hållet. Till viss del så kan erfarenhet bidra till en tillvänjningseffekt där risken upplevs som allt mindre med erfarenheten, men det har också visat sig bero på individens grunduppfattning. Är man redan negativt inställd till någonting från början så kan ett tillbud skärpa denna uppfattning samtidigt som en förespråkare tolkar det som ett tecken på att säkerhetsåtgärderna fungerar som planerat. Självklart så påverkar även förekomsten av faktiskt inträffade olyckor, särskilt då konsekvenserna är stora.

Olika risker ges olika mycket uppmärksamhet av samhället. Det är ofta så att vardagliga risker, som kanske ändå skördar många offer (exempelvis biltrafiken), inte ges något större utrymme till förmån för spektakulära risker som ger oproportionerligt stor uppståndelse. Här faller osökt massmedias roll in. Av media uppmärksammade risker upplevs vara större relativa risker genom att det är dessa som människor har aktuellt i tankarna och följaktligen vad de upplever som oroande. Detta går in under det fenomen som benämns *social förstärkning av risk* där varje aktör i kommunikationsledet, från ursprungskällan till individen, förstärker eller tonar ned olika aspekter av ursprungsinformationen (Enander, 2005).

3.2.3.2 Konsekvenser

Katastrofpotentialen för en given riskkälla inverkar, det vill säga hur stora konsekvenser en enskild oönskad händelse kan leda till. Därför kan trafikolyckor med dödlig utgång ske frekvent utan större efterfrågan på säkerhetsåtgärder samtidigt som enstaka tågolyckor med flertalet döda snabbt reser krav på förbättringar. Vidare tyder det på det olämpliga i att använda ett förväntat-värdesmått som enda variabel vid bedömningen av vad som anses vara acceptabel risk.

Även konsekvensens karaktär spelar in. Således är acceptansen mindre för vissa fall; de som innebär konsekvenser som drabbar människor som exponeras ofrivilligt och inte drar nytta av riskkällan; de där konsekvensen innebär fördröjda effekter (exempelvis för efterkommande generationer); och de fall där dödligheten är stor givet att en oönskad händelse inträffar. Etiska överväganden innebär att acceptansen för

teknologier som medför stor nytta, men där fördelningen av riskerna innebär att en liten grupp individer får bära upp större delen av dem, sjunker (Enander, 2005).

Sammantaget kan man säga att sällsynta men dramatiska risker missgynnas av den generella riskbedömningen av människor. Det beror bland annat på den faktor som kallas hemsighet (*dread*) vilket är ett samlingsnamn på faktorer som gör att konsekvenserna blir särskilt fruktade, ofta på grund av oöverskådliga eller långvariga effekter (Riskkollegiet, 1993).

3.2.3.3 Kontrollerbarhet

I korthet innebär kontrollerbarhet den utsträckning i vilken det går att kontrollera teknologin och förhindra olyckor från att växa till fullt utvecklade katastrofer. Här spelar även graden av tillit till den aktör som är ansvarig för risken in. I den här gruppen går det likaså att placera faktorn för huruvida riskkällan förekommer naturligt eller om den är introducerad av människan, då det antas att onaturliga risker är mer oöverskådliga. Visserligen går det att argumentera för att det vore mer naturligt att placera den i samband med uppkomstmekanismer, då erfarenheten bör vara större för naturligt förekommande risker, men på grund av att sin förmodade närhet till frågan om aktörsförtroende så har den kategoriserats till kontrollerbarhet (Enander, 2005).

3.2.3.4 Demografi

Enander (2005) redovisar hur riskupplevelsen och synen på säkerhetsåtgärder varierar enligt de demografiska aspekterna kön, ålder, med eller utan barn, civilstånd och etnicitet:

- Kvinnor värderar risker högre och känner större oro inför risker än män, särskilt när det gäller den personliga risken. Vidare uppger män både större erfarenhet av och kunskap om risk- och olycksfrågor. Kvinnor anser i högre grad att åtgärder för att öka säkerheten är mindre besvärliga och meningsfullare än vad män anser.
- I allmänhet ökar riskmedvetenheten och känslan av sårbarhet med åldern. Äldre upplever också säkerhetsåtgärder som meningsfulla medan yngre tycker att de är besvärliga.
- Hos de som har barn i hemmet är riskupplevelsen i allmänhet större. De vidtar också fler säkerhetsåtgärder.
- Sammanboende upplever risker starkare än ensamstående och vidtar fler åtgärder. Vidare anses familj och anhöriga vara väldigt viktiga informationskällor när det gäller risker, vilket skulle kunna vara en delförklaring till detta förhållande.
- Riskupplevelsen hos personer med utländsk bakgrund märker i allmänhet inte ut sig men villigheten till och erfarenheten av att vidta säkerhetsåtgärder är lägre.

I allmänhet går det att tala om att grupper som känner större sårbarhet även upplever en starkare riskuppfattning.

4 HYPOTESFORMULERING

I 3.2 redogörs för begreppet riskperception. Detta används här för att formulera hypoteser om vilka faktorer som kan inverka på allmänhetens acceptans för olika integritetskränkande teknologier. Dessutom väljs ett antal frågor från enkäten ut vilka ska analyseras med hjälp av statistiska metoder ut. Detta för att få en bild som täcker in mer än endast acceptansen.

Dels är det av intresse att undersöka hur olika demografiska grupper skiljer sig när det gäller uppfattningar om personlig integritet i anslutning till tekniska säkerhetsåtgärder och dels är det intressant att se vilka omständigheter och uppfattningar som påverkar detta. Alltså kan de formulerade hypoteserna delas upp på tre grupper:

- Demografiska faktorer
- Kontextuella faktorer
- Kognitiva faktorer

Nedan redogörs för hypoteserna som används för respektive grupp.

4.1 DEMOGRAFISKA FAKTORER

Litteraturstudien redovisade ett antal demografiska faktorer som visat sig inverka på den uppmätta riskperceptionen. De faktorer som ingått i den här rapportens studie är kön, ålder och föräldraskap, varför följande tre nollhypoteser med tillhörande mothypoteser formuleras:

H₀: Respondenternas kön påverkar inte acceptansen.

H₁: Respondenternas kön påverkar acceptansen.

H₀: Huruvida respondenterna har barn eller ej påverkar inte acceptansen.

H₁: Huruvida respondenterna har barn eller ej påverkar acceptansen.

H₀: Respondenternas ålder påverkar inte acceptansen.

H₁: Respondenternas ålder påverkar acceptansen.

Från enkäten väljs fyra frågor ut:

1. Anser du denna typ av användning av teknik är acceptabel? (ja/nej)
2. Anser du denna typ av användning av teknik som integritetskränkande? (ja/nej)
3. I vilken utsträckning litar du på de aktörer som samlar in denna information? (1-5)
4. Hur skulle du skatta denna teknikutveckling (dålig-bra)? (1-5)

Frågorna rör dels de två huvudfrågorna, huruvida tekniken är acceptabel och integritetskränkande, men också tillit och nytta. Både dessa faktorer är väsentliga inom riskperception, vilket framgick i litteraturstudien.

4.2 KONTEXTUELLA FAKTORER

Eftersom enkätstudien genomfördes med hjälp av scenarier, där det för varje enskild teknik fanns två olika scenarier, går det att åtminstone översiktligt undersöka hur kontextuella faktorer påverkar acceptansen. Eftersom detta arbete fokuserar på offentlig riskhantering med hjälp av tekniska säkerhetsåtgärder anses det intressant att undersöka om acceptansen är högre för tillämpningar vars syfte uppges vara ökad säkerhet. Följaktligen ska följande hypoteser prövas:

H_0 : Huruvida syftet med tillämpningen uppges vara ökad säkerhet eller ej påverkar inte acceptansen.

H_1 : Huruvida syftet med tillämpningen uppges vara ökad säkerhet eller ej påverkar acceptansen.

För att analysera den kontextuella inverkan vidare används dessutom samma fyra frågor som nämns ovan:

1. Anser du denna typ av användning av teknik är acceptabel? (ja/nej)
2. Anser du denna typ av användning av teknik som integritetskränkande? (ja/nej)
3. I vilken utsträckning litar du på de aktörer som samlar in denna information? (1-5)
4. Hur skulle du skatta denna teknikutveckling (dålig-bra)? (1-5)

Detta underlättar dessutom eventuella jämförelser.

4.3 KOGNITIVA FAKTORER

De kognitiva faktorer som undersöks vidare är de som inom riskperceptionen benämns nytta, tillit, sannolikhet och hemskhet. Faktorerna har valts för att täcka in de tre dimensionerna uppkomstmekanismer, konsekvenser samt kontrollerbarhet, och får i analysen representeras av följande enkätfrågor:

1. **Nytta:** I vilken utsträckning anser du att denna tillämpning av tekniken är effektiv för att uppnå det mål som är uppsatt? (1-5)
2. **Tillit:** I vilken utsträckning litar du på de aktörer som samlar in denna information? (1-5)
3. **Sannolikhet:** Hur stor risk tror du det är för att denna information kan missbrukas? (1-5)
4. **Hemskhet:** Hur pass orolig över denna utveckling och användning av teknik är du? (1-5)

Syftet är att undersöka om det finns ett samband mellan de här faktorerna och acceptansen respektive uppfattningen om huruvida tekniken är integritetskränkande. För att genomföra detta delas respondenterna upp i två grupper, beroende på om de anser tekniken vara acceptabel eller ej. Hur dessa två grupper har svarat på de valda frågorna jämförs därefter. Samma procedur upprepas sedan, fast uppdelningen sker då utefter huruvida respondenterna anser att tekniken är integritetskränkande. Hypoteserna blir då följande:

H_0 : Huruvida respondenterna anser att tillämpningen är acceptabel eller ej påverkar inte resultaten på de utvalda frågorna.

H_1 : Huruvida respondenterna anser att tillämpningen är acceptabel eller ej påverkar resultaten på de utvalda frågorna.

H_0 : Huruvida respondenterna anser att tillämpningen är integritetskränkande eller ej påverkar inte resultaten på de utvalda frågorna.

H_1 : Huruvida respondenterna anser att tillämpningen är integritetskränkande eller ej påverkar resultaten på de utvalda frågorna.

5 ENKÄTSTUDIE

Själva undersökningen genomfördes av *Sifo International* i form av en webbaserad enkät. Respondenterna valdes utifrån demografiska aspekter ut för att representera den svenska befolkningen i stort. I studien deltog sammanlagt 1511 respondenter som först fick svara på ett antal bakgrundsfrågor om sig själva och som sedan fick två slumpmässigt valda scenarier presenterade för sig. En begränsning som innebar att en respondent inte kunde ställas inför två olika scenarier för samma teknik tillämpades dock. Efter att respektive scenario hade presenterats fick respondenterna besvara en serie följdfrågor som på olika sätt behandlade den aktuella tillämpningen.

5.1 SCENARIER

Ett av de uttalade syftena med enkätundersökningen var att undersöka hur acceptansen för och attityden till olika integritetsinskränkande åtgärder beror på omständigheterna under vilka teknologin tillämpas. Detta innebar att ett scenariobaserat upplägg tillämpades, där det skapades två skilda scenarier för varje teknologi. Scenarierna skiljer sig åt med avseende på tillämpningens syfte, ansvarig aktör, placering och hur informationen samkörs med redan insamlad information. Antalet teknologier som ingick i undersökningen uppgick till sex: näthinnefotografering, övervakningskameror, mobiltelefonpositionering, mejlfilter, RFID och DNA-lagring. Följaktligen uppgick det totala antalet scenarier till tolv och antalet respondenter för varje scenario till ungefär 250. För samtliga tekniker utom RFID behandlar minst ett av de två scenarierna någon form av offentlig säkerhetstillämpning. Nedan presenteras samtliga scenarier, uppdelade efter teknik, exakt såsom de framgick i studien.

5.1.1 NÄTHINNEFOTOGRAFERING (RETINA)

5.1.1.1 Scenario 1-1

På flygplatsen blir du tillfrågad att lämna information om dig själv som syftar till att öka säkerhet inom flyget. Detta säkerhetsarbete är ett samarbete mellan alla Frequent flyer-program och Luftfartsstyrelsen. Den information du lämnar är ett fotografi av din näthinna som tas i en speciell kamera, en retina-scanner. Denna information lagras i ett år och personal som arbetar med flygsäkerhet har tillgång till den.

5.1.1.2 Scenario 1-2

På flygplatsen blir du tillfrågad att lämna information om dig själv som syftar till att öka effektiviteten vid incheckning. Detta program erbjuds som en del av ens flygbolags Frequent flyer-program. Detta skulle innebära att incheckningen och säkerhetskontrollen går fortare för dig. Den information du lämnar är ett fotografi av din näthinna som tas i en speciell kamera, en retina-scanner. Denna information lagras i ett år och personal på ditt flygbolag har tillgång till den.

5.1.2 ÖVERVAKNINGSKAMEROR (CCTV)

5.1.2.1 Scenario 2-1

Kommunen i vilken du bor har installerat övervakningskameror på torget i staden i syfte att öka säkerheten och tryggheten. Kamerorna är tänkta att ha ett avskräckande syfte eftersom de är synligt placerade och det kommer bli lättare att identifiera personer på inspelningen om ett brott begås. Kamerorna är kopplade till en bemannad övervakningscentral och inspelningarna lagras i tre månader.

5.1.2.2 Scenario 2-2

Kommunen i vilken du bor har installerat övervakningskameror på torget i staden i syfte att öka säkerheten och tryggheten. Kamerorna är utrustade med en teknik, så kallad maskningsteknik, som gör att identifiering av individer är svårt. Kamerorna är tänkta att ha ett avskräckande syfte då de placeras synligt. Kamerorna är kopplade till en bemannad övervakningscentral och inspelningarna lagras i tre månader.

5.1.3 MOBILTELEFONPOSITIONERING (MOBPOS)

5.1.3.1 Scenario 3-1

En ny tjänst lanseras av din teleoperatör som gör att man kan se var en mobiltelefon med ett visst telefonnummer befinner sig. Informationen visas på en kartbild som man kommer åt genom att logga in på en lösenordsskyddad internetsida. Denna teknik finns i de flesta mobiltelefonnummer, men för att få tillgång till denna funktion måste man aktivt anmäla sig.

5.1.3.2 Scenario 3-2

En ny tjänst lanseras av din teleoperatör som gör att man kan se var en mobiltelefon med ett visst telefonnummer befinner sig. Informationen visas på en kartbild som man kommer åt genom att logga in på en lösenordsskyddad internetsida. Denna teknik finns i de flesta mobiltelefoner, men för att få tillgång till denna funktion måste man aktivt anmäla sig. Dock kan polisen under särskilda omständigheter aktivera funktionen utan att meddela abonnenten.

5.1.4 MEJLFILTER (MEJL)

5.1.4.1 Scenario 4-1

Det företag du arbetar på använder sig av ett datorprogram som automatiskt går igenom alla mejl för att upptäcka eventuell information eller verksamhet som hotar företagets produktivitet. Programmet söker efter speciella ord eller kombinationer av ord för att på detta sätt identifiera mejl som kan innehålla känslig information. Om programmet upptäcker något misstänkt så granskas mejlet av säkerhetspersonal.

5.1.4.2 Scenario 4-2

En statlig myndighet använder sig av ett datorprogram som automatiskt går igenom alla mejl som skickas till och från mottagare inom Sverige för att upptäcka eventuell information eller verksamhet som hotar rikets säkerhet. Programmet söker efter speciella ord eller kombinationer av ord för att kunna identifiera mejl som innehåller misstänkt information. Om programmet upptäcker något misstänkt så granskas mejlet av säkerhetspersonal.

5.1.5 RFID

5.1.5.1 Scenario 5-1

Du har ett flertal olika kort som använder sig av RFID-teknik. Bland annat ett passerkort till din arbetsplats, ett periodkort för resor med lokaltrafik, och en transponder i din bil för att kunna betala vägavgifter. Den information som finns på dessa kort kan kopplas till en själv och ens vanor. Man använder sig dagligen av sitt periodkort för resor med lokaltrafiken. Detta kort hålls upp mot en speciell läsare där det läses av. Informationen om ens resor sparas i tre månader och används av lokaltrafikleverantören för att förbättra service och utbud, till exempel i form av tätare avgångar eller nya stationer.

5.1.5.2 Scenario 5-2

Det finns ett flertal olika användningsområden för RFID-teknologi. Bland annat för passerkort vid arbetsplatser, periodkort för resor med lokaltrafik och som märkning av varor både för transport och i affärer. Dessa RFID-kort kan placeras inuti klädesplagg vilket gör att information om dina kläder kan registreras av speciella läsare. Detta innebär att när du går in i en affär kan en expedient se var, när och till vilket pris du köpt de kläder du har på dig. Baserat på denna information kan butiken ge skräddarsydda erbjudanden.

5.1.6 DNA-LAGRING (DNA)

5.1.6.1 Scenario 6-1

När du går till vårdcentralen får du frågan om du kan tänka sig att lämna ett salivprov som ska ingå i en biodatabank som Universitetssjukhuset upprättar för forskningsändamål. Din DNA kommer kartläggas och de data man tar fram kommer att ge information om ärftliga och kroniska sjukdomar, ditt nuvarande hälsotillstånd och eventuella framtida sjukdomar. Dessa data kommer att sparas i en obestämd tid och du måste själv begära utträde ur databasen.

5.1.6.2 Scenario 6-2

När du går till vårdcentralen får du frågan om du kan tänka dig att lämna ett salivprov som ska ingå i en biodatabank som Rikspolisstyrelsen upprättar för brottsbekämpande ändamål. Din DNA kommer att kartläggas och registreras för att underlätta fastställande eller uteslutande av identitet vid utredning i framtida brottsmål. Dessa data kommer att sparas i en obestämd tid och du måste själv begära utträde ur databasen.

5.2 RESULTAT

Respondenterna fick som tidigare nämnts först besvara ett antal bakgrundsfrågor om sig själva. Dessa avhandlade kön, föräldraskap, ålder och intresseområde. Efter att varje scenario hade presenterats besvarades sedan ett antal följdfrågor vilka översiktligt kan delas in i fem kategorier:

- Acceptans
- Efterfrågan
- Frivillighet
- Fördelar kontra nackdelar
- Tillit och missbruk

Studiens ingående frågor, exakt såsom de framgick i enkäten, redovisas här i samband med resultaten för att underlätta överblicken. Efter varje fråga framgår också på vilken skala svaret kunde ges. Samtliga enkätfrågor redovisas gemensamt i Bilaga A – Enkätfrågor

Nedan presenteras resultaten, i form av medelvärden eller andel jakande respondenter, för samtliga frågor uppdelat efter de fem frågekategorierna. Varje kategori inleds med några enkätfrågor för vilka resultaten från samtliga scenarier presenteras i samma figur, detta för att underlätta jämförelser mellan olika tekniker. Sedan redovisas övriga svar för respektive teknik.

Det fåtal frågor som medgav att respondenten lämnade fritextsvar har exkluderats ur denna rapport på grund av utrymmesskäl. Dessa kan dock vara av intresse att studera om vidare undersökningar genomförs.

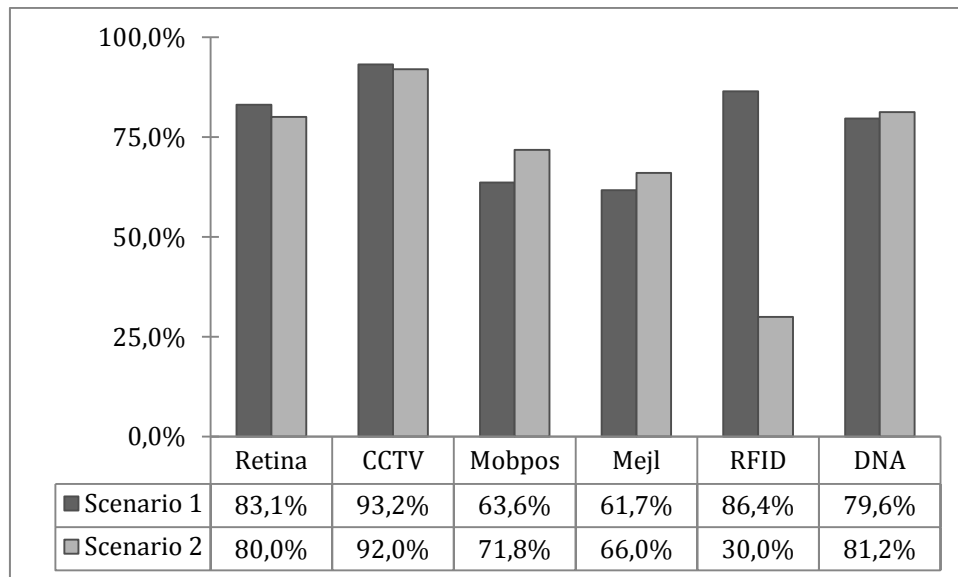
Läsaren förväntas vara uppmärksam på att det i resultatavsnitten för de enskilda teknikerna även redogörs för resultat som presenteras redan i den gemensamma resultatdelen.

