TØI rapport 1658/2018

Tom Erik Julsrud
Julie Runde Krogstad

Transportøkonomisk institutt
Stiftelsen Norsk senter for samferdselsforskning

Sporing av reiser ved hjelp av mobiltelefoner. Hva mener innbyggerne?

TØI-rapport
1658/2018

Sporing av reiser ved hjelp av mobil-telefoner. Hva mener innbyggerne?

Tom Erik Julsrud
Julie Runde Krogstad

Forsidebilde: Shutterstock

ISSN 2535-5104
ISBN 978-82-480-2176-6 Elektronisk versjon
Oslo, september 2018

Tittel:	Sporing av reiser ved hjelp av mobiltelefoner. Hva mener innbyggerne?	**Title:**	Tracking mobility using mobile phones. What do the citizens think?

Forfattere:	Tom Erik Julsrud Julie Runde Krogstad	**Authors:**	Tom Erik Julsrud Julie Runde Krogstad

Dato:	09.2018	**Date:**	09.2018
TØI-rapport:	1658/2018	**TØI Report:**	1658/2018
Sider:	51	**Pages:**	51
ISBN elektronisk:	978-82-480-2176-6	**ISBN Electronic:**	978-82-480-2176-6
ISSN:	2535-5104	**ISSN:**	2535-5104
Finansieringskilde:	Norges Forskningsråd	**Financed by:**	The Research Council of Norway

Prosjekt:	4427 – Smartchange	**Project:**	4427 – Smartchange
Prosjektleder:	Fredrik Alexander Gregersen	**Project Manager:**	Fredrik Alexander Gregersen
Kvalitetsansvarlig:	Silvia J Olsen	**Quality Manager:**	Silvia J Olsen
Fagfelt:	Reisevaner og mobilitet	**Research Area:**	Travel behaviour and Mobility
Emneord:	personvern, store data, smarte byer, mobilitetsdata	**Keyword(s):**	protection of privacy, big data, smart cities, mobility tracking data

Sammendrag:

Bruk av mobilteknologi i befolkningen, gjør det i økende grad mulig å spore individers bevegelsesmønstre. Slike data forventes å ha stor nytteverdi innenfor utvikling av smarte byer. Samtidig hefter det store personvernsutfordringer ved bruk av denne typen data. I denne rapporten undersøkes disse forholdene gjennom en litteraturgjennomgang, og en undersøkelse av holdninger blant innbyggerne i Oslo og Tallinn. I begge byer er bekymringen for misbruk av disse dataene er betydelig og overgår tidvis de positive forventningene. Tilliten til at offentlige og private virksomheter kan håndtere personvernhensyn er sterkere i Tallinn enn i Oslo. Den utbredte skepsisen til bruk av denne type data forklarer hvorfor det også er forståelse for tiltak som kan regulere bruken. Bekymringen mot de risikable sidene ved bruk av mobile tjenester som kan spores, har likevel ikke lagt noen demper på bruken denne typen tjenester.

Summary:

The rapid adoption of mobile technology in the population makes it increasingly possible to track individuals' patterns of movement. Such data are expected to be important in development of “smart cities”. Still, there are major privacy challenges when using this type of data. This report examines these issues through a literature review, and a panel survey of attitudes among the residents of Oslo and Tallinn. In both cities, the concern for abuse of these data is significant and in some area outweigh the positive expectations and possibilities. The confidence that public and private businesses can handle privacy concerns is stronger in Tallinn than in Oslo. The widespread skepticism of using this kind of data explains why it is high acceptance for measures that can regulate this use. The use of mobile data to record mobility depends on the confidence of those who retrieve these data and there is a strong link between trust in social institutions and the attitudes of using such data for public purposes.

Language of report: English

Transportøkonomisk Institutt
Gaustadalléen 21, 0349 Oslo
Telefon 22 57 38 00 - www.toi.no

Institute of Transport Economics
Gaustadalléen 21, 0349 Oslo, Norway
Telefon 22 57 38 00 - www.toi.no

Forord

Bruk av teknologi i befolkningen og utbygging av digital infrastruktur, gjør det i økende grad mulig å spore individers bevegelsesmønstre. Slike data forventes å ha stor nytteverdi innenfor forskning, samfunnsplanlegging, beredskap og kommersiell virksomhet. Samtidig hefter det store personvernsutfordringer ved bruk av denne typen data.

Gjennom en litteraturgjennomgang og spørreundersøkelser, belyser vi i denne rapporten mulighetene og utfordringene som bruk av nye data kan gi, og vi vil fremme noen foreløpige anbefalinger knyttet til bruk av mobildata innenfor transportforskning og planleggingsarbeid.

Rapporten er skrevet som en del av forskningsprosjektet 'Smart data for greener transport – potentials and pitfalls in evaluating behavioral changes (Smartchange)' som støttes av Norges Forskningsråd. Vi vil takke Catharina Nes i Datatilsynet og Vidar Enebakk i NESH som har delt sin kunnskap om lovverk og praksis gjennom samtaler underveis i prosjektet.

Rapporten er kvalitetssikret av Fredrik Gregersen.

Oslo, september 2018

Transportøkonomisk institutt

Gunnar Lindberg
Direktør

Silvia Olsen
Avdelingsleder

Innhold

Transportøkonomisk institutt
Stiftelsen Norsk senter for samferdselsforskning

Sammendrag

Sporing av reiser ved hjelp av mobiltelefoner. Hva mener innbyggerne?