5.2.1 ACCEPTANS

Följande enkätfrågor placeras in den frågekategori som rör acceptans:

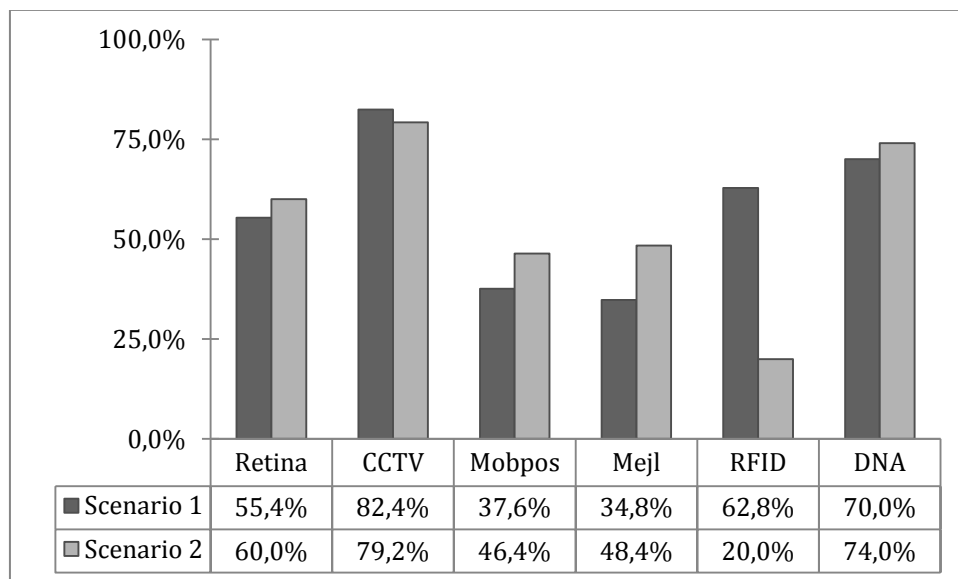
- Anser du att denna typ av användning av teknik som integritetskränkande (ja/nej)?
- Anser du denna typ av användning av teknik är acceptabel (ja/nej)?
- Anser du denna teknik kommer att förbättra samhället (ja/nej)?
- I vilken utsträckning anser du denna tillämpning av tekniken bidrar till att samhället blir mer sårbart (1-5)?
- I vilken utsträckning anser du att denna tillämpning av tekniken är effektiv för att uppnå det mål som är uppsatt (1-5)?
- I vilken utsträckning anser du att denna tillämpning av tekniken bidrar till att samhället blir säkrare eller mer effektivt (1-5)?

De första två frågorna anses vara särskilt intressanta eftersom de rör frågeställningar som är centrala för denna rapport.



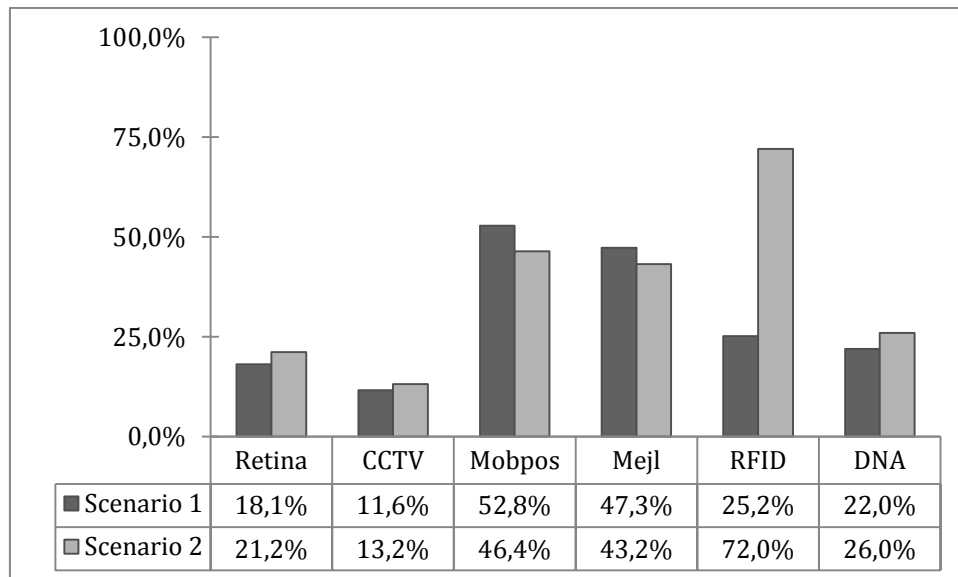
Figur 1. Utvisar för samtliga scenarier hur stor andel av respondenterna som svarar jakande på frågan "Anser du denna typ av användning av teknik är acceptabel?".

Som det går att utläsa i Figur 1 går det säga att acceptansen generellt är hög för de olika teknikerna. Det går att ana en eventuell trend som innebär att äldre, etablerad teknik erhåller högre acceptans än nyare teknik. Särskilt RFID 2, som visserligen inte behandlar någon säkerhetstillämpning och därför ligger utanför detta arbetes fokus, utmärker sig på ett negativt sätt. Det är också den enda teknik som inte kan sägas vara i bruk på ett eller annat sätt i dagsläget.



Figur 2. Utvisar för samtliga scenarier hur stor andel av respondenterna som svarar jakande på frågan "Anser du denna teknik kommer att förbättra samhället?".

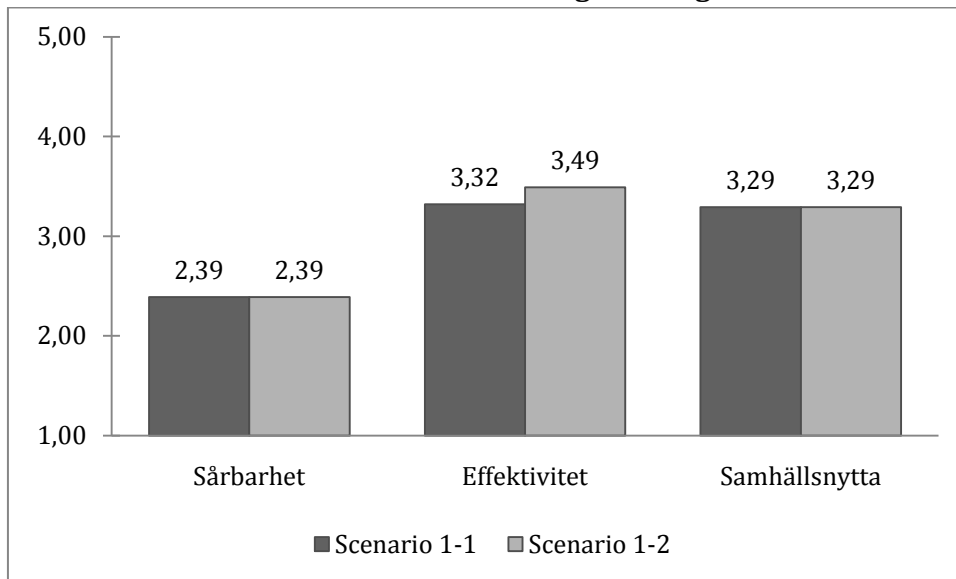
I Figur 2 går det att se något lägre nivåer än för acceptansen, men de inbördes förhållandena mellan scenarierna verkar tämligen konstanta. Bara för att en tillämpning accepteras behöver den alltså inte uppfattas som särskilt nyttig.



Figur 3. Utvisar för samtliga scenarier hur stor andel av respondenterna som svarar jakande på frågan "Anser du att denna typ av användning av teknik som integritetskränkande?".

Andelen av respondenterna som anser att tillämpningen är integritetskränkande är i princip lika stor som andelen som anser att den inte är acceptabel för respektive teknik, vilket Figur 3 utvisar. Viss överlappning förekommer dock. Särskilt de nyare teknikerna mobiltelefonpositionering, mejlfilter och RFID uppvisar denna överlappning.

5.2.1.1 Scenario 1 – Näthinnefotografering

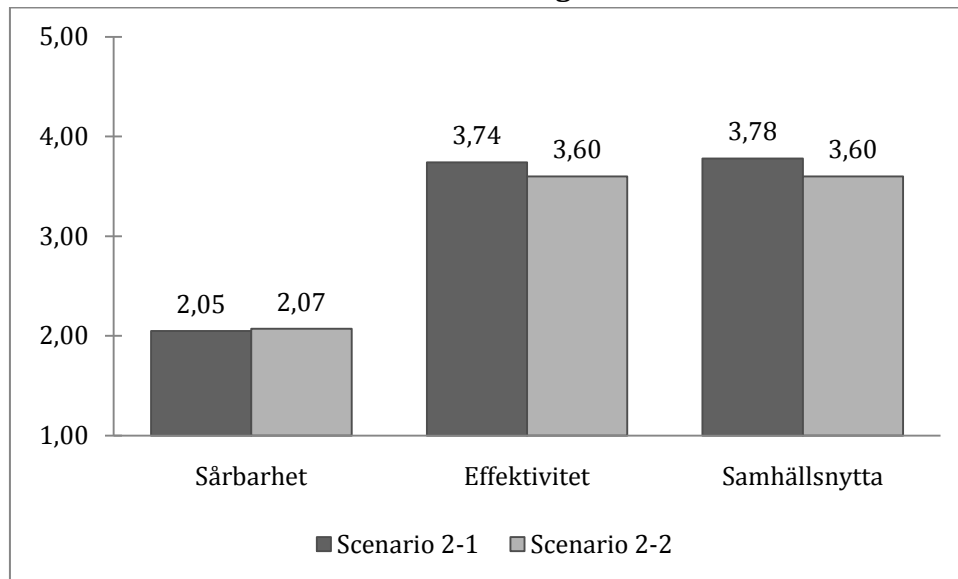


Figur 4. Utvisar för scenario 1-1 och 1-2 resultaten för frågorna "I vilken utsträckning anser du denna tillämpning av tekniken bidrar till att samhället blir mer sårbart", "I vilken utsträckning anser du att denna tillämpning av tekniken är effektiv för att uppnå det mål som är uppsatt" samt "I vilken utsträckning anser du att denna tillämpning av tekniken bidrar till att samhället blir säkrare eller mer effektivt" .

Acceptansen är generellt hög för näthinnefotografering, och inga större skillnader föreligger mellan de två delscenarierna. 18,1 respektive 21,2 procent tycker att tillämpningen är integritetskränkande, 83,0 respektive 80,0 procent anser att tillämpningen är acceptabel och 55,4 respektive 60,0 procent tycker att tillämpningen bidrar till att förbättra samhället. Acceptansen för tillämpningen vars syfte är ökad säkerhet är alltså marginellt högre än den för bekvämlighet, även om åsikten att tekniken är samhällsförbättrande är vanligare för säkerhetsscenarioet.

Enligt Figur 4 kan sägas att båda tillämpningarna anses bidra måttligt till samhällets sårbarhet (2,39 för båda delscenarierna), effektiviteten värderas ganska högt (3,32 respektive 3,49) och likaså samhällsnyttan (3,29 för båda). Det intressantaste resultatet i sammanhanget är det faktum att det verkar vara små skillnader i attityder beroende på om tillämpningens syfte är säkerhet eller bekvämlighet.

5.2.1.2 Scenario 2 - Övervakningskameror

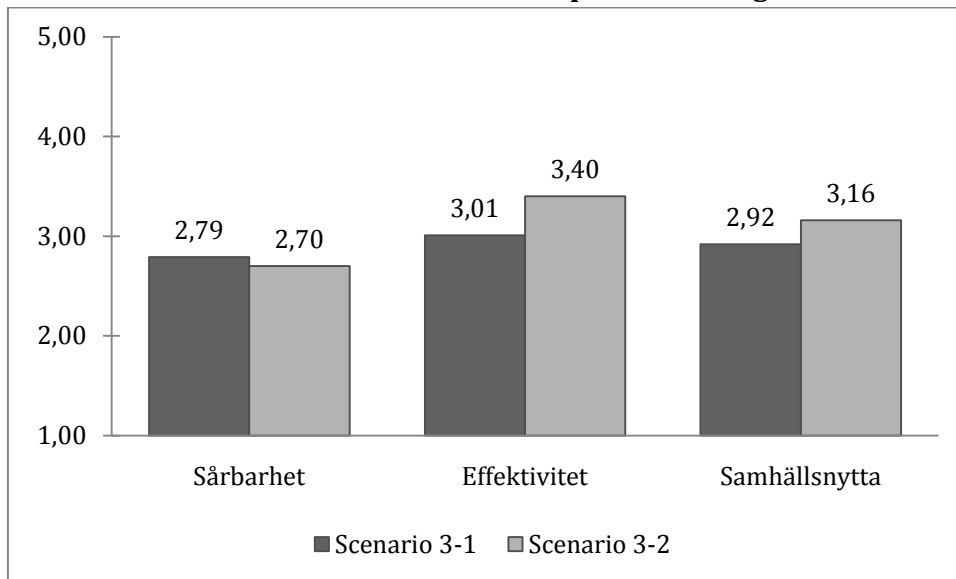


Figur 5. Utvisar för scenario 2-1 och 2-2 resultaten för frågorna "I vilken utsträckning anser du denna tillämpning av tekniken bidrar till att samhället blir mer sårbart", "I vilken utsträckning anser du att denna tillämpning av tekniken är effektiv för att uppnå det mål som är uppsatt" och "I vilken utsträckning anser du att denna tillämpning av tekniken bidrar till att samhället blir säkrare eller mer effektivt".

Även för övervakningskameror föreligger det inga större skillnader mellan de båda tillämpningarna. Acceptansnivån är väldigt hög. Integritetskränkande enligt 11,6 respektive 13,2 procent, acceptabel enligt 93,2 respektive 92,0 procent och 82,4 respektive 79,0 procent anser tekniken vara samhällsförbättrande.

Värderingen av sårbarhet (2,05 respektive 2,07), effektivitet (3,74 respektive 3,60) och samhällsnytta (3,78 respektive 3,70) som kan utläsas ur Figur 5 är likartad. Sammanfattningsvis verkar tekniken vara brett accepterad.

5.2.1.3 Scenario 3 – Mobiltelefonpositionering

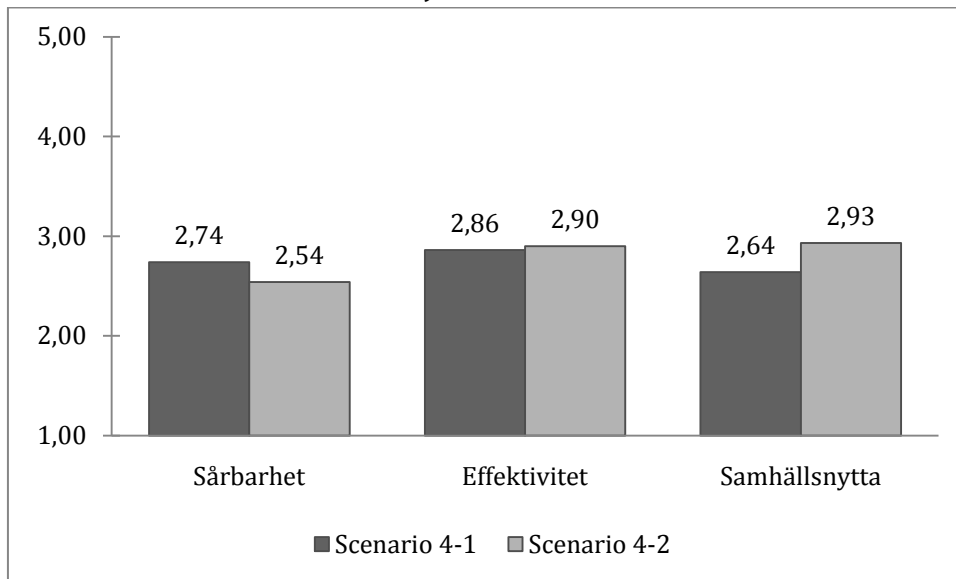


Figur 6. Utvisar för scenario 3-1 och 3-2 resultaten för frågorna "I vilken utsträckning anser du denna tillämpning av tekniken bidrar till att samhället blir mer sårbart", "I vilken utsträckning anser du att denna tillämpning av tekniken är effektiv för att uppnå det mål som är uppsatt" och "I vilken utsträckning anser du att denna tillämpning av tekniken bidrar till att samhället blir säkrare eller mer effektivt".

För mobiltelefonpositionering föreligger det vissa skillnader mellan delscenarierna och acceptansen får sägas vara måttlig. Scenario 3-2, där polisen kan använda sig av tekniken, skattas generellt högre än 3-1 som endast är en kommersiell tjänst. Integritetskränkande 52,8 respektive 46,4 procent, acceptabelt 63,6 respektive 71,8 procent och samhällsförbättrande 37,6 respektive 46,4 procent.

Inverkan på samhällets sårbarhet skattas likartat och måttligt (2,79 respektive 2,70) samtidigt som effektiviteten (3,01 respektive 3,40) och samhällsnyttan (2,92 respektive 3,16) värderas något högre i polistillämpningens favör enligt Figur 6.

5.2.1.4 Scenario 4 – Mejlfilter

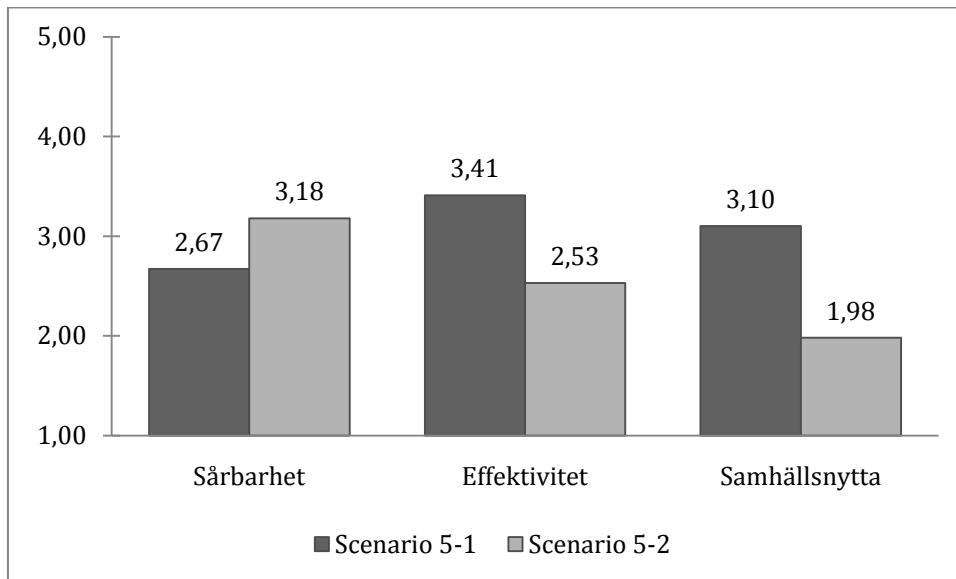


Figur 7. Utvisar för scenario 4-1 och 4-2 resultaten för frågorna "I vilken utsträckning anser du denna tillämpning av tekniken bidrar till att samhället blir mer sårbart", "I vilken utsträckning anser du att denna tillämpning av tekniken är effektiv för att uppnå det mål som är uppsatt" och "I vilken utsträckning anser du att denna tillämpning av tekniken bidrar till att samhället blir säkrare eller mer effektivt".

Acceptansen för mejlfilter är generellt sett måttlig och användning för nationell säkerhet är något mer accepterad än användningen för företagets säkerhet (61,7 respektive 66,0 procent). Integritetskränkande anser 47,3 respektive 43,2 procent och förbättrar samhället enligt 34,8 respektive 48,4 procent.

I Figur 7 syns att skattningen av sårbarhet (2,74 respektive 2,54), effektivitet (2,86 respektive 2,90) och samhällsnytta (2,66 respektive 2,93) inte är högre än måttlig, men något positivare i den nationella säkerhetens favör.

5.2.1.5 Scenario 5 - RFID

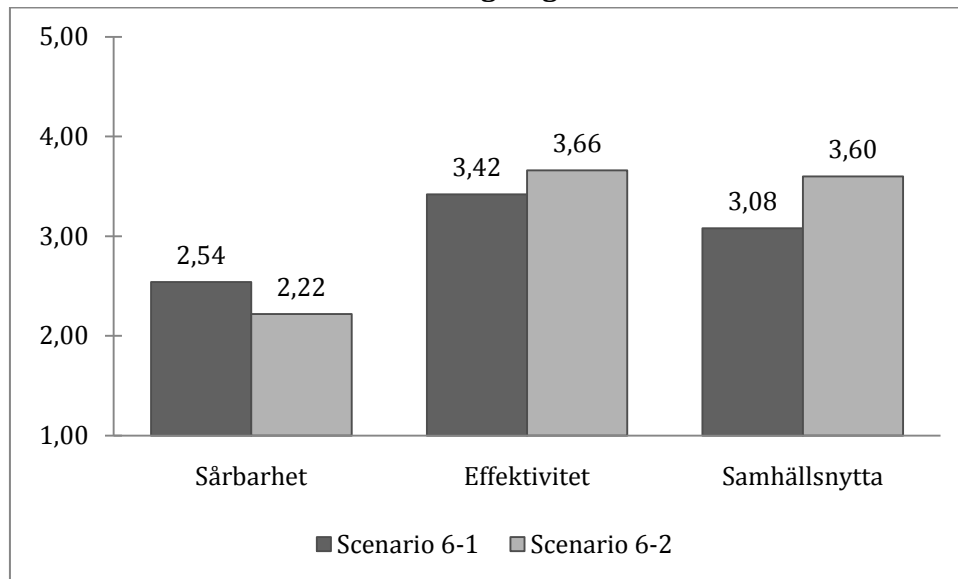


Figur 8. Utvisar för scenario 5-1 och 5-2 resultaten för frågorna "I vilken utsträckning anser du denna tillämpning av tekniken bidrar till att samhället blir mer sårbart", "I vilken utsträckning anser du att denna tillämpning av tekniken är effektiv för att uppnå det mål som är uppsatt" och "I vilken utsträckning anser du att denna tillämpning av tekniken bidrar till att samhället blir säkrare eller mer effektivt".