TØI rapport 1658/2018
Forfattere: Tom Erik Julsrud og Julie Runde Krogstad
Oslo 2018, 51 sider

Mennesker legger fra seg digitale spor hver dag når de reiser i byen, spesielt i form av signaler og registreringer fra mobiltelefonen. Denne rapporten viser at det eksisterer en viss aksept blant befolkningen i Oslo og Tallinn for at slike data brukes til å bekjempe kriminalitet og terror, og forbedre transporttilbudet. Imidlertid mener over halvparten av befolkningen at sporing via mobiltelefonen på generell basis i stor eller svært stor grad truer personvernet. Undersøkelsen viser at det vil være viktig for institusjoner og selskaper som ønsker legitimitet blant sine brukere, å ikke bryte gjeldende normer for bruk og deling av informasjon. De bør derfor søke å involvere innbyggerne for å gå i dialog om normer og forventninger til bruk av data, og hvordan de kan bidra til å forbedre tjenester. Undersøkelsen viser også at vi står ovenfor et personvernparadoks, ved at mange fortsetter å bruke teknologien som før, til tross for sterk bekymring om misbruk av data.

I byområder blir store mengder data samlet inn gjennom sensorer, apper og nettverk. Den omfattende bruken av smarttelefoner i befolkningen de siste årene har gjort det mulig å hente inn data som viser bevegelsesmønster med en større grad av nøyaktighet. Slike data kan bidra til at innbyggerne får hjelp til å planlegge sine hverdagsliv, og at myndighetene kan styre byen på en god og effektiv måte. Bruk av denne typen data er essensielle elementer i utvikling av såkalte «smarte byer», et konsept som betegner hvordan byene kan ta i bruk ny teknologi for å redusere kostnader, forbedre tjenester og øke innbyggernes deltagelse og livskvalitet.

Samtidig inneholder slike data personrelatert informasjon, blant annet om innbyggernes geografiske posisjon og mobilitetsmønster. Når mobilitetsmønsteret kartlegges ved bruk av disse dataene skaper det en rekke etiske problemstillinger. Bruk av mobildata for å utvikle byområder ved hjelp av digitale teknologier, er avhengig av at det er aksept for dette i befolkningen, og at bruken er innenfor eksisterende forventninger og normer. I denne rapporten undersøkes disse forholdene gjennom en litteraturgjennomgang av forskning omkring bruk av mobildata til transportanalyser, og en undersøkelse av holdninger til bruk av mobildata i Oslo og Tallinn.

Lovverk og etiske retningslinjer

EU vedtok i 2016 et nytt lovverk for personvern, som innføres i mai 2018. Det tidligere personverndirektivet stammer fra 1995. Med den nye personvernlovgivningen som innføres i 2018, får EU-borgere nye rettigheter knyttet til personvern. Det er i hovedsak fire nye hovedpunkter som står sentralt for EU-borgere (EU-forordning 2016/679): Enklere tilgang til personlige data; rett til å overføre persondata mellom ulike tjenestetilbydere; rett til å slette data om seg selv, og; rett til å vite når personlig informasjon har blitt hacket eller det har vært datainnbrudd.

OECD utarbeidet i 2016 en rapport om forskningsetikk og nye typer data i samfunnsforskning. I denne rapporten kommer de med anbefalinger knyttet til spesielle problemstillinger som oppstår når stordata brukes i forskning (OECD 2016, 8-11). Her fremheves spesielt individers muligheter for å verne om egne persondata og identiteter; muligheter for å innhente informert samtykke; avidentifisering og anonymisering; videresalg av data; sikkerhet ved deling av data; offentlige forpliktelser om informasjon og innsyn.

Informert samtykke og anonymitet er grunnleggende for hvordan myndigheter, selskaper og forbrukere forholder seg til personvern. Likevel kan det være vanskelig å opprettholde disse målene i praksis. Mange forhold gjør det vanskelig for individer å ta informerte valg og anonymiserte data kan i etterkant de-anonymiseres ved å koble dem mot andre datasett. Til tross for anonymisering kan mange store data brukes til å gjøre slutninger om en person basert på egne handlinger eller handlingene til et mindretall.

Tilgang og bruk

I det nye digitale landskapet oppstår det nye skillelinjer, og maktbalansen mellom aktørene endres. Det er oppstått et nytt hierarki mellom de som bevisst eller ubevisst genererer data, de som har verktøyene til å innhente data og de som har ekspertisen til å analysere dem. Det nye hierarkiet gir flere implikasjoner for forskning.

Forskere og nasjonale myndigheter hadde tidligere eksklusiv tilgang på data som andre aktører ikke hadde, ved å ha ressurser til å samle inn data gjennom spørreundersøkelser og intervjuer. I dag er dette endret ved at private selskaper har tilgang på data som forskningsinstitusjoner enten må kjøpe seg tilgang til, eller bruke ressurser på å samle inn. Disse selskapene har ikke et ansvar for å gjøre disse dataene tilgjengelige, og har full kontroll over hvem som får tilgang til dem Dette skaper et misforhold både mellom private aktører og forskningsinstitusjoner, men også mellom akademiske institusjoner som har ulik tilgang på ressurser til å skaffe til veie slike data og kompetanse til å analysere dem

Holdninger til bruk av mobildata

Bruk av store data for å utvikle smarte byer bør ikke bryte med grunnleggende normer for informasjonsdeling, personvern og kontroll. Nytteverdien av å dele data om bevegelsesmønstre, må stå i forhold til risikoen for uønsket overvåking og kontroll. Det er derfor viktig å ha innsikt i hva befolkningen forventer og aksepterer.

I denne rapporten presenteres data fra en panelundersøkelse av befolkningen i Tallinn og Oslo. Estland har kommet svært langt i å ta i bruk digitale data for å koordinere og effektivisere interaksjon mellom offentlige myndigheter og enkeltpersoner. Samtidig er dette et land der det generelt er lavere tillit til myndigheter og det politiske systemet, noe som også kommer til uttrykk i denne undersøkelsen. Tilliten til at offentlige og private virksomheter kan håndtere personvernhensyn er sterkere i Tallinn enn i Oslo. Dette kan tyde på at de (stort sett) effektive digitale systemene for offentlige tjenester har bidratt til å styrke tilliten til de offentlige institusjonene, om enn ikke til de politiske myndighetene.

Det er størst aksept for å bruke denne typen data for å forebygge terror og kriminalitet. Dette er det eneste feltet der det er et flertall som sier seg helt eller delvis enig i at dette er akseptabelt. Dernest kommer forbedring av transportsystemene, som drøyt halvparten synes er akseptabelt i stor eller svært stor grad. I Oslo er det 18 prosent som synes at det er

akseptabelt å bruke slike data for å utvikle kommersielle produkter. Generelt er aksepten for bruk av slike data noe høyere i Tallinn enn i Oslo.

I begge byer ser vi imidlertid at bekymringen for misbruk av disse dataene er betydelig og tidvis overgår de positive forventningene og tiltroen til at de offentlige myndighetene beskytter mot misbruk. Det ser ut som om det i Tallinn har vært en polariserende utvikling der aksept og nyttevurderinger verdsettes samtidig som skepsisen også har blitt styrket. Det er verdt å merke seg at godt over halvparten av borgerne i begge byer er bekymret for at sporingsdata skal komme på avveie.

Bekymringen mot de risikable sidene ved bruk av mobile tjenester som kan spores, har ikke lagt noen demper på bruken. De som er mest aktive brukere av sosiale medier og navigasjonstjenester på sine reiser, er ikke mindre bekymret for personvernrisiko enn andre. En forklaring er at mange føler at de er nødt til å bruke disse mobile tjenestene i sin hverdag, eller at de ikke mener at risikoen overgår fordelene.

Vi kan gjenfinne ulike underliggende oppfatninger til bruken av mobildata og personvern i utvalget. For det første en innstilling preget av *tiltro* til offentlige myndigheter, og at det er nødvendig med en stor grad av informasjonsdeling og overvåking. Samtidig er det en tydelig grunnholdning preget av *skepsis* til myndigheters bruk av digitale data, blant annet på grunn av fare for utilbørlig overvåking og risiko for misbruk av dataene. En tredje holdningstype preges av sterke forventninger om at *ny teknologi* vil bidra til å utvikle bedre transportsystemer for brukerne. Bruk av mobile data for å registrere mobilitet er avhengig av en viss grad av tillit til de som henter inn disse dataene. Det er derfor ikke overraskende at det er sterk sammenheng mellom tillit til samfunnsinstitusjoner og de holdningene en har til bruk av digitale data, mens mistillit til de politiske institusjonene er forbundet med en skeptisk holdning.

Utfordringer og muligheter

Resultatene fra undersøkelsen viser at det eksisterer en betydelig skepsis til bruk av mobildata, noe som tilsier at bruk dataene bør gjøres med varsomhet. Bruk av denne typen data i kommersielle sammenhenger vil kunne oppfattes som brudd på eksisterende normer for informasjonsdeling. Et brudd på normene rammer selskapene som henter inn dataene (teleoperatører), men også institusjoner og selskaper som bestiller og utnytter seg av disse.

Offentlige etater som ønsker å utnytte denne typen data i en videre utvikling av transporttilbudet, bør sikre seg at dette gjøres i samsvar med de normer, forventninger og ønsker som finnes i befolkningen. Utnyttelse av denne typen teknologier bør søke å involvere innbyggerne (som skal bruke systemene) slik at man kan utvikle løsninger som er tilpasset en gitt geografisk kontekst. På denne måten kan man også inngå i dialog om hvilke normer og forventninger en bør ha på dette feltet fremover.

Innenfor forskning bør man være særlig påpasselig med å informere om hvorfor data innhentes og hvordan de vil bli benyttet. De forskningsetiske retningslinjene som gjelder for bruk av store data bør ligge til grunn for alle typer prosjekter der en tar i bruk denne typen data (OECD 2016).

Institute of Transport Economics
Norwegian Centre for Transport Research

Summary

Tracking mobility through mobile phones. What do the citizens think?

TØI Report 1658/2018
Authors: Tom Erik Julsrud & Julie Runde Krogstad
Oslo 2018 51 pages Norwegian language

People leave digital tracks every day as they travel in the city, especially in the form of signals and registrations from the mobile phone. This report shows that there is a certain acceptance among the population in Oslo and Tallinn for such data to be used to combat crime and terror and to improve transport. However, more than half of the population believes that mobility tracking via the mobile phone on a general basis threatens to a high or very high degree the protection of privacy. The survey shows that it will be important for institutions and companies that want legitimacy among their users not to violate current standards for use and sharing of information. They should therefore seek to involve residents in dialogues on standards and expectations for using data and how they can help improve services. The survey also shows that we are facing a privacy paradox, because many continue to use the technology as before, despite the strong concern about data abuse.

In urban areas large amounts of data are collected through sensors, apps and digital networks. The extensive use of smartphones in the population in recent years has made it possible to retrieve data showing motion patterns with a greater degree of accuracy. Such data can help citizens to plan their everyday lives and improve the authorities' abilities to manage the city in a good and efficient manner. Use of this type of data is essential elements in the development of so-called "smart cities", a concept that describes how cities can deploy new technology to reduce costs, improve services, and increase citizens' participation and quality of life.

At the same time, such data contain person-related information, including the geographical position of the inhabitants and the mobility pattern. When the mobility pattern is mapped using these data, it raises a number of ethical issues. Use of mobile data to develop urban areas using digital technologies depends on the acceptance of this in the population, and that it is used in accordance with expectations and norms. This report investigates these conditions through a literature review of research on the use of mobile data for transport purposes, and a survey of attitudes for using mobile data in Oslo and Tallinn.

Legislative and ethical guidelines

In 2016, the EU adopted a new privacy policy, introduced in May 2018. The former personal protection directive dates back to 1995. With the new privacy legislation introduced in 2018, EU citizens have new rights to privacy[1]. There are essentially four new main points that are central to EU citizens (EU Regulation 2016/679): Easier access to personal data; the right to transfer personal data between different service providers; the right to delete data about himself and; Right to know when personal information has been hacked or there has been data interruption.