För RFID finns det stora skillnader i acceptans och uppskattning för de två tillämpningarna. Endast 25,2 procent tycker användningen i kollektivtrafiken är integritetskränkande medan 72,0 tycker detsamma om klädtillämpningen. Acceptansen skiljer sig kraftigt åt (86,4 respektive 30,0 procent) liksom frågan huruvida tekniken är samhällsförbättrande (62,8 respektive 20 procent).

I Figur 8 speglas skillnaderna även i uppskattningen av sårbarhet (2,67 respektive 3,18), effektivitet (3,41 respektive 2,53) och samhällsnytta (3,10 respektive 1,98).

5.2.1.6 Scenario 6 - DNA-lagring



Figur 9. Utvisar för scenario 6-1 och 6-2 resultaten för frågorna "I vilken utsträckning anser du denna tillämpning av tekniken bidrar till att samhället blir mer sårbart", "I vilken utsträckning anser du att denna tillämpning av tekniken är effektiv för att uppnå det mål som är uppsatt" och "I vilken utsträckning anser du att denna tillämpning av tekniken bidrar till att samhället blir säkrare eller mer effektivt".

Båda tillämpningarna anses vara integritetskränkande av en hyfsat låg andel respondenter (22,0 respektive 26,4 procent) med en något högre andel för den polisiära användningen. De anses också samhällsförbättrande av 70,0 respektive 74,0 procent. Den polisiära användningen anses alltså vara både mer kränkande och mer samhällsförbättrande än den för forskning. Acceptansen är i princip lika hög med 79,6 respektive 81,2 procent.

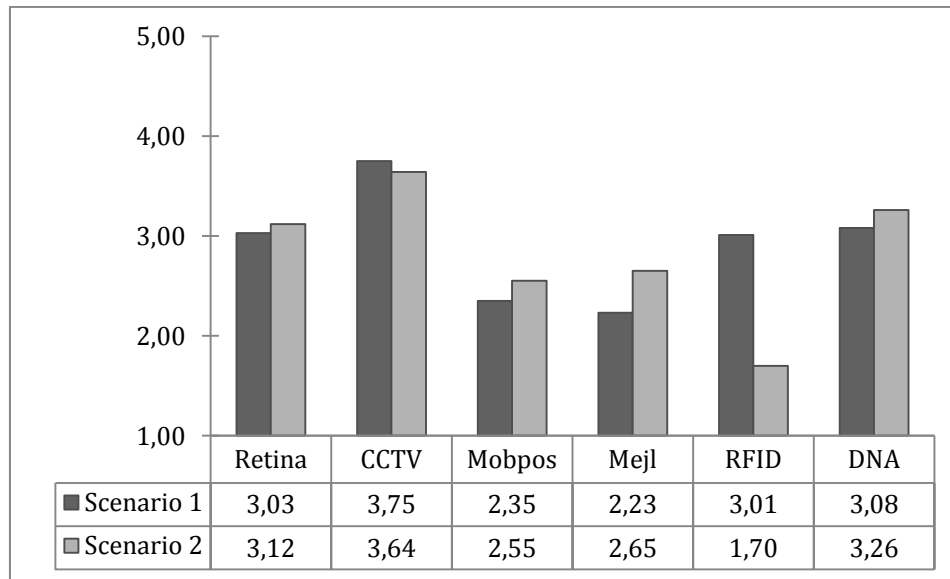
Tekniken anses bidra måttligt till samhällets sårbarhet (2,54 respektive 2,22) enligt Figur 9. Effektiviteten (3,42 respektive 3,66) och, i något mindre grad, samhällsnyttan (3,08 respektive 3,60) bedöms som hög med övervikt för den polisiära användningen.

5.2.2 EFTERFRÅGAN

De frågor som faller in under kategorin efterfrågan:

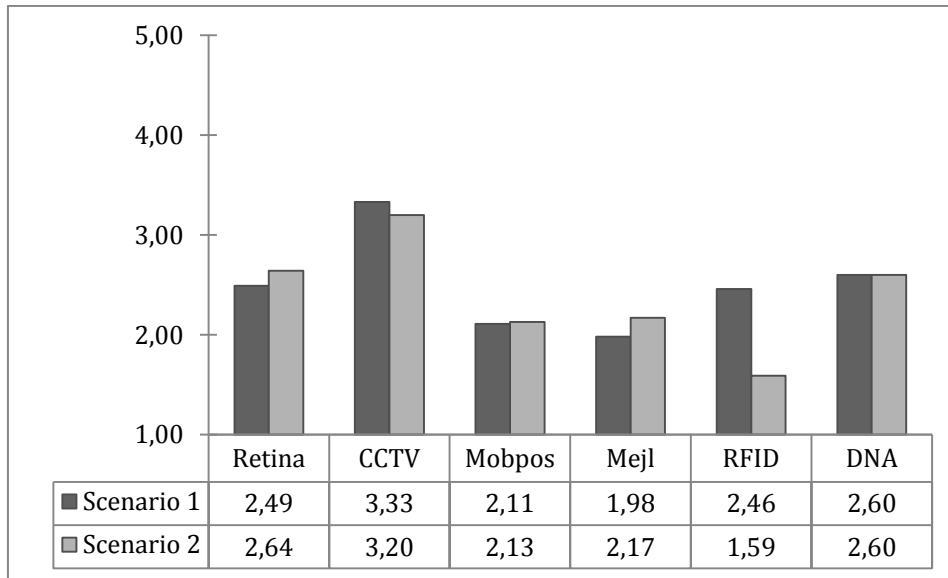
- Jag vill gärna ha denna tillämpning av tekniken (1-5).
- Jag skulle aktivt efterfråga denna teknik om jag fick tillfälle (1-5).
- Jag anser denna teknik kan användas av (ja/nej):
 - Alla myndiga personer.
 - Föräldrar som ger sitt medgivande att uppgifter om deras barn samlas in.
 - Personer som ger sitt tillstånd för att omyndig partners information samlas in.
 - Anser inte vi ska använda denna teknik.
 - Inte relevant.

För sista frågan redovisas resultaten för samtliga delfrågor men endast de tre första diskuteras . Detta på grund av att det näst sista svarsalternativet antas spegla acceptansen (som redovisas i ett eget avsnitt) och det sista är svårtolkat.



Figur 10. Utvisar för samtliga scenarier resultatet för frågan "Jag vill gärna ha denna tillämpning av tekniken".

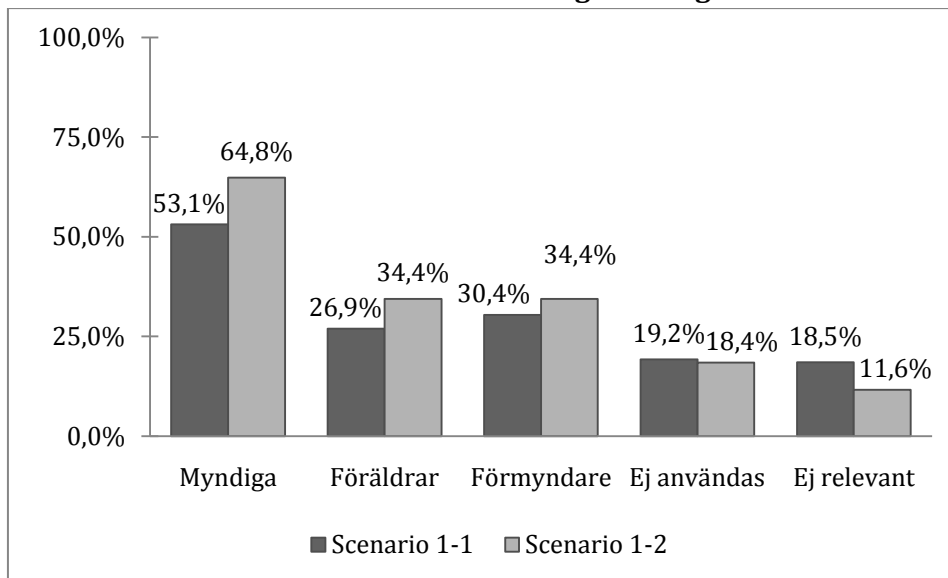
I Figur 10 framgår det att bedömningen av hur gärna respondenterna vill ha de olika tillämpningarna i princip följer acceptansnivån. Det kan dessutom ses att tillämpningar som syftar till att öka säkerheten är särskilt populära.



Figur 11. Utvisar för samtliga scenarier resultatet för frågan "Jag skulle aktivt efterfråga denna teknik om jag fick tillfälle".

Figur 11 visar siffror som liknar dem från förra frågan, men med nivåer som är ungefär 0,5 lägre. Båda scenarierna för mobiltelefonpositionering efterfrågas i princip lika mycket trots en märkbar acceptansskillnad.

5.2.2.1 Scenario 1 - Näthinnefotografering

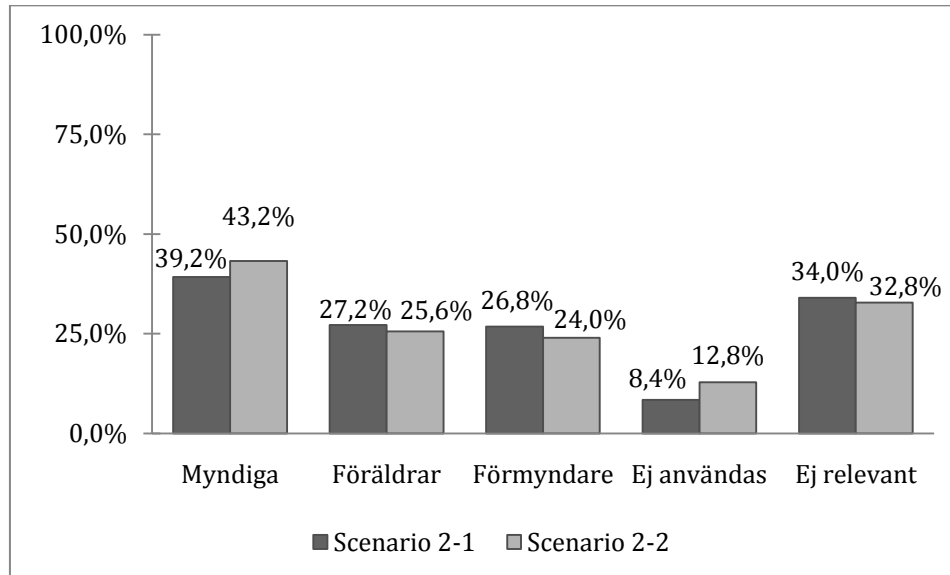


Figur 12. Utvisar för scenario 1-1 och 1-2 resultatet för frågan "Jag anser denna teknik kan användas av".

Det föreligger både en större önskan (3,03 respektive 3,12) och aktiv efterfrågan (2,49 respektive 2,64) för att införa tekniken av bekvämlighetsskäl enligt. Intressant att notera eftersom acceptansen för den tillämpningen var något lägre.

På frågan vilka som ska kunna använda tekniken, vars resultat presenteras i Figur 12, är resultaten ganska likartade för myndiga (53,1 respektive 64,8 procent), föräldrar (26,9 respektive 34,4 procent) och förmyndare (30,4 respektive 34,4 procent).

5.2.2.2 Scenario 2 – Övervakningskameror

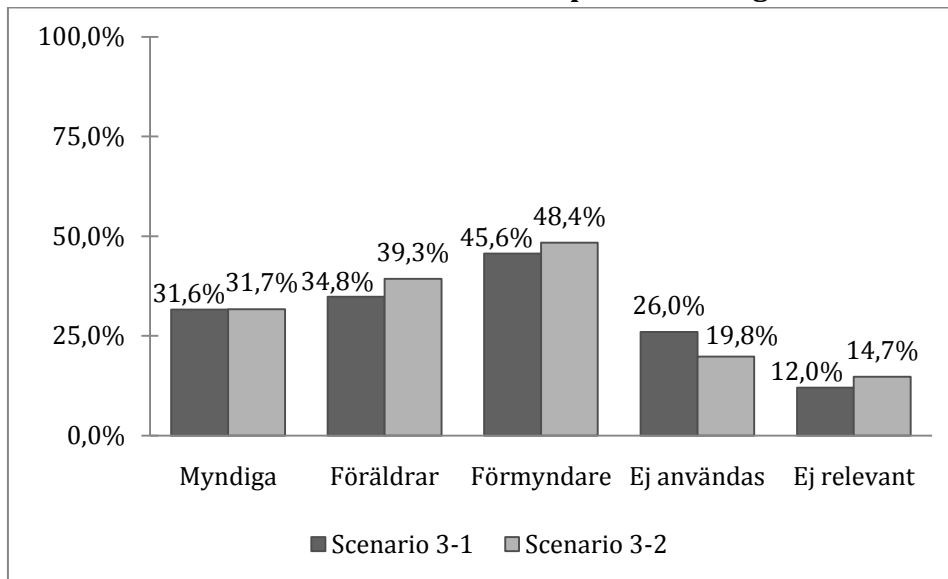


Figur 13. Utvisar för scenario 2-1 och 2-2 resultatet för frågan "Jag anser denna teknik kan användas av".

Det är något populärare med konventionell övervakningskamera jämfört med maskningsteknik, både när det gäller önskan (3,75 respektive 3,64) och efterfrågan (3,33 respektive 3,20) på tekniken. Även här alltså trots att den förstnämnda har högre acceptansnivå.

På frågan vilka som ska kunna använda tekniken, vars resultat presenteras i Figur 13, är resultaten ganska likartade för myndiga (39,2 respektive 43,2 procent), föräldrar (27,2 respektive 25,6 procent) och förmyndare (26,8 respektive 24,0 procent).

5.2.2.3 Scenario 3 – Mobiltelefonpositionering

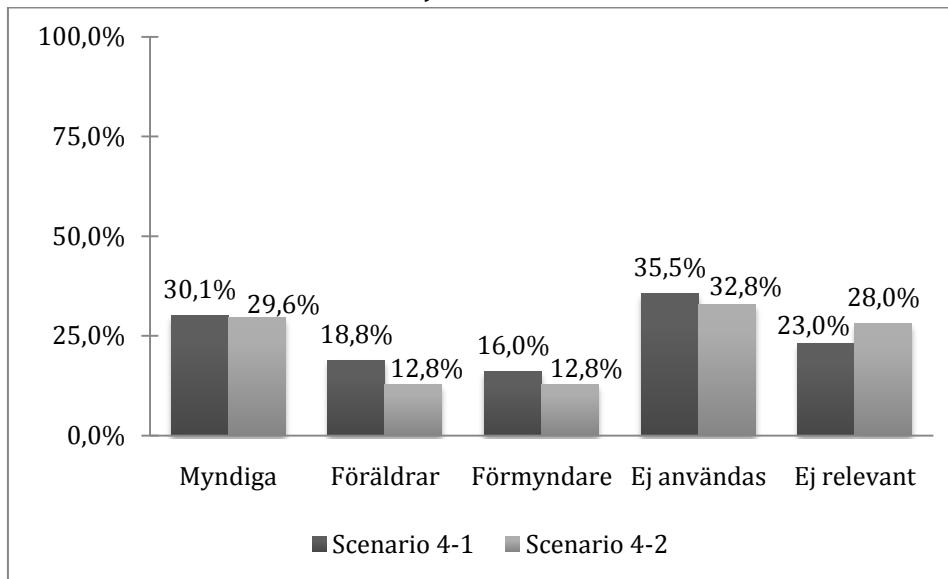


Figur 14. Utvisar för scenario 3-1 och 3-2 resultatet för frågan "Jag anser denna teknik kan användas av".

Den kommersiella tjänsten önskas i något mindre grad än den polisiära (2,35 respektive 2,55) samtidigt som den aktiva efterfrågan skiljer sig marginellt (2,11 respektive 2,13). Men båda tillämpningarna efterfrågas alltså i relativt låg utsträckning.

På användarfrågan skiljer sig inte svaren nämnvärt, förutom att föräldrar i något större utsträckning ska få använda sig av den polisiära tjänsten enligt Figur 14. Intressant är däremot att föräldrar (34,8 respektive 39,3 procent) och förmyndare (45,6 respektive 48,4 procent) för båda scenarierna anses bör få använda tekniken i större utsträckning än myndiga personer (31,6 respektive 31,7 procent).

5.2.2.4 Scenario 4 – Mejlfilter

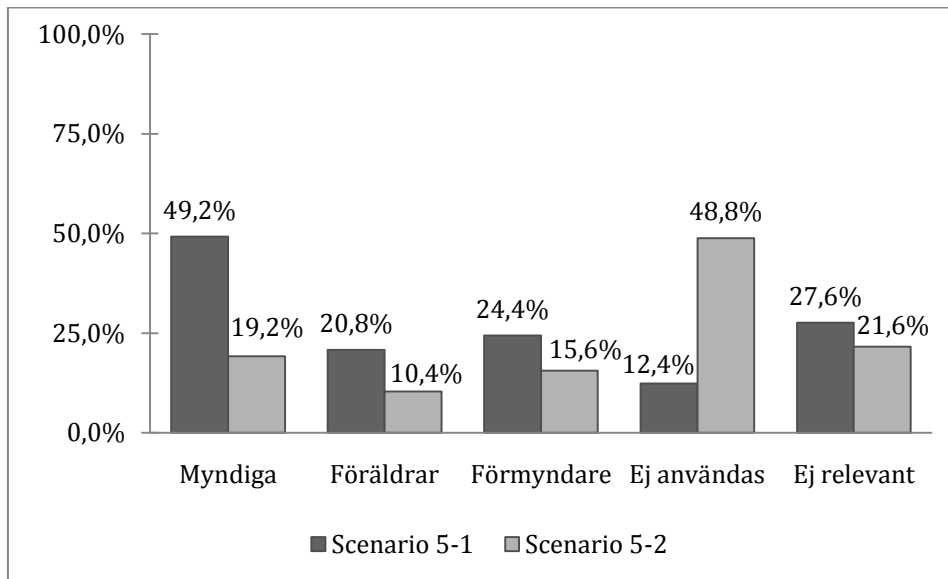


Figur 15. Utvisar för scenario 4-1 och 4-2 resultatet för frågan "Jag anser denna teknik kan användas av".

Användningen för nationell säkerhet är både mer önskad (2,23 respektive 2,65) och aktivt efterfrågad (1,98 respektive 2,17). Ingen av tillämpningarna kan dock sägas vara särskilt efterfrågad.

Figur 15 visar att *Ej relevant* (23,0 respektive 28,0 procent) är ett populärt svarsalternativ, varför det kan vara svårt att dra några slutsatser utifrån att det skiljer något i vilken utsträckning föräldrar (18,8 respektive 12,8 procent) och förmyndare (16,0 respektive 12,8 procent) ska få använda tekniken. Det kan mycket väl tänkas bero på att respondenterna anser att det är svårt att se hur frågan skulle tillämpas i respektive scenario.

5.2.2.5 Scenario 5 – RFID

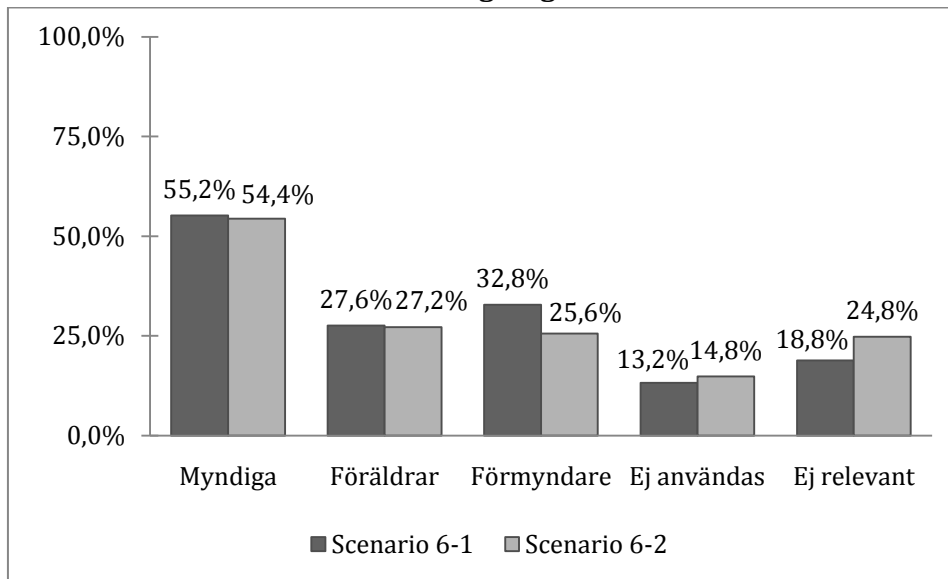


Figur 16. Utvisar för scenario 5-1 och 5-2 resultatet för frågan "Jag anser denna teknik kan användas av".

I linje med frågan om acceptans så är efterfrågan på klädtillämpningen extremt låg jämfört med kollektivtrafiken, både önskan (3,01 respektive 1,76) och aktiva efterfrågan (2,46 respektive 1,59). Efterfrågan på kollektivtrafiken får därför ses som måttlig samtidigt som densamma för kläder är väldigt låg.

Skillnaderna i vilka som ska få använda tekniken, redovisat i Figur 16, följer samma spår och blir svåra att tolka vidare. Nivåerna skiljer sig mycket mellan scenarierna vad gäller myndiga (49,2 respektive 19,2 procent), föräldrar (20,8 respektive 10,4 procent) och förmyndare (24,4 respektive 15,6 procent).

5.2.2.6 Scenario 6 - DNA-lagring



Figur 17. Utvisar för scenario 6-1 och 6-2 resultatet för frågan "Jag anser denna teknik kan användas av".

Önskan (3,08 respektive 3,22) och den aktiva efterfrågan (2,60 respektive 2,68) är i enlighet med acceptansnivån måttligt hög och skiljer sig knappt i favör till den polisiära tillämpningen.

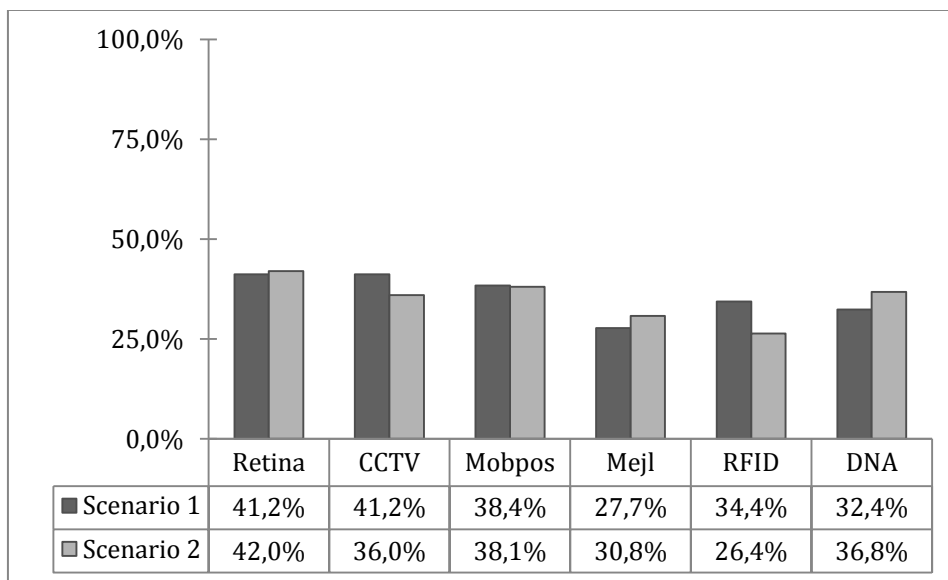
Enda noterbara skillnaden i användarfrågan, som visas i Figur 17, är att förmyndare anses lämpliga i högre grad för forskning än för den polisiära tillämpningen (32,8 respektive 25,6 procent). För både myndiga (55,2 respektive 54,4 procent) och föräldrar (27,6 respektive 27,2 procent) är resultaten däremot praktiskt taget lika.

5.2.3 FRIVILLIGHET

Under kategorin frivillighet återfinns följande frågor:

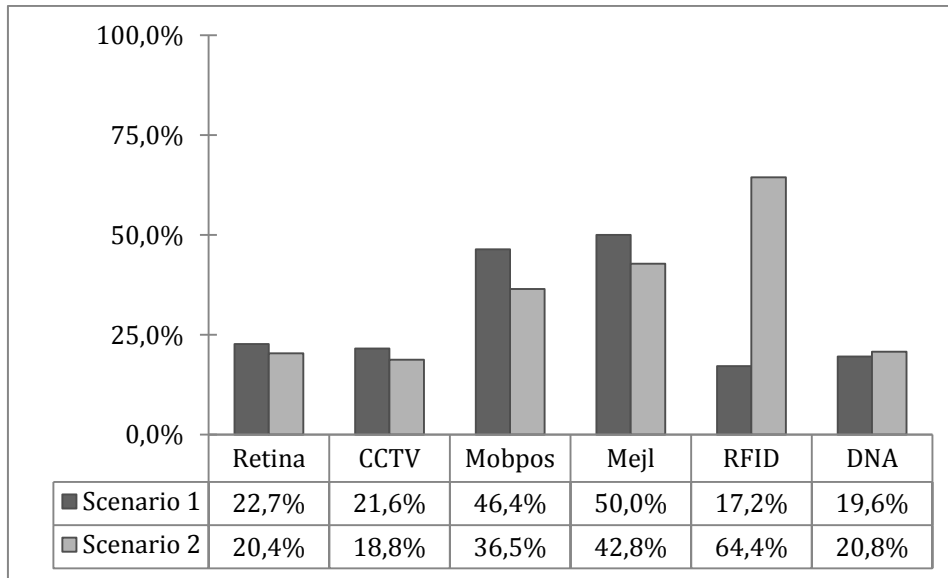
- Skulle du söka information om denna tillämpning av tekniken (ja/nej)?
- Skulle du aktivt arbeta för att undvika att du själv sätts i denna situation (ja/nej)?
- I vilken utsträckning skulle du diskutera denna tillämpning av tekniken på detta sätt (1-5):
 - Med personer på din arbetsplats.
 - Med relevant myndighet.
 - Med relevant företag.
 - Med dina förtroendevalda politiker.
 - Med din familj och dina vänner.

Resultaten från den sista frågan har bedömts som svåra att tolka på något tillfredsställande sätt varför endast jämförelser mellan delscenarierna har gjorts.



Figur 18. Utvisar för samtliga scenarier hur stor andel av respondenterna som svarar jakande på frågan "Skulle du söka information om denna tillämpning av tekniken".

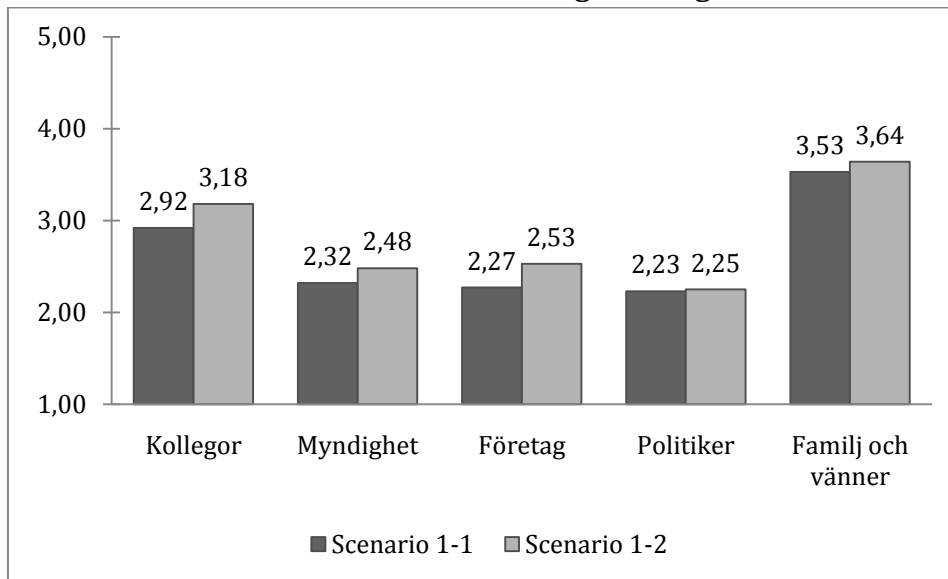
Figur 18 visar att andelen respondenter som anger att de skulle söka information om tillämpningen är ganska likvärdig mellan samtliga scenarier. Benägenheten att söka mer information verkar vara större för tillämpningar med högre acceptansnivåer.



Figur 19. Utvisar för samtliga scenarier hur stor andel av respondenterna som svarar jakande på frågan "Skulle du aktivt arbeta för att undvika att du själv sätts i denna situation".

I Figur 19 framgår för samtliga scenarier hur stor andel av respondenterna som uppger att de skulle undvika att sättas i en övervakningssituation. Detta resultat undersöks närmare under respektive scenario.

5.2.3.1 Scenario 1 - Näthinnefotografering

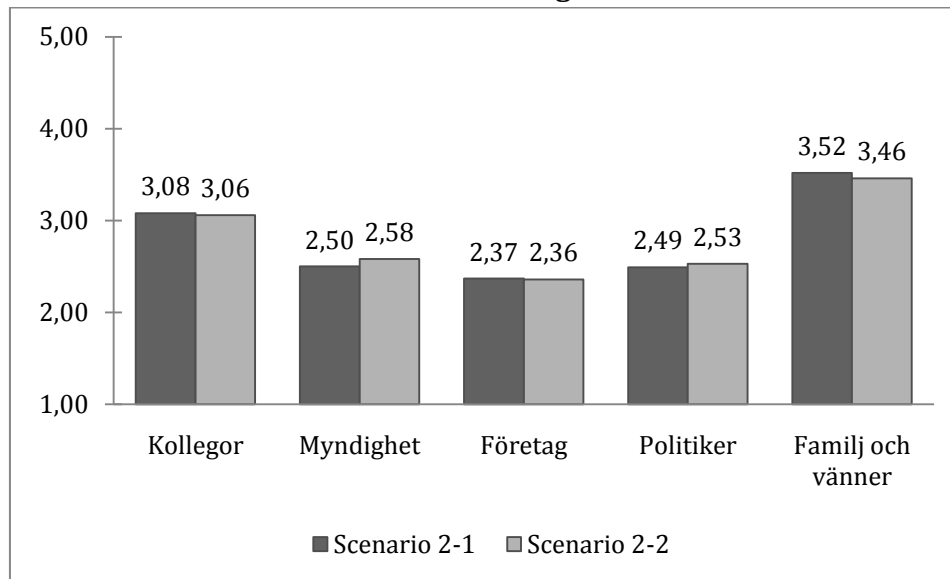


Figur 20. Utvisar för scenario 1-1 och 1-2 resultatet för frågan "I vilken utsträckning skulle du diskutera denna tillämpning av tekniken på detta sätt".

Andelen respondenter som skulle söka information (41,2 respektive 42,0 procent) och undvika situationen helt (22,7 respektive 20,4 procent) är ganska likartad för båda scenarier. Bekvämlighetstillämpningen skulle enligt Figur 20 i allmänhet diskuteras i något högre grad än säkerhetstillämpningen.

Jämför man med frågan om huruvida respondenterna anser att användningen är integritetskränkande så finner man att det är en större andel av respondenterna som uppger att de skulle undvika situationen (22,7 respektive 20,4 procent) än som tycker att den är integritetskränkande (18,1 respektive 21,2 procent). Detta är självklart ett anmärkningsvärt resultat som innebär att åtminstone en del av respondenterna undviker teknik som de inte anser vara integritetskränkande.

5.2.3.2 Scenario 2 – Övervakningskameror

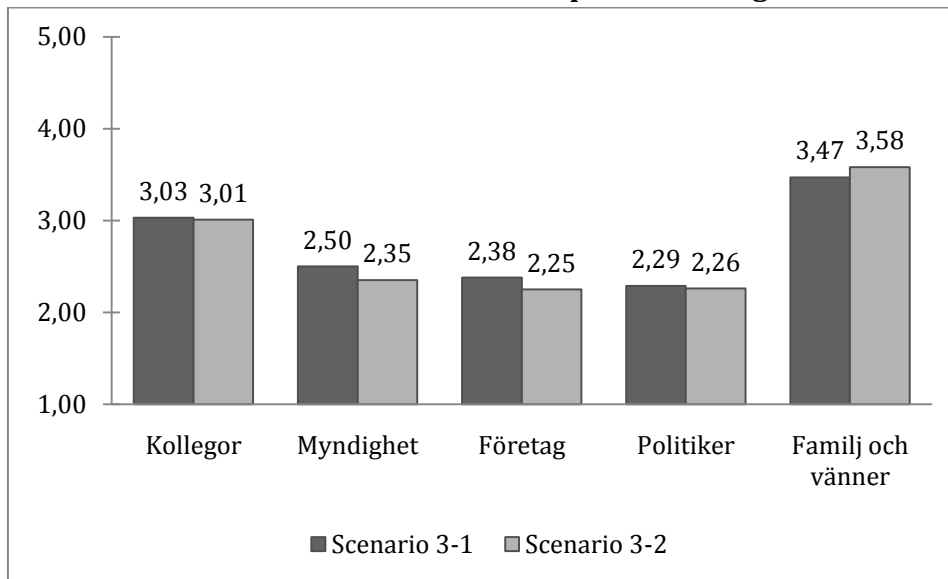


Figur 21. Utvisar för scenario 2-1 och 2-2 resultatet för frågan "I vilken utsträckning skulle du diskutera denna tillämpning av tekniken på detta sätt".

Resultaten är likartade men respondenterna skulle söka information (41,2 respektive 36,0 procent) och undvika (21,6 respektive 18,8 procent) konventionella övervakningskameror mer än dito utrustade med maskningsteknik. Figur 21 visar att båda tillämpningarna skulle diskuteras i ungefär samma utsträckning.

Observera att detta innebär att en relativt stor andel av respondenterna anser att tekniken är acceptabel men ändå uppger att de skulle försöka undvika den (acceptansen är i båda scenarierna över 90 procent). Det skulle således kunna tolkas som att den höga acceptansen beror på att den anses vara relativt lätt att undvika i jämförelse med annan teknik. Jämför dessutom med att endast 11,6 respektive 13,2 procent tycker användningen är integritetskränkande. Åtminstone knappt hälften av de som skulle undvika tekniken uppger alltså att de inte tycker att den är integritetskränkande.

5.2.3.3 Scenario 3 – Mobiltelefonpositionering

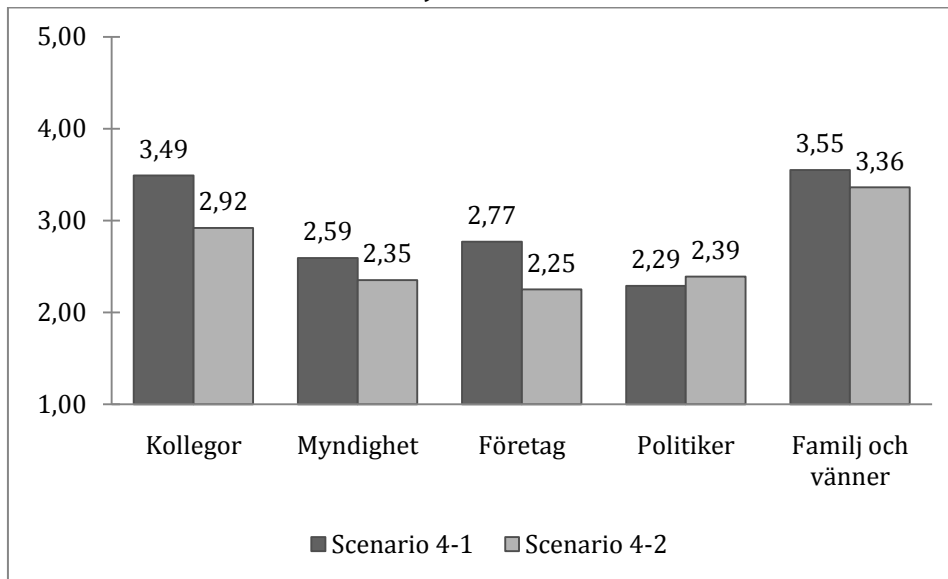


Figur 22. Utvisar för scenario 3-1 och 3-2 resultatet för frågan "I vilken utsträckning skulle du diskutera denna tillämpning av tekniken på detta sätt".

Båda tillämpningarna skulle innebära att ungefär lika stor andel av respondenterna skulle söka mer information (38,4 respektive 38,1 procent), men de skulle i mycket större utsträckning försöka undvika situationen där tekniken endast används som en kommersiell tjänst (46,4 procent respektive 36,5 procent). De skulle också i något högre grad diskutera denna tillämpning.

Återigen är det en relativt stor andel som accepterar tekniken men ändå skulle undvika den. Även här kan det bero på hur enkelt det verkar vara att avstå från övervakningen. Figur 22 visar inga större skillnader i vilken utsträckning tekniken diskuteras.

5.2.3.4 Scenario 4 - Mejlfilter

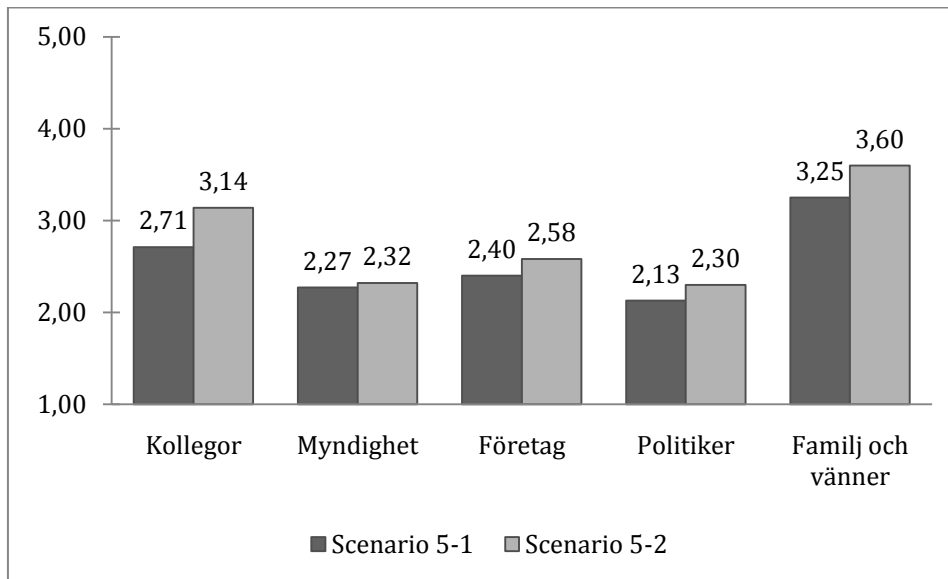


Figur 23. Utvisar för scenario 4-1 och 4-2 resultatet för frågan "I vilken utsträckning skulle du diskutera denna tillämpning av tekniken på detta sätt".

Respondenterna skulle söka mer information i ungefär samma utsträckning (27,7 respektive 30,8 procent), men undvika (50,0 respektive 42,8 procent) situationen där mejlfilter används av arbetsgivaren i större grad. Det är dessutom något fler som uppger att de skulle undvika arbetsgivarens tillämpning än vad som anser att den är integritetskränkande (47,3 procent). Enligt Figur 23 skulle den också diskuteras i högre grad än användningen för nationell säkerhet.

Trots dessa siffror så är acceptansen måttligt hög med nivåerna 61,7 respektive 66,0 procent.

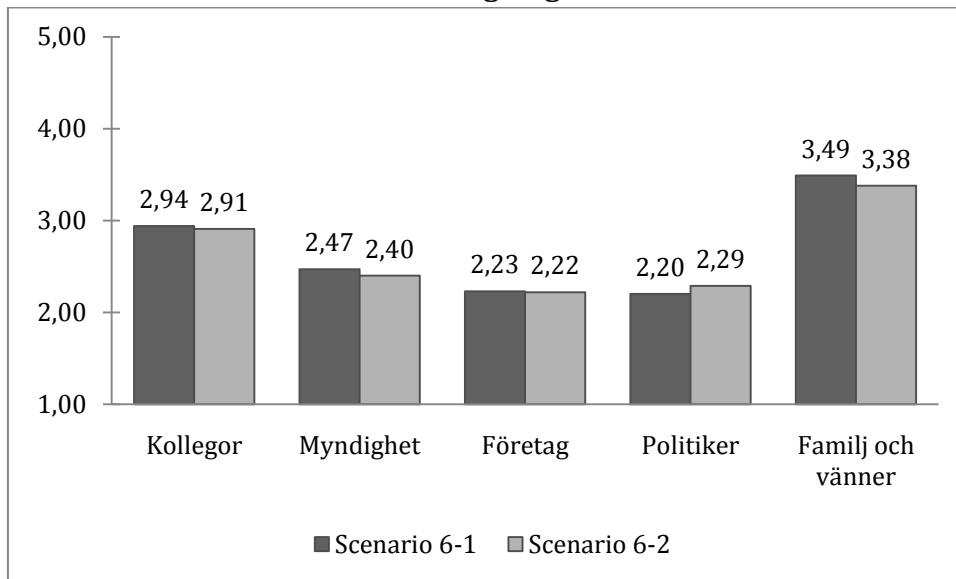
5.2.3.5 Scenario 5 – RFID



Figur 24. Utvisar för scenario 5-1 och 5-2 resultatet för frågan "I vilken utsträckning skulle du diskutera denna tillämpning av tekniken på detta sätt".

Tillämpningen för kläder är mycket impopulär och hela 64,4 procent väljer att undvika situationen helt, mot 17,2 procent för kollektivtrafiken. Fler väljer dock att söka mer information om kollektivtrafiken (34,4 respektive 26,4 procent) men det antas betyda att respondenterna helt enkelt inte ens tycker det är värt att veta mer om klädtillämpningen utan bojkottar den direkt. Figur 24 visar föga förvånande att den också uppges skulle leda till mer diskussion.

5.2.3.6 Scenario 6 - DNA-lagring



Figur 25. Utvisar för scenario 6-1 och 6-2 resultatet för frågan "I vilken utsträckning skulle du diskutera denna tillämpning av tekniken på detta sätt".

Svaren är likartade, 32,4 respektive 36,8 procent skulle söka mer information och 19,6 respektive 20,8 procent skulle undvika tekniken helt.