[1] The General Data Protection Regulation (GDPR)

In 2016, the OECD prepared a report on research ethics and new types of data in social research. In this report, they gave recommendations related to special issues that occur when data is used in scientific research (OECD 2016, 8-11). In particular, it emphasizes individuals rights to protect their own personal data and identities; opportunities for obtaining informed consent; identification and anonymization; resale of data; security of data sharing; public obligations regarding information and access.

Informed consent and anonymity are key issues when authorities, companies and consumers relate to privacy. Nevertheless, it can be difficult to maintain these goals in practice. Many circumstances make it difficult for individuals to give informed consent and anonymous data can subsequently be de-anonymized by connecting them to other datasets. Despite anonymization, many large data can be used to draw conclusions about a persons identity, based on his own actions or actions to a minority.

Access and use

In the new socio-technical digital landscape there are new dividing lines where the balance of power between actors is changing. A new hierarchy has occurred between those who deliberately or unconsciously generate data, those who have the tools to retrieve data and those who have the expertise to analyze them. This new hierarchy have important implications for research.
Researchers and national authorities have until recently had exclusive access to data that other actors did not have, by having resources and competence to collect data through scientific tools (surveys, interviews, etc). Today, this has changed as private companies increasingly has access to data sources that research institutions either have to purchase or use more resources to get access to. The companies that have access to digital mobility data are not responsible for making this data available and have full control over who can access them. This creates a disparity between private actors and research institutions, but also between academic institutions that have different access to resources to obtain weigh such data and expertise to analyze them

Attitudes for using mobile data

Use of large data to develop smart cities should not violate basic standards for information sharing, privacy and control. The usefulness of sharing data about mobility patterns must be balanced with the risk of undesired monitoring and control. Thus, it is important to have insight into what the population expects and accepts.

This report presents data from a panel survey of the population in Tallinn and Oslo. Estonia has come a long way in using digital data to coordinate and streamline interaction between public authorities and individuals. At the same time, this is a country where there is generally less confidence in government and the political system (which also was evident in this survey). The confidence that public and private businesses can handle privacy concerns is stronger in Tallinn than in Oslo. This may indicate that the (largely) effective digital public service systems have helped to strengthen trust in public institutions, albeit not to the political authorities.

It is in general high acceptance to use this type of data to prevent terror and crime. This is the only field where the majority states that this is acceptable. Secondly, use of mobility tracking data to improve the transport systems, was seen as acceptable (to a large or very

large extent) by approximately 50 % of the populations. In Oslo, 18 percent think that it is acceptable to use such data to develop commercial products. In general, the acceptance of such data is somewhat higher in Tallinn than in Oslo.

In both cities, however, we see that the concern of the possibilities of abuse of these data is significant, and to some outweigh the positive expectations and the confidence that public authorities protect against abuse. It seems that in Tallinn there has been a polarizing development where acceptance and utility assessments are valued while skepticism has also been strengthened. It is worth noting that well over half of the citizens in both cities are worried that tracking data will be abused.

However, concerns with the risky aspects of using mobile services have not put any damper on the use. Those who are the most active users of social media and navigation services on their travels are no less worried about privacy risks than others. One explanation is that many feel they need to use these mobile services in their everyday lives, or that they don't feel that the risk exceeds the benefits.

We locate different underlying views on the use of mobile data and privacy in the sample. Firstly, an attitude characterized by confidence in public authorities and the necessity for a high degree of information sharing and monitoring. Second, there is a clear ground of skepticism about the use of digital data by authorities, partly due to the risk of improper monitoring and the risk of misuse of the data. A third underlying attitude is characterized by strong expectations that new technologies will help develop better transport systems for users. The use of mobile data to record mobility depends on some confidence in those who retrieve and use this data. It is therefore not surprising that there is a strong correlation between trust in social institutions and positive attitudes to use of digital data, while the distrust of political institutions is associated with a skeptical attitude.

Benefits and challenges

The results of the survey show that there is considerable skepticism about the use of mobile data to track mobility patterns in the population, which suggest that such data should be used with much caution. Use of mobile data in commercial contexts could be perceived as breach of existing information sharing standards and social norms. A breach of the standards affects companies that collect data (in particular the telecom operators), but also institutions and companies that order and exploit them.

Public agencies wishing to exploit this type of data in further development of transport services should ensure that this is done within the limits put by the new privacy regulations, but also in accordance with norms and expectations in the population. Utilization of this type of technology should seek to involve the residents (those who will use the systems) to get information about their expectations, needs and resistance points.

Within social scientific research, attention should be paid to informing why data is collected and how they will be used. The research ethical guidelines that apply to the use of large data should be the basis for all types of projects where one uses this type of data (OECD 2016).

1 Mobilitet i smarte byer

Mennesker legger fra seg digitale spor hver dag når de reiser i byen. I byområder blir store mengder data samlet inn gjennom sensorer, apper og nettverk. Slike data kan bidra til at innbyggerne får hjelp til å planlegge sine hverdagsliv, og at myndighetene kan styre byen på en god og effektiv måte (Kitchin 2013). Samtidig inneholder slike data personrelatert informasjon, blant annet om innbyggernes geografiske posisjon og mobilitetsmønster. Når mobilitetsmønsteret kartlegges ved bruk av disse dataene, skaper det en rekke etiske problemstillinger: Forbrukeren har ikke samtykket til bruk av dataene på samme måte som man kan i spørreundersøkelser. De har heller ingen forutsetninger for å vite detaljeringsgraden i dataene eller hva de kan brukes til i fremtiden.

I denne rapporten vil vi sette søkelys på problemstillinger knyttet til etikk og lovverk når store mengder data som inneholder informasjon om mobilitetsmønstre analyseres uten informert samtykke. Gjennom spørreundersøkelser blant innbyggere i Oslo og Tallinn vil vi finne ut mer om holdninger til bruk av mobile data. Dette kan gi viktig kunnskap om hvordan vi kan og bør bruke de digitale sporene mennesker legger igjen hver dag, inn i beslutningsprosesser og til forskningsformål. Det finnes få studier som har undersøkt befolkningens syn på etiske problemstillinger knyttet til bruk av mobilitetsdata og smarte byer. Kitchin (2013) er en av dem som etterlyser flere empiriske studier av hvordan store data kan og bør brukes i en urban kontekst. Slike data kan legge et grunnlag for hvordan myndighetene planlegger byen i fremtiden. Derfor er det viktig med et kritisk søkelys på hvordan myndighetenes og forskernes behov for informasjon kan balanseres med individers behov for personvern.