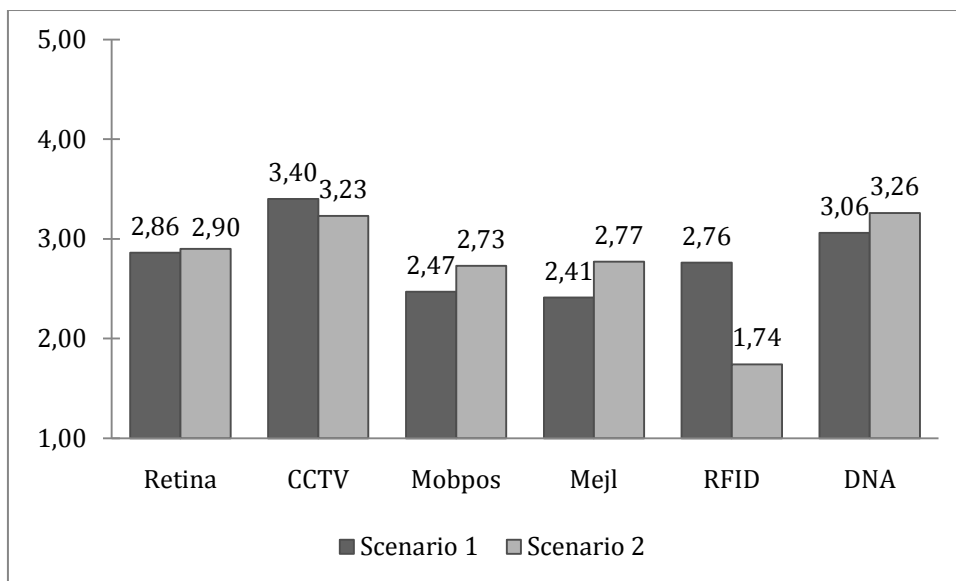
Även när det gäller vilka respondenterna skulle välja att diskutera användningen med är resultaten likartade, se Figur 25.

5.2.4 FÖRDELAR/NACKDELAR

I denna kategori finns frågorna som behandlar de fördelar och nackdelar teknikanvändningen medför och huruvida den information som samlas är nödvändig och användbar. Dessa frågor fick respondenterna besvara:

- Anser du att denna tillämpning av tekniken har: Många nackdelar – många fördelar (1-5)?
- Hur skulle du skatta denna teknikutveckling: En dålig tillämpning – en bra tillämpning (1-5)?
- Att samla in denna typ av information är:
 - Inte alls nödvändig – helt nödvändig (1-5).
 - Inte alls användbart – mycket användbart (1-5).

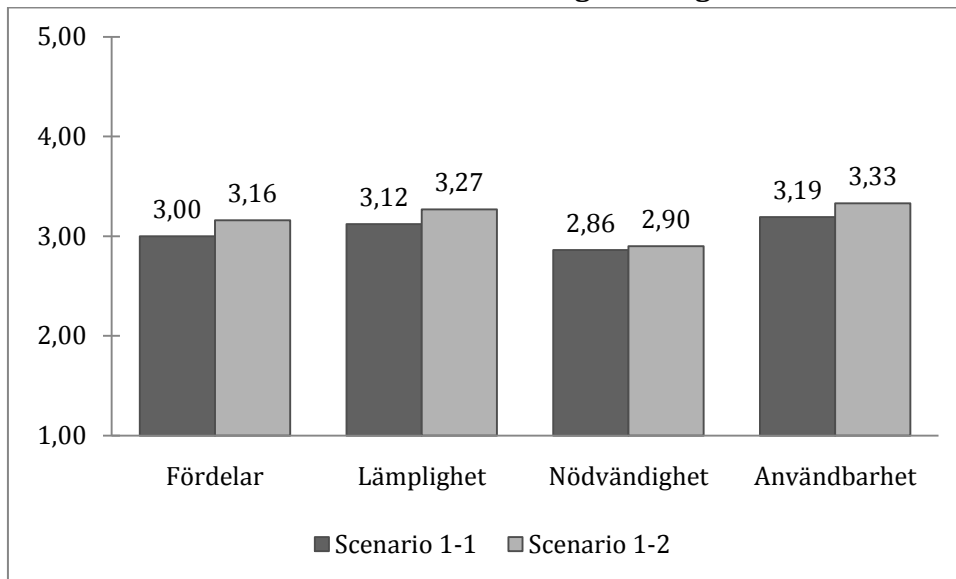
Den näst sista frågan redovisas två gånger: Först i en figur där samtliga scenarier ingår, och sedan tillsammans med övriga frågor för respektive teknik. Detta för att kunna göra en jämförelse mellan olika tekniker.



Figur 26. Utvisar för samtliga scenarier resultatet för frågan "Att samla in denna typ av information är: Inte alls nödvändig – helt nödvändig".

Figur 26 visar att det inte är entydigt huruvida informationsinsamling för säkerhetstillämpningar premieras. Resultaten skiljer sig heller inte nämnvärt från vad som kunde förväntas med tanke på övriga resultat, så som acceptans. Den skillnad som föreligger är att näthinnefotografering (retina) och RFID för lokaltrafik (scenario 1) skattas märkbart lägre än övervakningskameror och DNA-lagring, trots att dessa fyra hade liknande acceptansnivåer. Däremot verkar det stämma bra överens med frågan om huruvida tekniken är samhällsförbättrande, se 5.2.1.

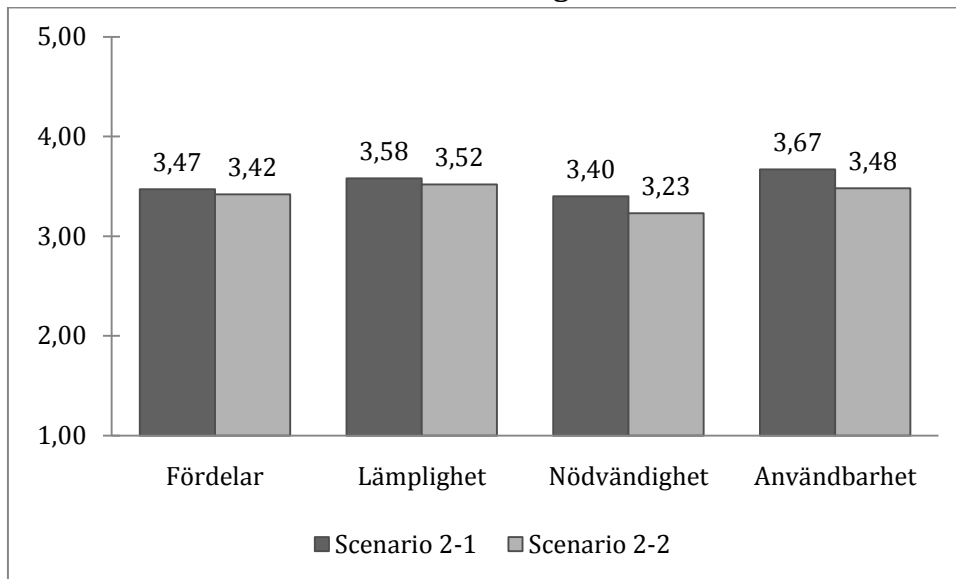
5.2.4.1 Scenario 1 - Näthinnefotografering



Figur 27. Utvisar för scenario 1-1 och 1-2 resultaten för frågorna "Anser du att denna tillämpning av tekniken har: Många nackdelar - många fördelar", " Hur skulle du skatta denna teknikutveckling: En dålig tillämpning - en bra tillämpning", "Att samla in denna typ av information är: Inte alls nödvändig - helt nödvändig", samt "Att samla in denna typ av information är: Inte alls användbart - mycket användbart".

I termer av fördelar och nackdelar föredrar respondenterna bekvämlighetstillämpningen något trots att den hade lite lägre acceptansnivå, se Figur 27. Skillnaderna är små men det visar trots allt att det inte finns ett direkt samband mellan fördelar och acceptans. Däremot så stämmer det överens med respondenternas uppfattning om att bekvämlighetstillämpningen är något mer samhällsförbättrande.

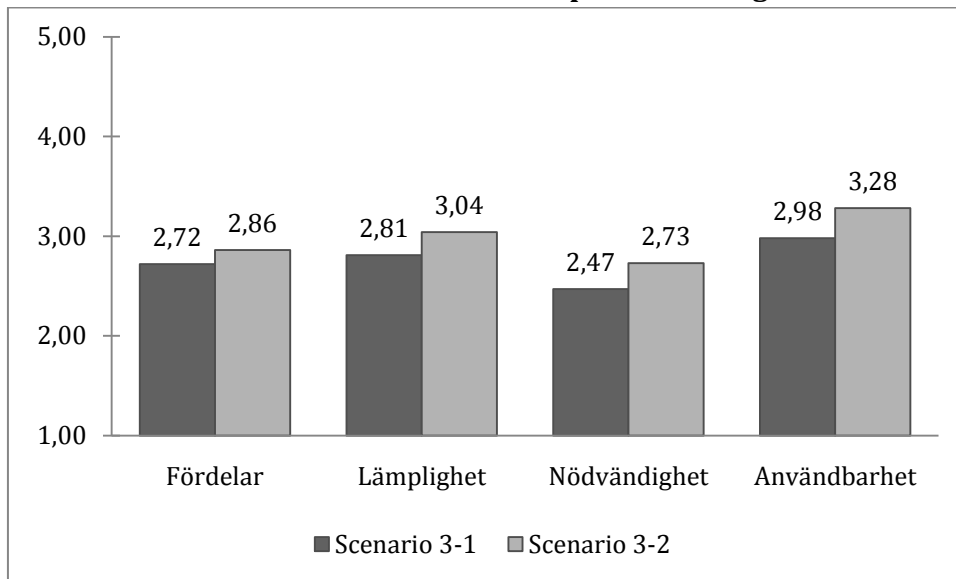
5.2.4.2 Scenario 2 - Övervakningskameror



Figur 28. Utvisar för scenario 2-1 och 2-2 resultaten för frågorna "Anser du att denna tillämpning av tekniken har: Många nackdelar - många fördelar", " Hur skulle du skatta denna teknikutveckling: En dålig tillämpning - en bra tillämpning", "Att samla in denna typ av information är: Inte alls nödvändig - helt nödvändig", samt "Att samla in denna typ av information är: Inte alls användbart - mycket användbart"..

Skillnaderna i acceptans var mycket små och så är även skattningen av fördelar, vilket Figur 28 visar. Den konventionella kameraövervakningen utan maskning skattas dock något högre, vilket också är i linje med att den värderades som mer samhällsförbättrande. Det bör dock nämnas att fördelarna värderas högt för båda delscenarierna.

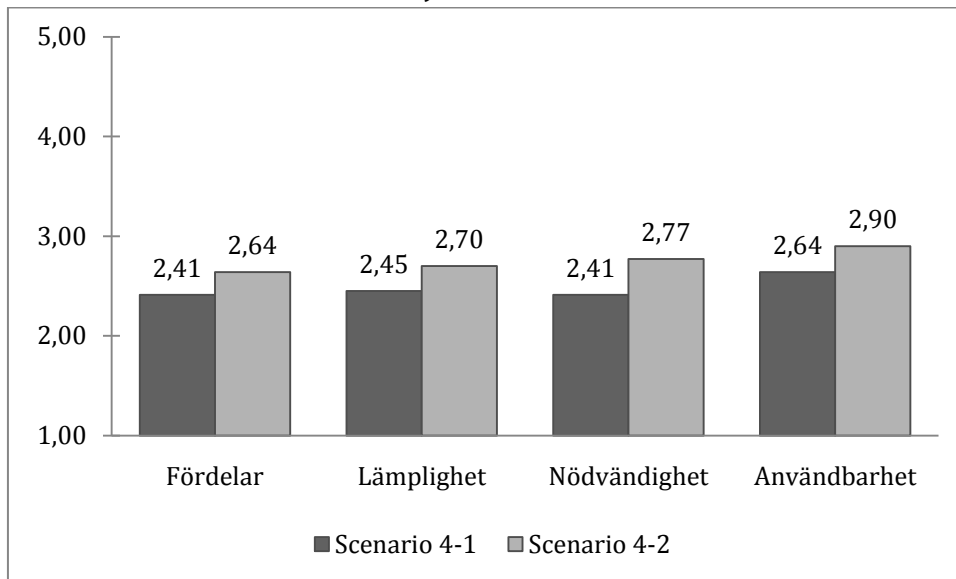
5.2.4.3 Scenario 3 – Mobiltelefonpositionering



Figur 29. Utvisar för scenario 3-1 och 3-2 resultaten för frågorna "Anser du att denna tillämpning av tekniken har: Många nackdelar - många fördelar", " Hur skulle du skatta denna teknikutveckling: En dålig tillämpning - en bra tillämpning", "Att samla in denna typ av information är: Inte alls nödvändig - helt nödvändig", samt "Att samla in denna typ av information är: Inte alls användbart - mycket användbart"..

Fördelarna skattas relativt högt och med en fördel för den polisiära tillämpningen, se Figur 29. Detta trots att endast 37,5 respektive 46,4 procent anser att tekniken bidrar till att förbättra samhället.

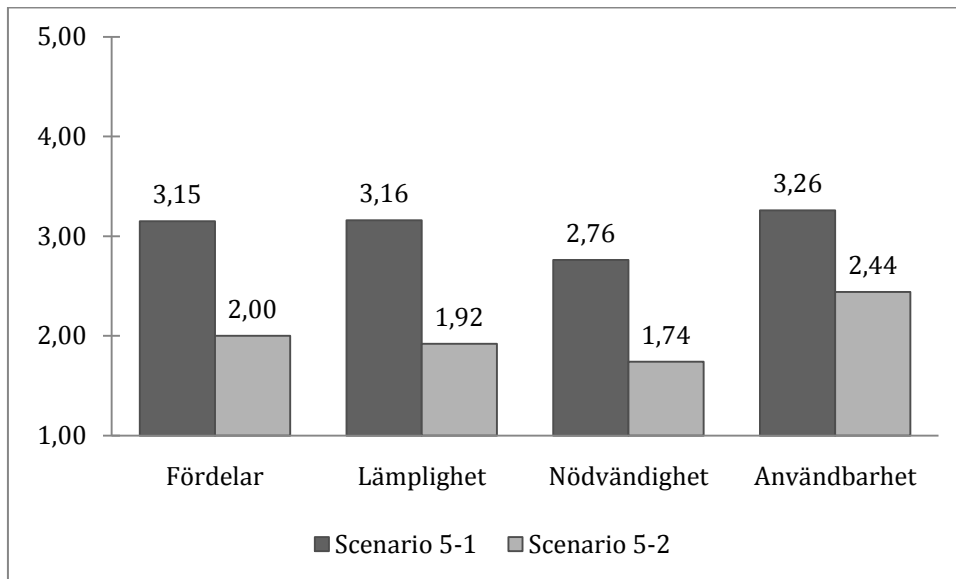
5.2.4.4 Scenario 4 - Mejlfilter



Figur 30. Utvisar för scenario 4-1 och 4-2 resultaten för frågorna "Anser du att denna tillämpning av tekniken har: Många nackdelar - många fördelar", " Hur skulle du skatta denna teknikutveckling: En dålig tillämpning - en bra tillämpning", "Att samla in denna typ av information är: Inte alls nödvändig - helt nödvändig", samt "Att samla in denna typ av information är: Inte alls användbart - mycket användbart".

Denna teknik hade likartade resultat som mobiltelefonpositionering för acceptans, samhällsförbättring och huruvida tekniken är integritetskränkande. Trots det värderas tekniken märkbart lägre på det här området, se Figur 30. Tillämpningen för nationell säkerhet värderas också högre än den för företagssäkerhet.

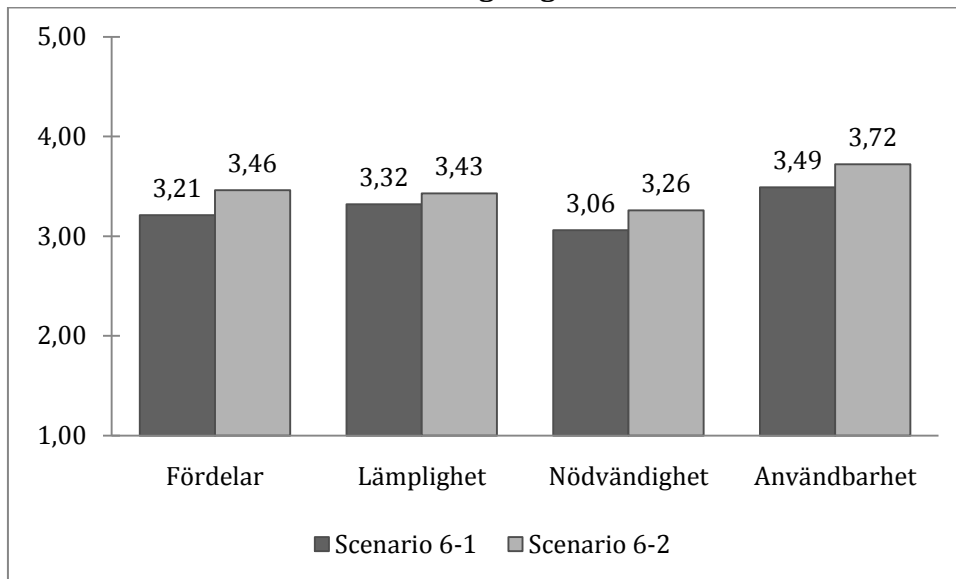
5.2.4.5 Scenario 5 - RFID



Figur 31. Utvisar för scenario 5-1 och 5-2 resultaten för frågorna "Anser du att denna tillämpning av tekniken har: Många nackdelar - många fördelar", " Hur skulle du skatta denna teknikutveckling: En dålig tillämpning - en bra tillämpning", "Att samla in denna typ av information är: Inte alls nödvändig - helt nödvändig", samt "Att samla in denna typ av information är: Inte alls användbart - mycket användbart".

Återigen visar respondenterna stor skepsis mot den tillämpning som innebär RFID-teknik i kläder, vilket kan ses i Figur 31. Trots detta får användbarheten överraskande hög skattning.

5.2.4.6 Scenario 6 - DNA-lagring



Figur 32. Utvisar för scenario 6-1 och 6-2 resultaten för frågorna "Anser du att denna tillämpning av tekniken har: Många nackdelar - många fördelar", " Hur skulle du skatta denna teknikutveckling: En dålig tillämpning - en bra tillämpning", "Att samla in denna typ av information är: Inte alls nödvändig - helt nödvändig", samt "Att samla in denna typ av information är: Inte alls användbart - mycket användbart".

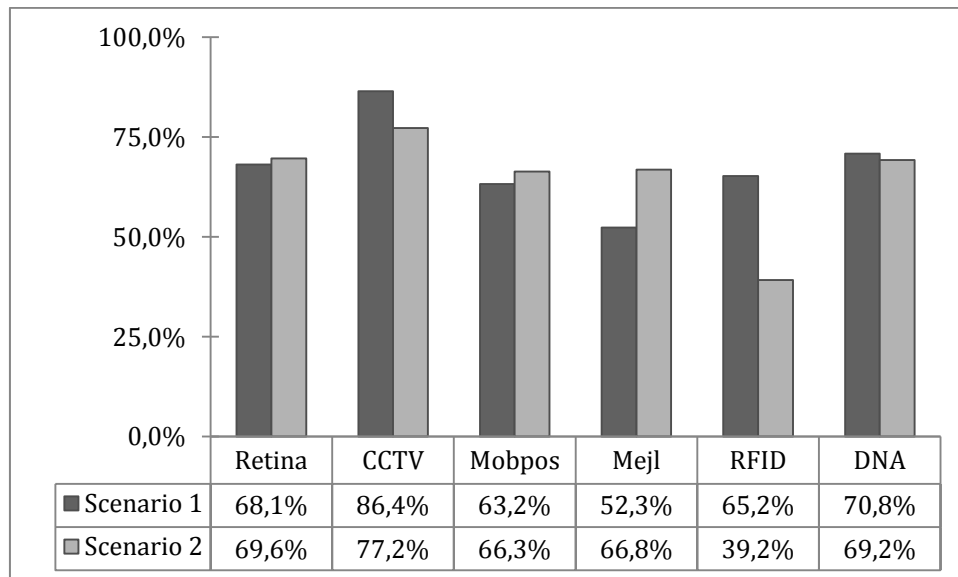
Den höga acceptansnivån och samhällförbättringen speglas i Figur 32 som utvisar de bedömda fördelarna. Den polisiära användningen får något större stöd än forskningsanvändningen..

5.2.5 TILLIT/MISSBRUK

Denna kategori rör frågor om tillit och missbruk, där dessa frågor ingår:

- I vilken utsträckning litar du på de aktörer som samlar in denna information? Inte alls – hög utsträckning (1-5).
- Hur stor risk tror du det är för att denna information kan missbrukas? Ingen risk – mycket stor risk (1-5).
- Anser du att detta är en risk som vi bör ta på samhällsnivå (ja/nej)?
- Hur pass orolig över denna utveckling och användning av teknik är du? Inte alls – mycket orolig (1-5).
 - Till alla som svarat mellan 3 och 5 på föregående fråga: Vad är du orolig för (öppet svar)?
- Hur pass stött eller upprörd blir du när du tänker på denna utveckling och användning av olika tekniker som kan användas för övervakning (1-5)?

Eftersom denna rapport har fokus på offentlig riskhantering anses frågan om huruvida risken bör tas på samhällsnivå vara särskilt intressant, varför den har en framträdande roll i denna del.



Figur 33. Utvisar för samtliga scenarier hur stor andel av respondenterna som svarar jakande på frågan "Anser du att detta är en risk som vi bör ta på samhällsnivå?".

Resultaten som redovisas i Figur 33 är intressanta att jämföra mot acceptansnivån. Bara för att en teknik är accepterad behöver man självklart inte nödvändigtvis tycka att den lämpar sig som ett samhällsligt åtagande.

Näthinnefotografering

För denna teknik ligger siffrorna ungefär 15 respektive 10 procentenheter under acceptansnivån. Överraskande nog tycker respondenterna alltså att bekvämlighetstillämpningen är något mer lämpad som samhällsligt åtagande.

Övervakningskameror

Differensen är ungefär 7 respektive 15 procentenheter mot acceptansen. Acceptansen var hög och likartad för båda tillämpningarna men här framgår alltså att respondenterna anser att övervakningskameror utan maskningsteknik lämpar sig bättre på samhällsnivå.

Mobiltelefonpositionering

Den polisiära användningen anses bättre lämpad som samhälleligt åtagande, men differensen jämfört med acceptansnivån är mindre (i princip noll) för den kommersiella tjänsten.

Mejlfiler

Tillämpningen för nationell säkerhet anses vara mest lämpad och skiljer sig också i princip ingenting mot acceptansnivån, vilket måste ses som väntat eftersom det är svårt att se hur detta skulle genomföras på annat sätt än på en samhällelig nivå.

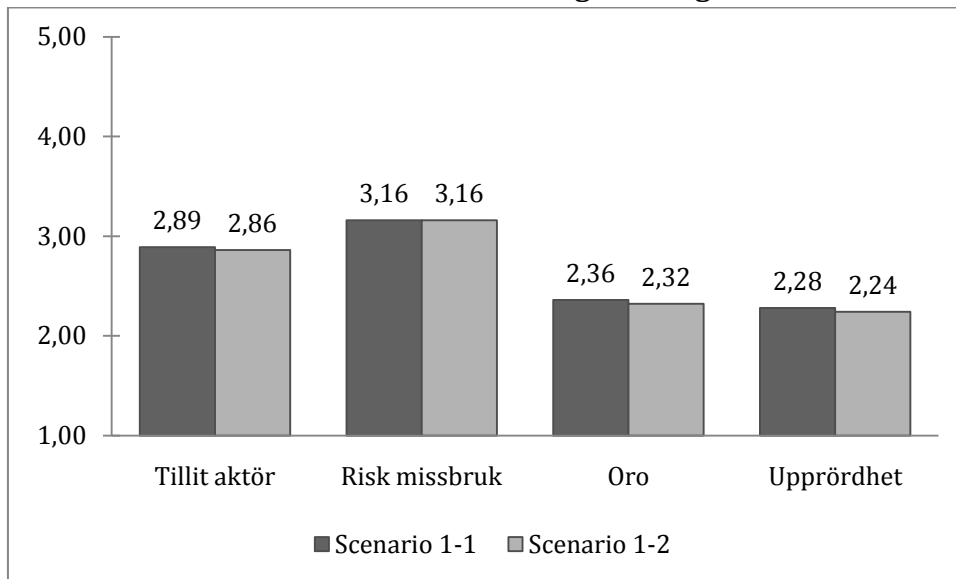
RFID

Den mest intressanta tekniken i detta avseende. Tillämpningen i kollektivtrafiken är väldigt väl accepterad, men anses i stor utsträckning vara illa lämpad på samhällsnivå. Differensen är ungefär 21 procentenheter. För tillämpningen i kläder är det anmärkningsvärt nog ungefär 9 procentenheter fler som anser att risken bör tas på samhällsnivå än som anser att tekniken är acceptabel. Detta skulle kunna tänkas bero på att respondenterna helt enkelt har tolkat det som om användningen av tekniken skulle varit annorlunda på samhällsnivå.

DNA-lagring

Differensen gentemot acceptansnivån är ganska likartad för båda scenarier(ungefär 9 respektive 11 procentenheter) där den polisiära tillämpningen anses något mindre lämplig trots att den är något mer accepterad.

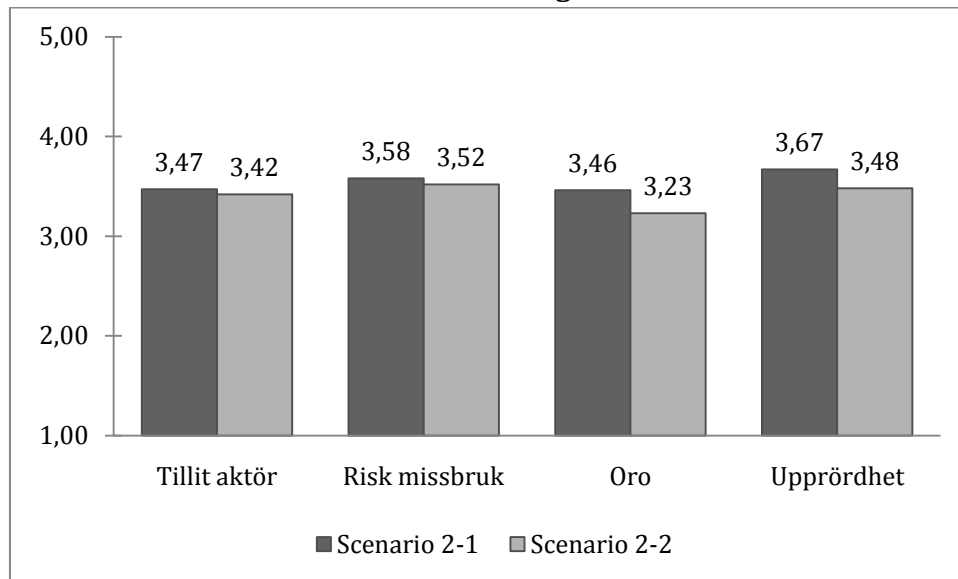
5.2.5.1 Scenario 1 - Näthinnefotografering



Figur 34. Utvisar för scenario 1-1 och 1-2 resultaten på frågorna "I vilken utsträckning litar du på de aktörer som samlar in denna information?", "Hur stor risk tror du det är för att denna information kan missbrukas?", "Hur pass orolig över denna utveckling och användning av teknik är du?" samt "Hur pass stött eller upprörd blir du när du tänker på denna utveckling och användning av olika tekniker som kan användas för övervakning?".

Figur 34 visar i princip samma resultat för båda delscenarierna. Trots att en statlig myndighet alltså var inblandad i första delscenariot, men inte andra. Anmärkningsvärt är att risken för missbrukas skattas högt trots att tilliten är måttlig och oron låg.

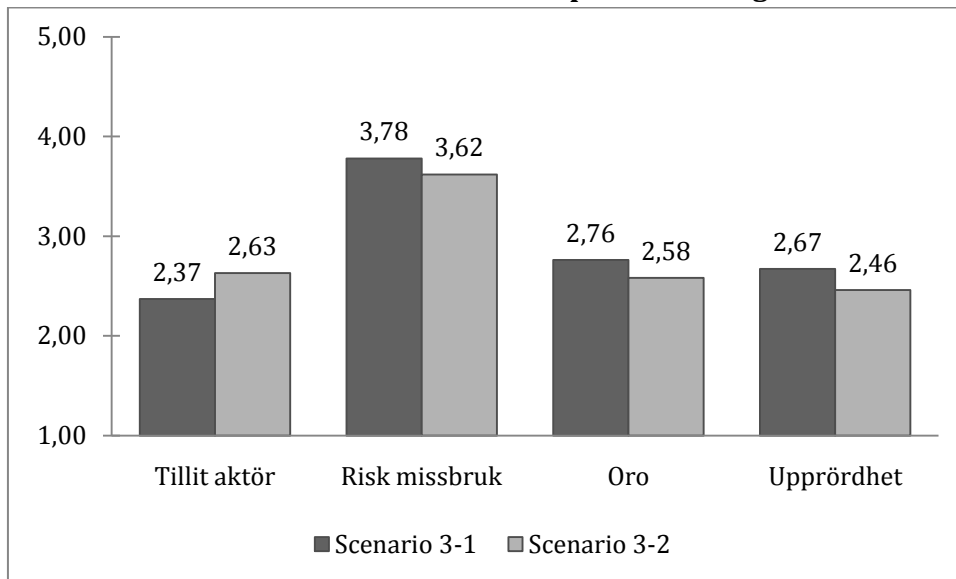
5.2.5.2 Scenario 2 - Övervakningskameror



Figur 35. Utvisar för scenario 2-1 och 2-2 resultaten på frågorna "I vilken utsträckning litar du på de aktörer som samlar in denna information?", "Hur stor risk tror du det är för att denna information kan missbrukas?", "Hur pass orolig över denna utveckling och användning av teknik är du?" samt "Hur pass stött eller upprörd blir du när du tänker på denna utveckling och användning av olika tekniker som kan användas för övervakning?".

I Figur 35 är det intressant att notera hur stor risken för missbruk anses trots att tekniken är brett accepterad och tilliten är hög. Dessutom får tekniken högst skattning av oro och upprördhet, trots att den också innehar högst acceptansnivå. Här verkar det helt klart vara så att respondenterna får göra en kompromiss där de accepterar en teknik som upplevs medföra potentiellt stora konsekvenser för att den anses för innebära fördelar, här i form av ökad säkerhet. Vad som kan tyckas vara lite märkligt är att båda scenarierna har fått väldigt likartad skattning på missbruksrisken, trots att övervakningskameror med maskningsteknik torde vara betydligt svårare att missbruka än konventionella sådana.

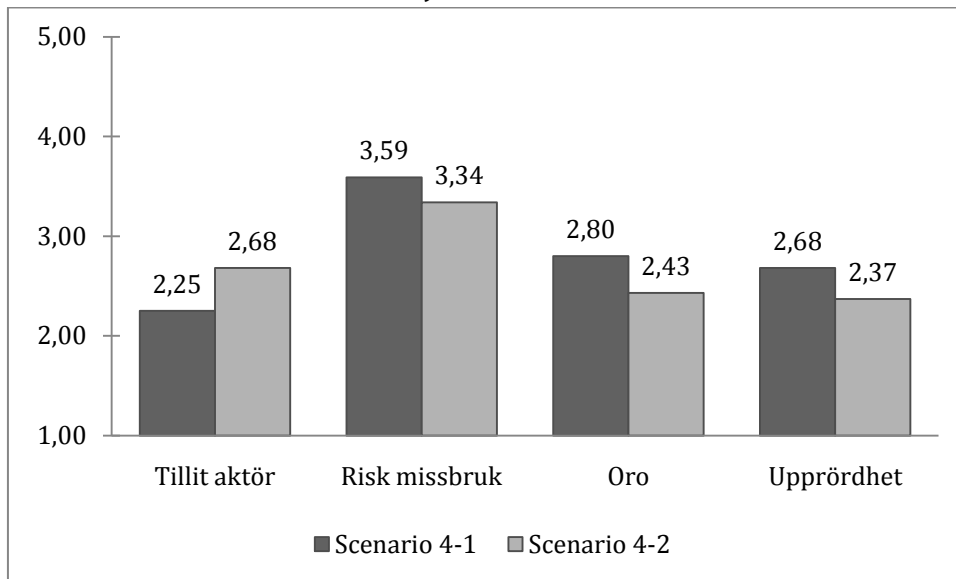
5.2.5.3 Scenario 3 – Mobiltelefonpositionering



Figur 36. Utvisar för scenario 3-1 och 3-2 resultaten på frågorna "I vilken utsträckning litar du på de aktörer som samlar in denna information?", "Hur stor risk tror du det är för att denna information kan missbrukas?", "Hur pass orolig över denna utveckling och användning av teknik är du?" samt "Hur pass stött eller upprörd blir du när du tänker på denna utveckling och användning av olika tekniker som kan användas för övervakning?".

Tilliten till aktören är måttlig och så även oron och upprördheten, se Figur 36. Risken för missbruk anses dock vara hög. Tilliten är också högre till den polisiära tillämpningen.

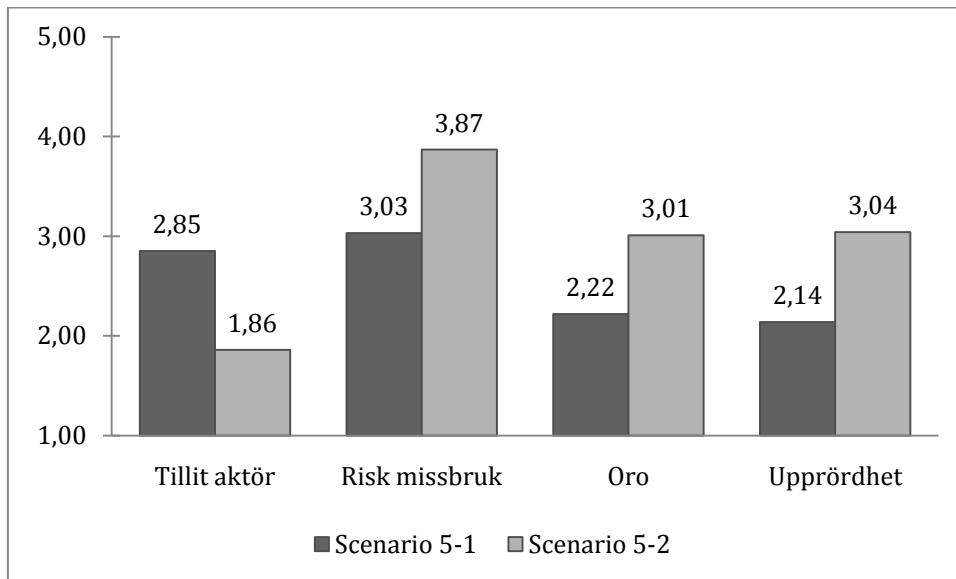
5.2.5.4 Scenario 4 - Mejlfilter



Figur 37. Utvisar för scenario 4-1 och 4-2 resultaten på frågorna "I vilken utsträckning litar du på de aktörer som samlar in denna information?", "Hur stor risk tror du det är för att denna information kan missbrukas?", "Hur pass orolig över denna utveckling och användning av teknik är du?" samt "Hur pass stött eller upprörd blir du när du tänker på denna utveckling och användning av olika tekniker som kan användas för övervakning?".

Figur 37 visar att tilliten är betydligt högre vid användningen för nationell säkerhet, vilket också speglas resultaten för övriga frågor. Respondenterna har dock bedömt missbruksrisken som ganska hög för båda delscenarierna.

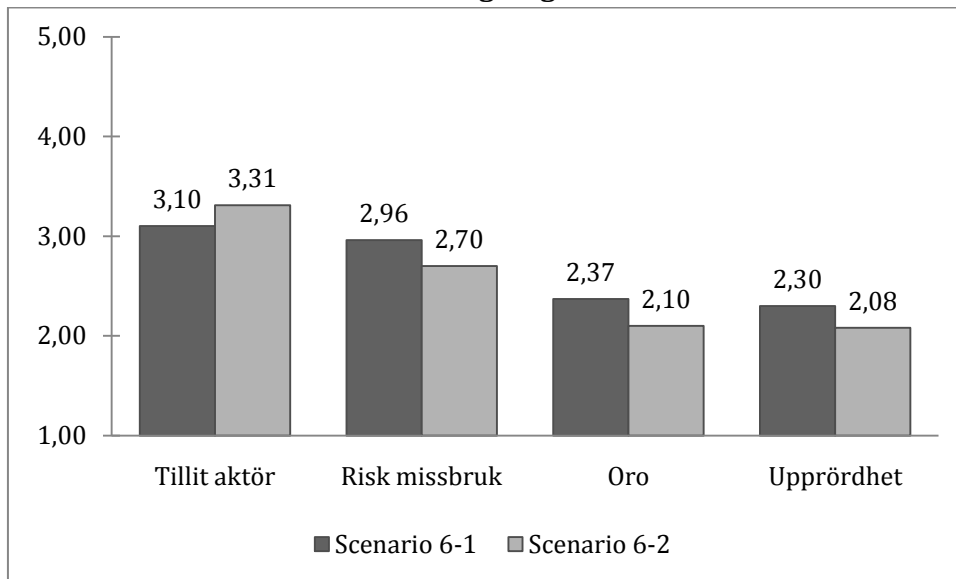
5.2.5.5 Scenario 5 - RFID



Figur 38. Utvisar för scenario 5-1 och 5-2 resultaten på frågorna "I vilken utsträckning litar du på de aktörer som samlar in denna information?", "Hur stor risk tror du det är för att denna information kan missbrukas?", "Hur pass orolig över denna utveckling och användning av teknik är du?" samt "Hur pass stött eller upprörd blir du när du tänker på denna utveckling och användning av olika tekniker som kan användas för övervakning?".

Figur 38 visar återigen dåliga siffror för scenario 5-2, som behandlar RFID i kläder. Skattningarna för scenario 5-1, RFID i lokaltrafiken, är betydligt mer moderata.

5.2.5.6 Scenario 6 - DNA-lagring



Figur 39. Utvisar för scenario 6-1 och 6-2 resultaten på frågorna "I vilken utsträckning litar du på de aktörer som samlar in denna information?", "Hur stor risk tror du det är för att denna information kan missbrukas?", "Hur pass orolig över denna utveckling och användning av teknik är du?" samt "Hur pass stött eller upprörd blir du när du tänker på denna utveckling och användning av olika tekniker som kan användas för övervakning?".

Respondenterna är genomgående mer positivt inställda till den polisiära användningen av DNA-lagring, även om tilliten är relativt hög vid båda delscenarierna, se Figur 39. Missbruksrisken är måttlig och både oro samt upprördhet bedöms som ganska låga.

6 ANALYS

I kapitel 5 redovisas och jämförs resultat från enkätstudien i form av medelvärden och som andelar av populationen. För att dra någorlunda säkra slutsatser utifrån materialet behövs det också kontrolleras huruvida det går att observera signifikanta skillnader, och i sådana fall till vilken grad de är signifikanta. I det här avsnittet görs detta med hjälp av statistiska metoder och de hypoteser som tidigare formulerats, se kapitel 4. De områden som studeras är demografiska faktorer, kontextuella faktorer och kognitiva faktorer.

Resonemanget för huruvida hypoteser förkastats eller inte görs på ett nyanserat sätt för att inte ge det felaktiga intrycket av att signifikansnivån 0,05 är någon skarp gräns för vad som utgör verkligheten. I samtliga fall gäller dock att nollhypotesen anses kunna förkastas om det visar sig att signifikanta skillnader uppmätts i fler än hälften av de undersökta scenarierna.

6.1 DEMOGRAFISKA FAKTORER

De demografiska faktorer som studeras är variablerna kön, föräldraskap och ålder. Fyra frågor väljs ut från enkäten för vidare analys:

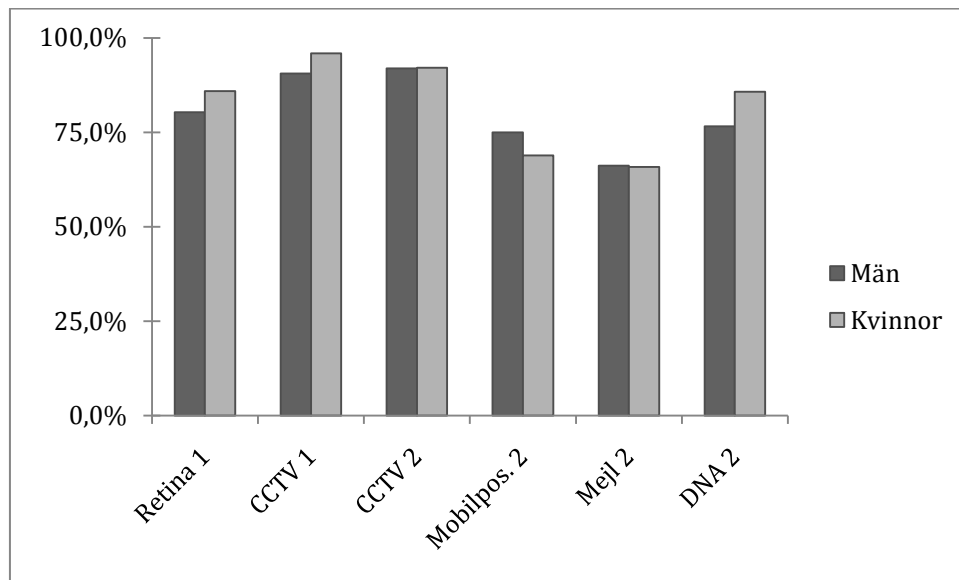
1. Anser du denna typ av användning av teknik är acceptabel? (ja/nej)
2. Anser du denna typ av användning av teknik som integritetskränkande? (ja/nej)
3. I vilken utsträckning litar du på de aktörer som samlar in denna information? (1-5)
4. Hur skulle du skatta denna teknikutveckling? (1-5)

Dessa väljs för att för att fånga in de fyra dimensionerna acceptans, integritet, tillit och effektivitet – men också för att både få med binära svar (ja/nej) såväl som svar på ordinalskala (1-5).

Nedan presenteras först hur de olika grupperna har besvarat de utvalda frågorna, sedan redovisas utgången av de statistiska testen i form av signifikansnivåer och slutligen analyseras resultatet. Eftersom rapporten fokuserar på offentlig riskhantering används endast de scenarier som innebär någon form av offentlig säkerhetsåtgärd, det vill säga scenario 1-1 (*Retina 1*), 2-1 (*CCTV 1*), 2-2 (*CCTV 2*), 3-2 (*Mobpos 2*), 4-2 (*Mejl 2*) och 6-2 (*DNA 2*).

6.1.1 KÖN

I litteraturstudien framgick det att skillnader mellan könen har observerats när det gäller riskperception. Kvinnor upplever i allmänhet större utsatthet än män och bedömer därför också risker som större än män. Går det att finna sådana skillnader även när det gäller integritetskränkande teknik och visar det sig då genom högre acceptans för tekniken eller större skepsis?



Figur 40. Utvisar för valda scenarier stor del av respondenterna som svarar jakande på frågan "Anser du denna typ av användning av teknik är acceptabel?", uppdelat på kön,

För att visa en översiktlig bild av skillnaderna mellan könen redovisas i Figur 40 hur män och kvinnor bedömer acceptansen i de olika säkerhetsscenarierna. Det går att ana en trend som innebär att kvinnor i högre grad accepterar teknikanvändningen, men sambandet verkar inte starkt. För ett scenario uppger männen rentav högre acceptans än kvinnorna, och för två andra scenarier är acceptansnivåerna praktiskt identiska. Resultaten från de statistiska hypotesprövningar som görs på de fyra utvalda frågorna redovisas i Tabell 1.