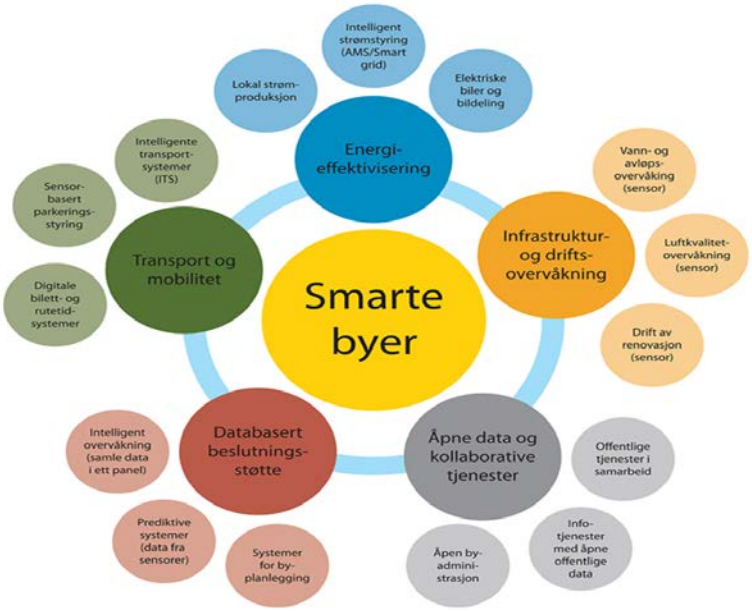
'Smarte byer' er et mye brukt begrep som betegner bruk av teknologi i en urban kontekst. I denne rapporten kan smarte byer forstås som et konsept som betegner hvordan byene kan ta i bruk ny teknologi for å redusere kostnader, forbedre tjenester og øke innbyggernes deltagelse og livskvalitet (Kitchin 2016, s. 13). Det innebærer blant annet å integrere teknologiske løsninger i byen slik at innbyggerne enkelt får informasjon til å planlegge sine hverdagsliv. 'Stordata' er et annet tvetydig begrep. I denne rapporten definerer vi stordata som omfattende datasett med registreringer av faktiske hendelser, interaksjoner og transaksjoner som kan knyttes til individer (Steen-Johnsen og Enjolras 2015, 125). Begrepene smarte byer og stordata vil vi utdype nærmere nedenfor. I tillegg vil vi si noe om potensialet for bruk av stordata for å kartlegge mobilitet i byområder.

Rapporten er strukturert i følgende deler: *Kapittel 2* gir en oversikt over forskningsdesign og datagrunnlaget som er brukt i rapporten. *Kapittel 3* gir en oversikt over lovverk og tidligere forskning på etiske problemstillinger knyttet til stordata og smarte byer. For å få oversikt over lovverket har vi hatt samtaler med personer i Datatilsynet og Den nasjonale forskningsetiske komité for samfunnsvitenskap og humaniora. *Kapittel 4* presenterer resultatene fra spørreundersøkelsene blant befolkningen i Norge og Estland, som ble gjennomført høsten 2017. *Kapittel 5* inneholder noen refleksjoner rundt hvordan hensynet til personvern og behovet for mobilitetsdata kan balanseres, og hvordan utfordringer knyttet til etikk kan løses, i lys av resultatene fra spørreundersøkelsen.

1.1 Hva er smarte byer?

Smarte byer er et begrep som har blitt definert på mange ulike måter. På den ene siden brukes begrepet om 'harde sektorer' som bygninger, vannforvaltning, avfallshåndtering, mobilitet og logistikk, hvor informasjons- og kommunikasjonsteknologi (IKT) kan spille en avgjørende rolle. På den andre siden kan smarte byer også betegne 'myke sektorer' som utdanning, kultur, innovasjon, sosial inkludering og politisk styring, hvor IKT ikke nødvendigvis er avgjørende (Kitchin's (2016, s. 13) definisjon som vi bruker i denne rapporten inneholder både harde og myke elementer: Smarte byer er et konsept som betegner hvordan byene kan ta i bruk ny teknologi for å redusere kostnader, forbedre tjenester og øke innbyggernes deltagelse og livskvalitet.

Mobilitet er en viktig dimensjon i smarte byer, og betegner hvordan IKT kan brukes for å forbedre bytransport (Lombardi mfl. 2012). Mobilitet er en avgjørende del av et fungerende byområde. For at innbyggerne skal kunne delta i arbeidslivet og samfunnet, må myndighetene legge til rette for enkle og sømløse reiser. For å planlegge transportsystemene på en god måte, er det nyttig å vite hvor transportstrømmene går, slik at myndighetene kan iverksette tiltak og gjøre investeringer der behovene er størst. Samtidig gir smarttelefonen muligheter for nye tjenester til innbyggerne. Gjennom mobiltelefonen kan man for eksempel bestille parkering, kjøpe kollektivbillett, få sanntidsinformasjon om kollektivtrafikk, få varsel om snørydding av gatene, eller få vite om det er mye kø i den retningen man ønsker å reise. En grunntanke er at ulike ressurser, blant annet knyttet til transport, vil gjøres tilgjengelig gjennom delingsplattformer, understøttet av såkalt «blockchain teknologi»[2] (Sun and Yan 2016; Tapscott and Tapscott 2018).



Figur 1.1 Sentrale elementer innenfor begrepet smarte byer Kilde: Meld. St. 27 (2015-2016).