Tabell 1. Utvisar för valda scenarier och frågor signifikansnivåerna för nollhypotesen, att kön inte påverkar hur respondenterna har svarat. Signifikanta skillnader (under signifikansnivån 0,05) har markerats.

	Retina 1	CCTV 1	CCTV 2	Mobilpos 2	Mejlfilter 2	DNA 2
Fråga 1	0,227	0,098	0,941	0,286	0,944	0,082
Fråga 2	0,003	0,102	0,303	0,857	0,807	0,075
Fråga 3	0,279	0,332	0,336	0,623	0,536	0,384
Fråga 4	0,492	0,012	1,000	0,115	0,862	0,360

I tabellen går det att utläsa att det överhuvudtaget inte går att observera någon signifikant skillnad vad gäller acceptansen. De enda skillnaderna som är signifikanta rör huruvida scenario 1-1 (retina 1) bedöms som integritetskränkande och om scenario 2-1 (CCTV 1) utgör en lämplig teknikanvändning. I

Tabell 2 redovisas hur män respektive kvinnor har svarat i de aktuella frågorna.

Tabell 2. Resultaten för valda scenarier och frågor, uppdelat på kön. Signifikanta skillnader (under signifikansnivån 0,05) har markerats.

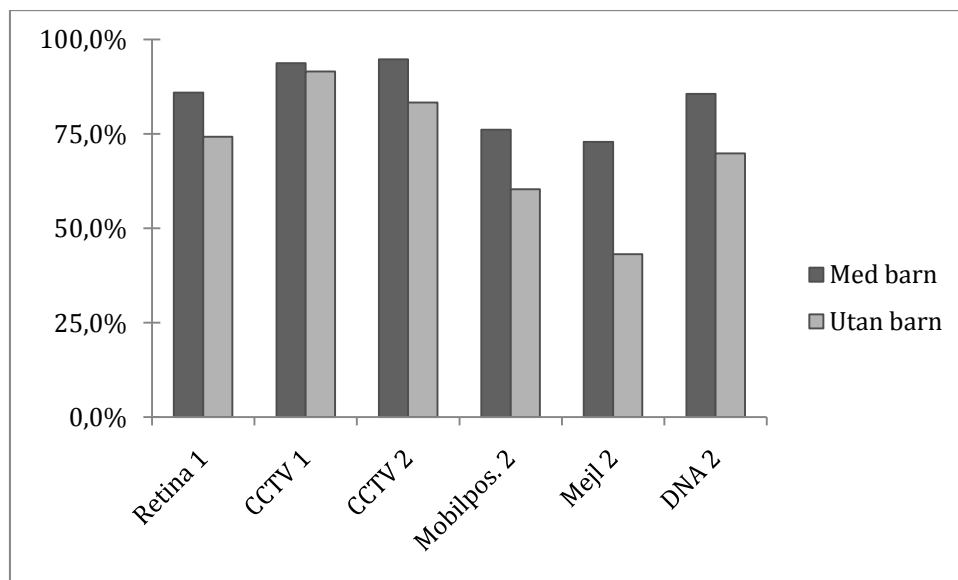
	Retina 1		CCTV 1		CCTV 2		Mobpos 2		Mejlfilter 2		DNA 2	
	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor
1	80,3	85,9	90,6	95,9	91,9	92,1	75,0	68,9	66,2	65,8	76,6	85,7
2	25,0	10,9	14,8	8,2	15,4	11,0	45,8	47,0	43,9	42,3	31,3	21,3
3	2,81	2,97	3,28	3,17	3,06	3,24	2,67	2,60	2,63	2,73	3,36	3,26
4	3,06	3,19	3,70	3,47	3,51	3,53	3,16	2,94	2,72	2,68	3,48	3,38

Det går alltså att konstatera att män i högre grad än kvinnor anser att näthinnefotografering är en integritetskränkande säkerhetsteknik och att konventionella övervakningskameror är en lämplig teknikanvändning. Övriga skillnader går det inte att säkert bekräfta.

Nollhypotesen, att respondenternas kön inte påverkar acceptansen, kan därför inte förkastas.

6.1.2 FÖRÄLDRASKAP

Det är inte svårt att intuitivt förstå varför personer som har barn bedömer risker som större än de utan barn, vilket framgick i litteraturstudien. Det borde även betyda att de i högre grad även accepterar teknik som syftar till att öka säkerhet. I Figur 41 framgår hur de två grupperna skiljer sig när det gäller acceptansen i för de aktuella scenarierna.



Figur 41. Utvisar för studerade scenarier hur stor andel av respondenterna, som svarar jakande på frågan "Anser du denna typ av användning av teknik är acceptabel?", uppdelat på respondenter med barn respektive utan barn.

Här går det genomgående att skönja ett ganska starkt samband mellan föräldraskap och en högre acceptans. Huruvida detta samband går att XX som signifikant görs med hypotesprövningarna, vilka redovisas i Tabell 3. Sambandet är uppenbarligen mycket starkt.

Tabell 3. Utvisar för valda scenarier och frågor signifikansnivåerna för nollhypotesen, att föräldraskap inte påverkar hur respondenterna har svarat. Signifikanta skillnader (under signifikansnivån 0,05) har markerats.

	Retina 1	CCTV 1	CCTV 2	Mobpos 2	Mejlfiler 2	DNA 2
Fråga 1	0,033	0,560	0,005	0,014	0,000	0,007
Fråga 2	0,010	0,004	0,008	0,000	0,003	0,043
Fråga 3	0,037	0,003	0,051	0,008	0,002	0,039
Fråga 4	0,059	0,088	0,051	0,001	0,000	0,033

För samtlig säkerhetsteknik förutom konventionella övervakningskameror går det att med stor säkerhet säga att det föreligger skillnader både vad gäller acceptans och huruvida tekniken upplevs vara integritetskränkande. Vidare föreligger det även stora skillnader för frågorna om tillit respektive lämplighet, men i några fall ligger signifikansnivån precis över 0,05 och kan därför inte sägas vara bekräftad.

Tabell 4. Resultaten för valda scenarier och frågor, uppdelat på respondenter med barn respektive utan barn. Signifikanta skillnader (under signifikansnivån 0,05) har markerats.

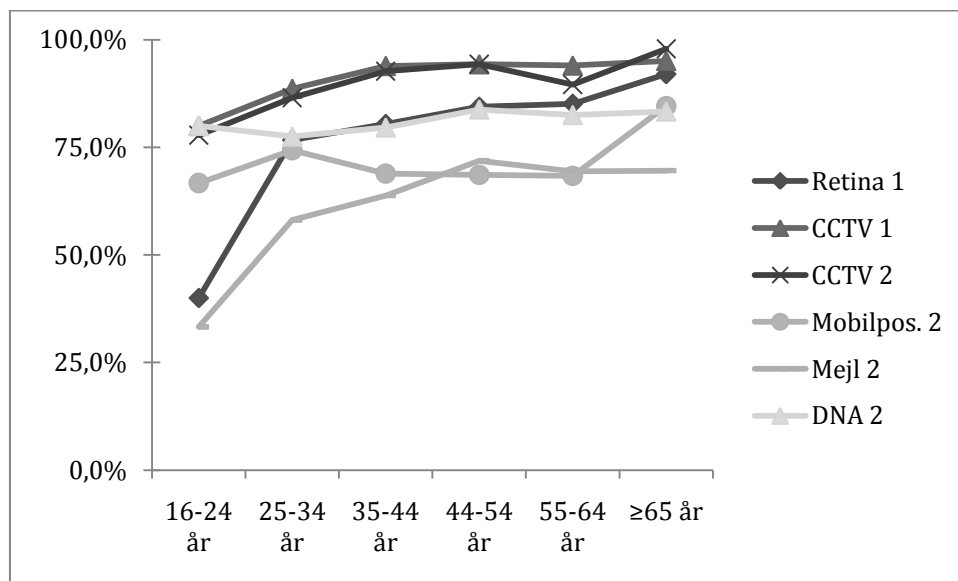
	Retina 1		CCTV 1		CCTV 2		Mobpos 2		Mejlfiler 2		DNA 2	
	Barn	Ej barn	Barn	Ej barn	Barn	Ej barn	Barn	Ej barn	Barn	Ej barn	Barn	Ej barn
1	85,9	74,2	93,7	91,5	94,7	83,3	76,1	60,3	72,9	43,1	85,6	69,8
2	14,6	29,0	8,4	22,0	10,0	23,3	39,1	66,2	38,0	60,3	22,7	35,1
3	2,97	2,63	3,35	2,85	3,22	2,92	3,76	2,29	2,81	2,24	3,43	3,04
4	3,20	2,87	3,65	3,36	3,59	3,30	3,20	2,63	2,86	2,17	3,54	3,16

Med hjälp av Tabell 4 ses att det i samtliga fall innebär att respondenter med barn uppger högre acceptans, upplever tekniken som integritetskränkande i lägre grad, känner större tillit till ansvariga aktörer och upplever tillämpningarna som mer lämpliga.

Nollhypotesen, att huruvida respondenterna har barn eller ej inte påverkar acceptansen, anses därför kunna förkastas med stor säkerhet. Det föreligger väsentliga skillnader i svaren.

6.1.3 ÅLDER

Med högre ålder ökar känslan av sårbarhet och därmed den upplevda risken framgick det i litteraturstudien, vilket väcker misstanken att acceptansen för integritetskränkande säkerhetsteknik följer samma trend. Yngre människor växer dock i större utsträckning upp med modern teknik och tjänster som gör att gränsen för vad som är privat och offentligt ständigt flyttas, vilket skulle kunna innebära att acceptansen för eventuella integritetskränkningar stiger.



Figur 42. Utvisar för valda scenarier hur stor andel av respondenterna som svarar jakande på frågan "Anser du denna typ av användning av teknik är acceptabel?", uppdelat på sex åldersgrupper.

Figur 42 visar grafiskt hur acceptansen varierar med åldern för respektive säkerhetsscenario. I allmänhet så verkar acceptansen öka något med åldern, med vissa undantag. Näthinnefotografering och mobiltelefonpositionering sticker ut som exempel där yngre åldersgrupper är betydligt mer skeptiskt inställda än äldre. Efter statistisk analys i SPSS erhålls följande resultat i form av signifikansnivåer, vilka redovisas i Tabell 5.

Tabell 5. Utvisar för utvalda scenarier och frågor signifikansnivåerna för nollhypotesen att svaren inte skiljer sig beroende på respondenternas ålder. Signifikanta skillnader (under signifikansnivån 0,05) har markerats.

	Retina 1	CCTV 1	CCTV 2	Mobpos 2	Mejl 2	DNA 2
Fråga 1	0,050	0,700	0,215	0,520	0,248	0,980
Fråga 2	0,005	0,145	0,036	0,098	0,172	0,122
Fråga 3	0,102	0,002	0,377	0,033	0,264	0,311
Fråga 4	0,620	0,067	0,294	0,264	0,022	0,012

Inga skillnader i acceptans går alltså att säkert bekräfta, men signifikansnivån för näthinnefotografering tangerar vad som anses vara statistiskt signifikant. Det finns däremot en signifikant skillnad i huruvida näthinnefotografering och övervakningskameror med maskningsteknik anses vara integritetskränkande. I allmänhet går det att säga att uppfattningen att tekniken är integritetskränkande minskar med åldern.

Dessutom föreligger det skillnader i skattningen av tillit för konventionella övervakningskameror och mobiltelefonpositionering, samt för skattningen av lämplighet för mejlfilter och DNA-lagring. Här är det där-

emot inte möjligt att säga att det finns ett generellt samband mellan ålder och uppfattning genom att studera svarsresultaten.

Det finns inte stöd för att förkasta nollhypotesen.

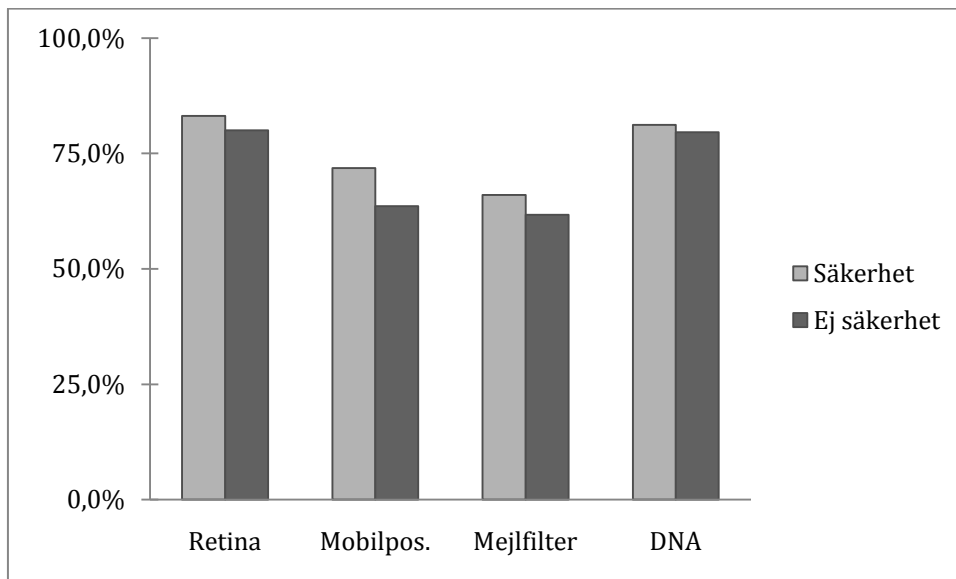
Däremot går det att konstatera låga signifikansnivåer för övriga studerade frågor. Ett eventuellt samband mellan ålder och perceptionen för integritetskränkande säkerhetsåtgärder utesluts därför inte.

6.2 KONTEXTUELLA FAKTORER

Till kontextuella faktorer räknas en variabel: Huruvida teknikanvändningen syftar till ökad offentlig säkerhet eller inte. För fyra tekniker fanns ett scenario med någon form av offentlig säkerhetstillämpning och ett utan. Här undersöks huruvida det går att finna samband mellan tillämpningens syfte samt acceptans och inställning. Liksom för de demografiska faktorerna används resultaten från följande frågor:

1. Anser du denna typ av användning av teknik är acceptabel? (ja/nej)
2. Anser du denna typ av användning av teknik som integritetskränkande? (ja/nej)
3. I vilken utsträckning litar du på de aktörer som samlar in denna information? (1-5)
4. Hur skulle du skatta denna teknikutveckling? (1-5)

På samma sätt som tidigare inleds analysen med en snabb jämförelse av acceptansen:



Figur 43. Utvisar hur stor andel av respondenterna som svarat jakande på frågan "Anser du denna typ av användning av teknik är acceptabel?", beroende på om tillämpningen gäller offentlig säkerhet eller inte.

Det verkar föreligga ett konsekvent samband mellan syftet och acceptansen när man studerar Figur 43. I samtliga fall är acceptansen för det scenario vars syfte uppges vara säkerhet högre än för det alternativa scenariot.

Med hjälp av hypotesprövningar undersöks styrkan i detta samband, vilket redovisas i

Tabell 6.

Tabell 6. Utvisar för valda scenarier och frågor signifikansnivåerna för nollhypotesen, att huruvida tillämpningen rör offentlig säkerhet eller ej inte påverkar hur respondenterna har svarat. Signifikanta skillnader (under signifikansnivån 0,05) har markerats.

	Retina	Mobpos	Mejlfiler	DNA
Fråga 1	0,975	0,049	0,317	0,669
Fråga 2	0,910	0,154	0,359	0,251
Fråga 3	0,555	0,015	0,000	0,025
Fråga 4	0,508	0,229	0,026	0,192

Slutsatsen blir att sambandet i själva verket inte är särskilt starkt. Endast när det gäller mobiltelefonpositionering, där polisen var inblandad som aktör i säkerhetstillämpningen, går det att konstatera en signifikant skillnad i acceptans.

Tabell 7. Resultaten för valda scenarier och frågor, uppdelat på huruvida scenarierna behandlar offentlig säkerhet eller ej. Signifikanta skillnader (under signifikansnivån 0,05) har markerats.

	Retina		Mobpos		Mejlfiler		DNA	
	Säkerhet	Ej säk	Säk	Ej säk	Säk	Ej säk	Säk	Ej säk
1	83,1	80,0	71,8	63,6	66,0	61,7	81,2	79,6
2	18,1	21,2	46,4	52,8	43,2	47,3	26,4	22,0
3	2,89	2,86	2,63	2,37	2,68	2,25	3,31	3,10
4	3,12	3,27	3,04	2,81	2,70	2,45	3,43	3,32

Det går dock att konstatera att tilliten i tre fall av fyra är betydligt högre då syftet uppges vara offentlig säkerhet. För tekniken mejlfiler skattas dessutom lämpligheten högre.

Generellt sett går det inte att säga att det finns ett samband mellan acceptans och huruvida tillämpningens syfte är offentlig säkerhet eller inte, och nollhypotesen förkastas inte. Det verkar däremot som det finns ett samband med tilliten, vilket dock inte slår igenom i acceptansnivåerna.

6.3 KOGNITIVA FAKTORER

Syftet med litteraturstudien var att identifiera faktorer vilka visat sig vara viktiga för riskupplevelsen och försöka överföra dessa på personlig integritet. Detta användes sedan i kapitel 4, där ett antal frågor valdes ut och hypotesen formulerades som att respondenternas svar på dessa frågor var oberoende av huruvida de ansåg tekniken vara acceptabel eller integritetskränkande. Förkastas nollhypotesen kan man således konstatera att det föreligger åtminstone ett beroende, och ett eventuellt samband är möjligt. De fyra frågor som valdes ut var följande:

1. **Nytta:** I vilken utsträckning anser du att denna tillämpning av tekniken är effektiv för att uppnå det mål som är uppsatt? (1-5)
2. **Tillit:** I vilken utsträckning litar du på de aktörer som samlar in denna information? (1-5)
3. **Sannolikhet:** Hur stor risk tror du det är för att denna information kan missbrukas? (1-5)
4. **Hemskhet:** Hur pass orolig över denna utveckling och användning av teknik är du? (1-5)

Frågorna har valts ut för att representera de centrala faktorerna nytta, tillit, sannolikhet och hemsighet. För att kontrollera nollhypotesen prövas om gruppen som anser teknikanvändningen är acceptabel har svarat likvärdigt på dessa fyra frågor jämfört med gruppen som inte anser den vara acceptabel. Resultaten redovisas i Tabell 8.

Tabell 8. Utvisar för valda scenarier och frågor signifikansnivåerna för nollhypotesen, att huruvida respondenterna anser att tillämpningen är acceptabel eller ej inte påverkar hur de besvarat övriga frågor.

	Retina 1	CCTV 1	CCTV 2	Mobpos 2	Mejlfiler 2	DNA 2
Fråga 1	0,000	0,000	0,000	0,000	0,000	0,000
Fråga 2	0,000	0,000	0,000	0,000	0,000	0,000
Fråga 3	0,000	0,001	0,000	0,000	0,000	0,000
Fråga 3	0,000	0,000	0,000	0,000	0,000	0,000

För samtliga frågor visar det sig vara extremt osannolikt att gruppen som accepterar tekniken delar uppfattningarna som mäts i de fyra frågorna med gruppen som inte accepterar tekniken. Medelvärden av hur grupperna har svarat framgår i Tabell 9. Skillnaderna mellan grupperna är följaktligen stora.

Tabell 9. Resultaten för valda scenarier och frågor, uppdelat på huruvida respondenterna ansåg tillämpningen vara acceptabel eller ej.

	Retina 1		CCTV 1		CCTV 2		Mobpos 2		Mejlfiler 2		DNA 2	
	Ja	Nej	Ja	Nej	Ja	Nej	Ja	Nej	Ja	Nej	Ja	Nej
1	2,30	3,54	2,59	3,89	2,33	3,79	3,07	3,69	2,30	3,35	2,83	3,96
2	1,68	3,15	1,93	3,40	1,91	3,34	1,92	3,25	1,93	3,25	2,05	3,77
3	4,30	2,91	4,28	2,79	3,82	2,76	4,30	3,03	4,02	2,83	3,56	2,39
4	3,55	2,09	3,62	1,88	3,55	1,86	3,28	1,96	3,09	1,92	3,21	1,71

Samma prövning görs igen, men respondenterna delas istället upp beroende på om de svarat att de anser tekniken vara integritetskränkande eller inte. I Tabell 10 redovisas resultaten från denna prövning.

Tabell 10. Utvisar för valda scenarier och frågor signifikansnivåerna för nollhypotesen, att huruvida respondenterna anser att tillämpningen är integritetskränkande eller ej inte påverkar hur de besvarat övriga frågor.

	Retina 1	CCTV 1	CCTV 2	Mobpos 2	Mejlfiler 2	DNA 2
Fråga 1	0,000	0,000	0,000	0,000	0,000	0,000
Fråga 2	0,000	0,000	0,000	0,000	0,000	0,000
Fråga 3	0,000	0,000	0,000	0,000	0,000	0,000
Fråga 4	0,000	0,000	0,000	0,000	0,000	0,000

Återigen går det att konstatera att samtliga skillnader är högst signifikanta. Medelvärdena på svaren, vilka redovisas i Tabell 11, utvisar vilka stora skillnader det är mellan grupperna.

Tabell 11. Resultaten för valda scenarier och frågor, uppdelat på huruvida respondenterna ansåg tillämpningen vara integritetskränkande eller ej.