[2] «Blokkjeder» (Blockchains) er teknologi for utveksling av krypterte økonomiske transaksjoner og sensitiv informasjon. Transaksjonene er sikret med algoritmer som gjør forfalskninger av signaturer og utvekslinger tilnærmet umulig, og de kan gjøres uten involvering av tredjeparter.

Norske byer er for små til å investere i teknologi og kompetanse på samme nivå som store byer i øvrige deler av verden. I mange tilfeller er norske smartby-prosjekter finansiert av FoU-midler (Meld. St. 27, 2015-2016, s. 112). Stavanger kommune deltar sammen med flere lokale partnere fra næringsliv og akademia i et stort smartby-prosjekt gjennom EUs rammeprogram Horisont 2020, og har fått status som en av EUs 11 europeiske fyrtårnsbyer. Prosjektene i Stavanger omhandler hovedsakelig energieffektivisering i offentlige bygg og et prøveprosjekt om el-busser (Meld. St. 27, 2015-2016, s. 111). Mange av de største byene i Norge har en smartby-strategi. Foreløpig mangler de fleste av disse strategiene et helhetlig rammeverk, de er gjerne lite detaljerte og basert på enkeltprosjekter. I et internasjonalt perspektiv er smartby-initiativer også preget av enkeltprosjekter og det kan være vanskelig å gripe fatt i konkrete resultater. Et smartby pionerprosjekt som er godt kjent, er etableringen av et samlet driftssenter i Rio de Janeiro. Arbeidet startet i 2010 med en avtale mellom IBM og Rio de Janeiro. Driftssystemene fra om lag 30 ulike offentlige organisasjoner ble samlet i ett driftssenter (Kitchin 2014). Gaffney og Robertson (2016) viser at de smarte systemene i Rio de Janeiro er geografisk begrenset og konsentrert i de mest velstående områdene av byen. Her er responstiden i nødsituasjoner, trafikkovervåkning og koordinering mellom ulike organisasjoner og etater bedret. De smarte systemene har imidlertid ikke forbedret de «myke» elementene i visjonen om smarte byer. Teknologien fungerer kun på toppen av eksisterende strukturer. Det betyr at de smarte systemene ikke har utjevnet ulikhet i befolkningen eller gitt økt deltagelse i samfunnet. Politiske myndigheter styrer ikke byen «bedre» og byplanlegging og transport er fremdeles bilbasert. På disse områdene er Rio de Janeiro fremdeles ikke så «smart» (Gaffney og Robertson 2016).

Smarte byer er et fenomen som etter hvert har fått økende interesse fra forskere. Mora mfl. (2017) har analysert litteraturen på smarte byer som er kommet ut mellom 1992 og 2012, og konkluderer med at forskningen er fragmentert, og preget av mangel på faglig diskurs. Ved å se på sammenhenger mellom siteringer i de ulike publikasjonene finner de at mange av bidragene er isolerte, fordi de ikke støtter seg på de sentrale og mest siterte bidragene. I tillegg er det ikke etablert noen felles enighet om en definisjon av smarte byer. Mora mfl. (2017) mener at forskningen kan deles i to hovedretninger: Bidrag som har en helhetlig tilnærming til smarte byer og som utgjør mye av den europeiske forskningen på temaet, og en teknofiksert tilnærming, i hovedsak produsert av det amerikanske næringslivet. Derfor er det kanskje ikke rart at forskning på smarte byer har blitt kritisert for å være unyansert og teknologifiksert (Grossi og Pianezzi 2017; Kitchin 2015; Hollands 2008). Grossi og Pianezzi (2017) mener visjonen om smarte byer er skapt for å tjene interessene til store multinasjonale IT-selskaper, mens behovet for gode politiske svar på befolkningens behov blir oversett. Kitchin (2015) viser til at beskrivelser av smarte byer ofte er unyanserte i form av at de er for idealistiske eller for tekniske, eller de er kritiske uten nyanser eller empiriske bevis. Som Hollands (2008) skriver: «Til tross for en rekke eksempler på denne 'urbane merkelappen', vet vi overraskende lite om de såkalte smarte byene […]».

I et smartby perspektiv skaper teknologien flere utfordringer for personvern. I dag er det nesten umulig å ferdes i byen uten å etterlate seg elektroniske spor. Datasett som kobles sammen kan si mye om individer, som ofte kan identifiseres. Samtidig er produksjonen, lagringen og bruken av dataene skjult for brukeren som vanskelig kan ha kontroll over hvordan dataene brukes, til hvilke formål og av hvem. Vi vil gå nærmere inn på spesifikke utfordringer knyttet til dette i kapittel 3.

1.2 Hva er stordata?

Begrepet 'Big Data', eller 'stordata' på norsk, har tradisjonelt vært brukt om datamengder som inneholder så mye informasjon, at man ikke kan bruke vanlige dataverktøy til å hente den ut (Manovich 2012). Når vi snakker om stordata i samfunnsforskning, er dette imidlertid en noe snever definisjon. Som Boyd og Crawford (2012) viser til, er noen typer data som omfattes av stordatabegrepet (for eksempel alle Twitter-meldinger relatert til et spesielt tema) ikke på langt nær like omfattende som datasett som ikke regnes som stordata (for eksempel folketellinger). Derfor kan vi si at stordata er datasett med følgende kjennetegn (Kitchin 2014):

- De er store i volum og produseres i høy hastighet – ofte i sanntid.
- De er preget av mangfold og ofte knyttet til tid eller sted.
- De er uttømmende i størrelse og omfatter ofte hele populasjoner, eller betydelig større utvalg enn tradisjonelle forskningsmetoder kan gi.
- De er ekstremt detaljerte og fleksible, og kan derfor enkelt kombineres med nye datasett, utvides eller økes.

Stordata inneholder registreringer av faktiske hendelser, interaksjoner og transaksjoner som kan knyttes til individer (Steen-Johnsen og Enjolras 2015, 125). Ifølge Kitchin (2013) kan stordata deles inn i tre grupper, basert på hvordan de produseres: Målrettet, automatisert eller frivillig.

Målrettet data er data hvor en menneskelig operatør overvåker en person eller et sted (for eksempel ved overvåkningskamera eller bruk av sensorer). Dette kan være data som samles inn når man betaler med kort, kjøper eller sveiper billetten i kollektivsystemet.

Automatisert data er data som passivt samles inn via et operativt system eller annen teknologi. Dette kan være radar eller tellesystemer gravd ned i vegbanen, registreringer i bomstasjoner eller automatiske tellesystemer satt opp ved på- og avstigning på busser, tog og T-bane. Det innebærer også CDR[3]-data, som er passive datasignaler fra mobiltelefonen knyttet til den mobilmasten som telefonen kobler seg opp til når den er aktiv.

Frivillig data er data som aktivt eller passivt produseres gjennom brukerplattformer som sosiale medier eller andre applikasjoner. For eksempel må brukere av Google Maps eller Instagram godkjenne at applikasjonen kan lagre posisjonen deres for å ta i bruk tjenesten (en diskusjon om valgfrihet knyttet til informert samtykke og bruk av applikasjoner finnes i avsnitt 3.3.1.). En annen mulighet er å utvikle egne apper som kartlegger brukeres reisevaner. Dette er data som brukere samtykker i å gi fra seg.

Undersøkelsen inkluderer alle disse typer data, men vi vil fokusere på data som samles inn via mobiltelefonen: Automatiserte «passive» data som CDR-data, og frivillige data som samles inn gjennom apper.

1.3 Bruk av stordata for å kartlegge mobilitet

Det er to aspekter ved stordata som har implikasjoner for samfunnsforskning. For det første er stordata forskjellig fra surveydata ved at stordata reflekterer individers faktiske handlinger og ikke deres oppfatning av hva de har gjort eller kommer til å gjøre. For det andre gjør stordata det mulig å undersøke hele populasjonen og ikke kun et lite utvalg

[3] Call Detail Record

(Steen-Johnsen og Enjolras 2015, 125). I en tid med stadig fallende svarprosent i undersøkelser, kan stordata gi nye muligheter for kompliserte analyser, som er mindre ressurskrevende og kan gi et mer riktig bilde av populasjonen enn det store surveyer kan gi.

For å undersøke mobilitet i Norge er den nasjonale reisevaneundersøkelsen blitt gjennomført omtrent hvert fjerde år siden 1985. Undersøkelsene er gjennomført på samme måte slik at resultatene kan sammenlignes over tid. Den finansieres av Samferdselsdepartementet, Statens vegvesen, Jernbanedirektoratet, Kystverket og Avinor. Fra høsten 2016 skal den åttende reisevaneundersøkelsen gjennomføres for første gang som kontinuerlige undersøkelser i fire år, frem til 2019. Den nasjonale reisevaneundersøkelsen består av et basisutvalg på 10 000 respondenter fordelt over hele landet, samt regionale tilleggsundersøkelser. Undersøkelsen som ble gjennomført i 2013/2014 er den største nasjonale reisevaneundersøkelsen som har blitt gjennomført hittil, med i overkant av 60 000 intervjuer (Hjorthol mfl. 2014, 4).

Svarprosenten i de nasjonale reisevaneundersøkelsene har gradvis gått ned, slik trenden er også for andre lignende undersøkelser (Stopher og Greaves 2007). I Norge var svarprosenten på 77 prosent i 1985, mens den i 2013 var på 20 prosent. To tredeler av frafallet skyldtes problemer med å oppnå kontakt og andre tekniske problemer, mens en tredel skyldtes at personen ikke ønsket å delta i undersøkelsen (Hjorthol, mfl. 2014, s. 5). Den lave svarprosenten har aktualisert spørsmålet om respondentene ikke lenger er representative for den øvrige befolkningen, og dermed om dataene er valide (Gregersen og Weber 2016; Stopher og Greaves 2007). Måler reisevaneundersøkelsen det den har til hensikt å måle, altså reisevanene i et gjennomsnitt av befolkningen?

Data fra den nasjonale reisevaneundersøkelsen er en grunnleggende kilde til informasjon om hvordan nordmenn reiser, og brukes som grunnlag i transportmodeller og i myndighetenes beslutningsprosesser. Som Stopher og Greaves (2007) poengterer, så er en modell ikke bedre enn dataene den er basert på. Til tross for lav svarprosent og kostnader forbundet med gjennomføring, er det også store fordeler med reisevaneundersøkelsen: Den inneholder et rikt datamateriale med mange detaljer og analysemuligheter, samtidig som man kan studere befolkningens reisevaner over tid (Gregersen og Weber 2016). Det er likevel viktig å se nærmere på nye metoder for å samle inn data om mobilitetsmønstre og reisevaner på, som kan supplere eller kanskje på sikt også erstatte tradisjonelle reisevaneundersøkelser. Spesielt data som kan samles inn via mobiltelefonen har stort potensiale, da nesten alle mennesker i dag bruker en mobiltelefon og har den med seg stort sett hele tiden: I Norge har 91 prosent av befolkningen tilgang til smarttelefon i hjemmet (SSB 2017), mens 77 prosent av den voksne befolkningen i USA eier en smarttelefon (Pew Research Centre 2016).

Mobildata er data som inneholder personrelatert informasjon uten at brukerne har gitt samtykke til at slike data kan brukes til forskningsformål. Dette fører med seg flere problemstillinger knyttet til etikk og lovverk som vi vil diskutere i denne rapporten: Er det etisk forsvarlig å bruke denne type data til forskningsformål? Hvem har eierskap til dataene? Hvem skal kunne få tilgang til dataene og til hvilket formål? Hvordan skal man forebygge misbruk?