	Retina 1		CCTV 1		CCTV 2		Mobpos 2		Mejlfiler 2		DNA 2	
	Ja	Nej	Ja	Nej	Ja	Nej	Ja	Nej	Ja	Nej	Ja	Nej
1	3,56	2,11	3,84	2,41	3,72	2,20	3,64	2,79	3,32	2,08	3,91	2,79
2	3,14	1,64	3,32	2,00	3,28	1,65	2,98	1,75	3,15	1,75	3,47	1,79
3	2,95	4,20	2,90	3,88	2,80	4,05	3,36	4,28	2,93	4,15	2,72	4,41
4	2,13	3,48	1,98	3,47	1,94	3,75	2,25	3,41	2,04	3,19	1,96	3,43

Nollhypotesen, att svaren på de valda frågorna inte påverkas av huruvida respondenterna anser att tekniken är acceptabel eller integritetskränkande, förkastas helt. Frågan om det finns ett orsakssamband mellan svaren på frågorna och acceptansen respektive huruvida tillämpningen anses vara integritetskränkande eller ej går dock inte att besvara endast med dessa resultat. Frågan avhandlas närmare i diskussionskapitlet.

7 DISKUSSION

Analysen pekar på att det inte i någon större utsträckning verka föreligga demografiska skillnader i hur tekniska säkerhetstillämpningar uppfattas och accepteras ur ett integritetsperspektiv. I den här rapporten konstateras det endast statistiskt signifikanta skillnader i svaren mellan respondenter som har barn respektive ej har barn. Det finns inte stöd för att konstatera generella könsskillnader, då de uppmätta skillnaderna varken är entydiga eller statistiskt signifikanta. Situationen ser likadan ut när det gäller sambandet med ålder.

Ett intressant resultat som dock är värt att diskutera är att det finns respondenter som inte upplever teknik som integritetskränkande, men trots detta uppger att de kommer försöka undvika situationen helt. Kan det helt enkelt bero på att de inte uppfattar teknik som integritetskränkande så länge den går att undvika? En central roll inom riskperception är som tidigare nämnts risk denial, alltså att den subjektiva risken systematiskt bedöms vara lägre än den generella risken. Ju större kontroll över risken som individen upplever, desto större blir effekten av risk denial. En fråga som bör ställas i sammanhanget är om det förhåller sig på samma sätt med personlig integritet, alltså att acceptansen blir högre om respondenterna upplever att de har kunskap eller möjlighet att undvika övervakningen. På så sätt åtnjuter de ju fördelarna i form av exempelvis högre säkerhet, samtidigt som man undviker nackdelar i form av ökad övervakning.

Det skulle förklara den något motsägande bild som målas upp av exempelvis övervakningskameror. Å ena sidan upplevs oron för och upprördheten över att tekniken kan missbrukas på något sätt vara överlägset högre än för någon annan teknik. Å andra sidan åtnjuter tekniken mycket hög acceptans, rentav högst i studien. Det ligger nära till hands att dra slutsatsen att övervakningskameror får representera en kategori av säkerhetsteknik som är konkret och lätt urskiljbar, både vad gäller hur och var den används samt vilken typ av övervakning den innebär. Därför upplevs tekniken som enkel att medvetet undvika samtidigt som konsekvenserna av ouppsåttligt eller medvetet missbruk lätt inses. Om respondenterna sedan i praktiken kan eller vill utnyttja denna möjlighet är en annan fråga, själva förekomsten kan vara tillräcklig. Jämför med vad många flygrädda upplever: De drar sig för att flyga då det till skillnad från andra transportsätt inte finns en möjlighet att kliva av fordonet mitt under resan, trots att denna möjlighet självklart inte minskar risken för att råka ut för en olycka. Blotta illusionen av kontroll räcker för att mildra riskupplevelsen.

I vilken utsträckning en teknik accepteras torde dessutom i hög grad bero på just riskperception. Toleransen för de integritetskränkningar som en teknikanvändning medför borde rimligtvis stå i proportion till hur allvarligt hotet från riskkällan anses vara. Därför hade det varit välkommet att även inkludera sådana frågor som undersöker hur respondenterna upplever riskkällan för att även fånga in den dimensionen av acceptans. Här kan det tänkas att en sådan sak som hur aktuell och uppmärksam riskkällan i fråga är. Kan det inte tänkas att acceptansen för övervakningskameror ökade dramatiskt efter att en man sprängde ihjäl sig själv vid Drottninggatan i Stockholm? Och hur påverkas acceptansen när ett säkerhetssystem väl införts? Debatten om den så kallade FRA-lagen var hård innan dess införande, men därefter har frågan i stort sett varit död.

7.1 UTFÖRANDE

Enkäten var utformad på ett sätt som innebar att respondenten ställdes inför ett hypotetiskt scenario, och sedan blev tillfrågade huruvida teknikanvändningen ansågs vara acceptabel och integritetskränkande. Först därefter ställdes frågor om hur respondenterna upplevde tekniken, tillit till aktörerna, nytta, efterfrågan och så vidare. Det ligger inte långt bort att tro att dessa senare bedömningsfrågor färgas av vilken inställning respondenten har till det aktuella scenariot. Således kanske en respondent vanligtvis känner hög tilltro till en viss myndighet. När myndigheten i studien presenteras som aktör i en säkerhetsåtgärd för vilken respondenten är negativt inställd till, uppger denne istället att tilliten är mycket låg. En situation som således borde tolkas som att sambandet mellan tillit och acceptans är svag leder istället till slutsatsen att ett samband verkar gå

att styrka! Att respondenten som andra fråga i enkäten explicit utfrågas om acceptansen kan tänkas öka denna polarisering. Det överväldigande resultatet för att de kognitiva faktorerna har ett samband med acceptans och perception av integritetskränkningar kan alltså betyda att det snarast handlar om ett systematiskt mätfel.

Förutom de frågor som handlar om hur enkätstudien är utformad, finns det mer tekniskt potentiella felkällor. All behandling av data från studien har tagits fram, behandlats och tolkats av författaren. En sådan sak som fel i avläsningen vid överföringen av siffror skulle kunna vara grund till felkällor. Att det skulle föreligga systematiska sådana fel verkar dock inte troligt eftersom materialet har gått igenom ett flertal gånger, och resultaten därför i stor utsträckning har dubbelkontrollerats.

7.2 FÖRSLAG

Utöver de frågor som tagits med i enkätstudien finns det ett flertal ytterligare variabler som skulle vara intressanta att undersöka för att erhålla en bättre bild av hur upplevelser och acceptans påverkas av olika faktorer. Många av de faktorer som framkom i litteraturstudien saknar representation i enkätstudien. Dessutom skulle det vara önskvärt om respondenterna fick besvara frågor om sin inställning till exempelvis olika aktörer, tekniker och riskkällor redan innan de presenteras för de olika scenarierna. På så sätt borde risken för att dessa bedömningar färgas av inställningen till de presenterade scenarierna minimeras.

Vidare skulle det vara intressant att låta enkätstudiens utformning föregås av en intervjustudie med respondenter med vitt skilda inställningar till personlig integritet (likgiltiga, pragmatiker och förespråkare). Detta för att få en uppfattning om hur de själva upplever att inställningen till personlig integritet formas, och ta hänsyn till detta när frågor till en mer omfattande enkätstudie formuleras. Ett alternativ vore att studera det mycket stora material som fritextsvaren utgör, där respondenterna bland annat har fått svara på frågor som rör vilka farhågor de känner inför olika typer av teknik. Materialet är dock som sagt mycket omfattande och en sådan analys skulle bli väldigt tidskrävande och nyttan är svår att förutsäga.

8 SLUTSATSER

Vissa samband mellan demografiska faktorer och inställningen till integritetskränkande säkerhetsteknik har konstaterats i denna rapport:

- Det verkar inte föreligga skillnader mellan hur män respektive kvinnor ser på acceptans och integritetskränkningar. De flesta skillnader som uppmätts går att stryka som icke-signifikanta.
- Signifikanta skillnader mellan hur respondenter med respektive utan barn ställer sig till frågor om acceptans och integritetskränkningar går att konstatera. Det föreligger alltså troligtvis skillnader mellan dessa grupper.
- Ett samband mellan ålder och perception för integritetskränkande teknik kan finnas.

Vidare undersöktes om en situationsspecifik omständighet, närmare bestämt huruvida tillämpningen syftade till att öka den offentliga säkerheten eller inte, hade någon inverkan på acceptans och perception för tekniken. Något sådant generellt samband kunde dock inte fastställas.

Slutligen undersöktes ett antal kognitiva faktorer genom att pröva huruvida respondenter svarat olika på ett antal frågor, representativa för olika kognitiva dimensioner, beroende på om de ansåg att tekniken var acceptabel respektive integritetskränkande eller ej. I samtliga prövade frågor gick det att konstatera kraftigt signifikanta skillnader. Huruvida de här resultaten ger stöd för att det finns ett klart samband, eller om det tyder på att svaren i studien har färgats av grundinställningen till tekniken, problematiseras dock i diskussionskapitlet.

Framför allt ska det framhävas att arbetet väckt ytterligare frågor och bör fungera som underlag för vidare studier på området. Litteraturstudien har lyft fram många faktorer som skulle behöva undersökas för att ge en mer fullödlig bild av hur acceptansen för integritetskränkande teknik formas. Fortsatta, mer fokuserade studier rekommenderas.

9 KÄLLFÖRTECKNING

- Backman, J. (2010). *Rapporter och uppsatser* (2 uppl.). Lund: Studentlitteratur.
- Beaney, W. M. (1966). The Griswold Case and the Expanding Right to Privacy. *Wisconsin Law Review*, 979, 979-995.
- Bok, S. (1984). *Secrets : on the ethics of concealment and revelation*. New York: Vintage Books.
- Borg, E., & Westerlund, j. (2009). *Statistik för beteendevetare* (2 uppl.). Stockholm: Liber.
- Council of Europe. (u.d.). *Convention for the Protection of Human Rights and Fundamental Freedoms*. Hämtat från Council of Europe - Treaty Office: <http://conventions.coe.int/treaty/en/treaties/html/005.htm> den 11 januari 2011
- Culnan, M. J., & Armstrong, P. K. (Organization Science). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *10* (1), 104-115.
- Dagens Nyheter. (den 08 12 2010). *FRA anklagas för bristande kontroll*. Hämtat från Dagens Nyheter: <http://www.dn.se/nyheter/sverige/fra-anklagas-for-bristande-kontroll-1.1223938> den 10 januari 2011
- Datainspektionen. (2009). *Datainspektionen Årsredovisning 2009*. Stockholm: Datainspektionen.
- Enander, A. (2005). *Människors förhållningssätt till risker, olyckor och kriser*. Huskvarna: Räddningsverket.
- European Parliamentary Technology Assessment. (2006). *ICT and Privacy in Europe*. Hämtat från <http://epub.oeaw.ac.at/ita/ita-projektberichte/e2-2a44.pdf> den 4 november 2010
- Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., & Combs, B. (1978). How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. *Policy Sciences*, 9 (2), 127-152.
- Garrick, J. B. (1998). Technological stigmatism, risk perception, and truth. *Reliability Engineering & System Safety*, 59 (1), 41-45.
- Gavison, R. (1980). Privacy and the Limits of Law. *The Yale Law Journal*, 89 (3), 421-471.
- Klinke, A., & Renn, O. (2002). A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies. *Risk Analysis*, 22 (6), 1071-1094.
- Kroes, E. P., & Sheldon, R. J. (1988). Stated Preference Methods: An Introduction. *Journal of Transport Economics and Policy*, 22 (1), 11-25.
- Körner, S., & Wahlgren, L. (2006). *Statistisk dataanalys*. Lund: Studentlitteratur.
- Lindley, R. (1986). *Autonomy*. London: Macmillan Education.
- Lyon, D. (2007). *Surveillance Studies: An Overview*. Cambridge: Polity Press.
- Marx, G. T. (1988). *Undercover: Police Surveillance in America*. Berkeley: University of California Press.
- Nationalencyklopedin 1. (u.d.). *Kvantitativ metod*. Hämtat från <http://www.ne.se/lang/kvantitativ-metod> den 9 december 2010

- Nationalencyklopedin 2. (u.d.). *Signifikanstest*. Hämtat från <http://www.ne.se/lang/signifikanstest> den 9 december 2010
- Nationalencyklopedin 3. (u.d.). *Integritet*. Hämtat från <http://www.ne.se/sve/integritet> den 6 november 2010
- Nationalencyklopedin 4. (u.d.). *Demografi*. Hämtat från <http://www.ne.se/lang/demografi> den 28 mars 2011
- Nationalencyklopedin 5. (u.d.). *Kognitiv*. Hämtat från <http://www.ne.se/lang/kognitiv> den 28 mars 2011
- Nationalencyklopedin 6. (u.d.). *Kontext*. Hämtat från <http://www.ne.se/sve/kontext> den 28 mars 2011
- Nationalencyklopedin 7. (u.d.). *RFID*. Hämtat från <http://www.ne.se/lang/rfid> den 28 mars 2011
- Palm, E., & Wester, M. (2010). Privacy and Public Access in the Light of E-Government: The Case of Sweden. i M. J. Dark, *Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives* (ss. 206-225). Hershey, PA: IGI Global.
- Priest, S. H., & Bonfadelli, H. (2003). The "Trust Gap" Hypothesis: Predicting Support for Biotechnology Across National Cultures as a Function of Trust in Actors. *Risk Analysis*, 23 (4), 751-766.
- Rachels, J. (1975). Why Privacy is Important. *Philosophy and Public Affairs*, 4 (4), 323-333.
- Risikollegiet. (1991). *Att jämföra risker*. Stockholm: Risikollegiet.
- Risikollegiet. (1993). *Upplevd risk*. Stockholm: Risikollegiet.
- Rössler, B. (2005). *The Value of Privacy*. Cambridge: Polity Press.
- Sjöberg, L. (2000). Factors in Risk Perception. *Risk Analysis*, 20 (1), 1-12.
- Sjöberg, L., & Wester-Herber, M. (2008). Too much trust in (social) trust? The importance of epistemic concerns and perceived antagonism. *International Journal of Global Environmental Issues*, 8 (1), 30-44.
- Slovic, P. (1993). Perceived Risk, Trust, and Democracy. *Risk Analysis*, 13 (6), 675-682.
- Slovic, P. (2001). The risk game. *Journal of Hazardous Materials*, 86 (1-3), 17-24.
- Slovic, P. (1999). Trust, Emotion, Sex, Politics, and Science: Surveying the Risk-Assessment Battlefield. *Risk Analysis*, 19 (4), 689-701.
- SPSS. (u.d.). *About SPSS Inc*. Hämtat från SPSS: <http://www.spss.com/corpinfo/history.htm> den 11 februari 2010
- Starr, C. (1969). Social Benefit versus Technological Risk. *Science*, 165, 1232-1238.
- The Washington Post. (u.d.). *A hidden world, growing beyond control*. Hämtat från Washington Post: <http://projects.washingtonpost.com/top-secret-america/articles/> den 2 december 2010
- United Nations. (u.d.). *The Universal Declaration of Human Rights*. Hämtat från United Nations: <http://www.un.org/en/documents/udhr/index.shtml> den 11 januari 2011
- Varian, H. R. (2006). Revealed Preference. i M. Szenberg, L. Ramrattan, & A. A. Gottesman, *Samuelsonian economics and the twenty-first century*. Oxford University Press.

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, 4 (5), 193-220.

Westin, A. F. (2003). Social and Political Dimensions of Privacy. *Journal of Social Issues*, 59 (2), 431-453.

BILAGA A – ENKÄTFRÅGOR

- Anser du att denna typ av användning av teknik som integritetskränkande (ja/nej)?
- Anser du denna typ av användning av teknik är acceptabel (ja/nej)?
- Anser du denna teknik kommer att förbättra samhället (ja/nej)?
- I vilken utsträckning anser du denna tillämpning av tekniken bidrar till att samhället blir mer sårbart (1-5)?
- I vilken utsträckning anser du att denna tillämpning av tekniken är effektiv för att uppnå det mål som är uppsatt (1-5)?
- I vilken utsträckning anser du att denna tillämpning av tekniken bidrar till att samhället blir säkrare eller mer effektivt (1-5)?
- Jag vill gärna ha denna tillämpning av tekniken (1-5).
- Jag skulle aktivt efterfråga denna teknik om jag fick tillfälle (1-5).
- Jag anser denna teknik kan användas av (ja/nej):
 - Alla myndiga personer.
 - Föräldrar som ger sitt medgivande att uppgifter om deras barn samlas in.
 - Personer som ger sitt tillstånd för att omyndig partners information samlas in.
 - Anser inte vi ska använda denna teknik.
 - Inte relevant.
- Skulle du söka information om denna tillämpning av tekniken (ja/nej)?
- Skulle du aktivt arbeta för att undvika att du själv sätts i denna situation (ja/nej)?
- I vilken utsträckning skulle du diskutera denna tillämpning av tekniken på detta sätt (1-5):
 - Med personer på din arbetsplats.
 - Med relevant myndighet.
 - Med relevant företag.
 - Med dina förtroendevalda politiker.
 - Med din familj och dina vänner.
- Anser du att denna tillämpning av tekniken har: Många nackdelar – många fördelar (1-5)?
- Hur skulle du skatta denna teknikutveckling: En dålig tillämpning – en bra tillämpning (1-5)?
- Att samla in denna typ av information är:
 - Inte alls nödvändig – helt nödvändig (1-5).
 - Inte alls användbart – mycket användbart (1-5).
- Anser du denna teknik har andra för- och nackdelar (öppet svar)?
- I vilken utsträckning litar du på de aktörer som samlar in denna information? Inte alls – hög utsträckning (1-5).
- Hur stor risk tror du det är för att denna information kan missbrukas? Ingen risk – mycket stor risk (1-5).
- Anser du att detta är en risk som vi bör ta på samhälls nivå (ja/nej)?
- Hur pass orolig över denna utveckling och användning av teknik är du? Inte alls – mycket orolig (1-5).
 - Till alla som svarat mellan 3 och 5 på föregående fråga: Vad är du orolig för (öppet svar)?
- Hur pass stött eller upprörd blir du när du tänker på denna utveckling och användning av olika tekniker som kan användas för övervakning (1-5)?
 - Till alla som svarat mellan 3 och 5 på föregående fråga: Vad är det som gör dig upprörd (öppet svar)?

BILAGA B – STATISTISKA METODER

I följande bilaga beskrivs de statistiska test som används i rapporten utförligare. För ytterligare information hänvisas till exempelvis Borg och Westerlund (2009).

ICKE-PARAMETRISKA TEST

Parametriska test, eller fördelningsberoende metoder, förutsätter att data följer någon typ av fördelning. Då kriterierna för att använda parametriska test inte är uppfyllda kan man istället använda icke-parametriska dito. Dessa utnyttjar inte några särskilda parametrar så som medelvärde eller standardavvikelse. De är inte heller beroende av att frekvensfördelningen antar någon speciell form. De använder däremot mindre information från data än vad parametriska metoder gör, vilket gör dem mindre kraftfulla. Vid någon av följande situationer bör man använda en icke-parametrisk metod:

- När man har nominaldata
- När data inte kan anses vara normalfördelade
- När man inte är intresserad av någon parameter som medelvärde eller standardavvikelse.

Nedan redogörs för de två icke-parametriska test som används vid hypotesprövningarna i rapporten.

MANN-WHITNEYS U-TEST

För att testet ska kunna användas bör stickproven vara slumpmässiga och oberoende av varandra. Testet prövar hypoteserna

H_0 : De två fördelningarna är identiska.

H_1 : De två fördelningarna är inte identiska.

I praktiken används testet ofta för att hypotespröva likheter eller skillnader för populationsmedelvärden.

Först rangordnas alla värden på en gemensam rangskala, varvid värden som är lika (*ties*), tilldelas medelrangvärdet. Sedan beräknas summan av alla rangvärden för ena stickprovet (R_1). Testvariabeln som används kallas *Mann-Whitney U*

$$U = n_1 n_2 + \frac{n_1(n_1 + 1)}{2} - R_1$$

I vilken n_1 och n_2 är de två stickprovsstorlekarna och R_1 är summan av rangvärdena för det ena stickprovet. Vid större stickprovsstorlekar, då båda stickproven är större än 10, kan man göra en approximation till z enligt

$$z = \frac{U - \frac{n_1 n_2}{2}}{\sqrt{\frac{n_1 n_2 (n_1 + n_2 + 1)}{12}}}$$

Om det beräknade z-värdet överstiger det kritiska värdet för signifikansnivån α förkastas nollhypotesen.

KRUSKAL-WALLIS TEST

Om man har tre eller flera oberoende stickprov och det finns anledning att tro att data inte är normalfördelade finns det även då icke-parametriska metoder att tillgå.

En sådan metod är Kruskal-Wallis test som använder sig av rangordnade data och som inte gör några antaganden om fördelningsformen för populationsdata. Kraven på data är att stickproven är slumpmässiga och oberoende. Det används då man vill testa populationer mot hypoteserna

H₀: De k populationernas fördelningar är identiska.

H₁: De k populationernas fördelningar är inte identiska.

Tillvägagångssättet liknar det för Mann-Whitneys test. Först rangordnas alla data på en gemensam skala. Sedan numreras stickprovsstorlekarna och benämns n₁ till n_k. Sedan låter man n = n₁ + n₂ + ... + n_k. Summan av rangvärdena benämns på liknande sätt R₁, R₂... R_k. Testvariabeln som används definieras som

$$H = \frac{12}{n(n+1)} \left(\sum_{j=1}^k \frac{R_j^2}{n_j} \right) - 3(n+1)$$

H₀ förkastas om det beräknade H-värdet är större än ett kritiskt tabellvärde, $\chi^2_{(k-1)}$, för signifikansnivån α .