2 Forskningsdesign og data

I denne studien har vi innhentet ulike typer data. For det første er det gjort en litteraturgjennomgang for få oversikt over eksisterende forskning på feltet. I den sammenheng har vi også gjennomført samtaler med informanter fra Datatilsynet og den nasjonale forskningsetiske komite for samfunnsvitenskap og humaniora (NESH). For det andre er det gjort en spørreundersøkelse blant innbyggere i Oslo og Tallin. Spørreundersøkelsen har en komparativ tilnærming der innbyggernes synspunkter på personvern, tillit, overvåking og mobilitet sammenlignes. Dette gir grunnlag for å diskutere forklaringsfaktorer knyttet til aksept og holdninger til bruk av mobildata.

Norge og Estland har både likheter og forskjeller når det kommer til digitalisering. For eksempel er den norske befolkningen generelt langt fremme på bruk av internett i hjemmet og på farten, mens Estland er en pioner når det gjelder digitalisering av offentlige tjenester. Vi gir en mer detaljert beskrivelse av ulike forhold i landene i kapittel 4. Nedenfor vil vi beskrive hvordan vi har gått frem for å hente inn informasjon til litteraturgjennomgangen, som har utgjort kunnskapsgrunnlaget for spørreundersøkelsen. I kapittel 5 beskriver vi spørreundersøkelsen, som ble gjennomført blant befolkningen i Oslo og Tallinn i desember 2017.

2.1 Litteraturgjennomgang

Vi utarbeidet en litteraturgjennomgang høsten 2017, som utgjorde kunnskapsgrunnlaget for spørreundersøkelsen. Det ble gjennomført søk i ulike databaser (utvalgte tidsskriftdatabaser, google scholar) for å finne litteratur relatert til smarte byer, personvern og store data. Vi hadde et spesielt fokus rettet mot bruk av mobildata for å kartlegge mobilitet.

For å få kunnskap om hvordan norske myndigheter forholder seg til stordata og etiske problemstillinger og hva slags kunnskap de har om temaet, gjennomførte vi samtaler med Datatilsynet og den nasjonale forskningsetiske komite for samfunnsvitenskap og humaniora (NESH). Fra dem fikk vi både tips om viktige rapporter, samt et innblikk i konkrete problemstillinger som har vært diskutert. Samtalene ble gjennomført i august 2017.

2.2 Spørreundersøkelse

Datainnsamlingen ble foretatt av Kantar TNS, basert på deres aksesspanel i Norge og Estland[4]. Panelene består av forhåndsrekrutterte utvalg av personer 15 år og eldre som er villige til å delta i undersøkelser. Deltagerne er tilfeldig rekrutterte gjennom andre telefon- (fast- og mobil) og postale undersøkelser, og utgjør aktive paneler. Ønsket utvalg var 500 respondenter i hver by, til sammen 1000 respondenter som er representative for

[4] http://www.tns-gallup.no/metoder-og-verktoy/metoder/galluppanelet/

målgruppen. Spørreundersøkelsen sammenligner deres synspunkter på personvern, overvåking og mobilitet. Datainnsamlingen ble gjennomført parallelt i Oslo og Tallinn i november 2017.

Spørreskjemaet ble sendt ut som e-post med invitasjon til deltakelse, sammen med en lenke til spørreskjemaets adresse på internett. Spørreskjemaet finnes som vedlegg til rapporten (se vedlegg 1). I Norge ble en norsk versjon av spørreskjemaet benyttet. Ettersom en betydelig del av befolkningen i Tallinn er russisktalende, ble spørreskjemaet oversatt til russisk i tillegg til estisk.

Tabell 2.1: Utvalg (uvektet) etter alder, kjønn og bosted. Prosent.

UTVALG	Alder				
Oslo, n=516	15-29	30-44	45-59	60-89	Total
Kjønn					
Mann	2	6	17	16	41
Kvinne	13	18	12	17	59
Total	15	23	29	33	100
Tallinn, n=501					
Mann	8	8	10	15	41
Kvinne	12	16	11	20	59
Total	20	24	21	35	100

Tabell 2.1 viser utvalgets fordeling etter kjønn og alder for de to byene, som kan sammenstilles med befolkningsfordelingen. I Oslo-utvalget er andelen som er yngre enn 44 år noe underrepresentert til fordel for de eldste, samtidig som kvinner er noe overrepresenterte. I Tallinn er de under 29 år noe overrepresentert på bekostning av aldersgruppen 30-44 år. Kjønnsbalansen er om lag som i befolkningen. Det endelige utvalget er veiet tilsvarende befolkningsfordelingen, for alder, kjønn, bosted. For ytterligere informasjon om data, utvalg og vekting henvises til undersøkelsesbeskrivelse fra TNS Kantar (se vedlegg 2).

3 Kunnskapsgrunnlag: Lovverk og etikk ved bruk av stordata

Befolkningen blir overvåket og kontrollert mer enn noen gang tidligere (Kitchin 2016). I dag er det nesten umulig å leve et vanlig liv uten å etterlate seg digitale spor. De nye dataene som genereres skaper muligheter, men også utfordringer. Det digitale landskapet har endret seg – og nye digitale skillelinjer har kommet til syne.

Tidligere har det i hovedsak vært forskningsinstitusjoner og offentlige myndigheter som har samlet inn og hatt eierskap til store datasett. Store dataregistre med personinformasjon har hatt en viktig rolle innenfor ulike forskningsområder og i tilknytning til samfunnsplanlegging. I dag eies stordata i økende grad også av private aktører. Store datamengder kanaliseres gjennom internasjonale selskaper som Facebook, Google og Twitter, men også andre kommersielle aktører som teleselskaper og banker har tilgang til detaljerte persondata (Steen-Johnsen og Enjolras 2015, 131). Dette gjør at maktbalansen mellom aktørene endres, samtidig som analyser av store data i større grad finner sted utenfor de tradisjonelle forskningsinstitusjonene og offentlige etater.

Det er et paradoks at forbrukerne, til tross for ønsket om å verne om personlige opplysninger, likevel tar i bruk tjenester som krever at de gir fra seg personopplysninger. En undersøkelse blant innbyggerne i samtlige EU-land (EU 2015), viser at to av tre ikke føler at de har kontroll over informasjonen de legger ut på nett. Samme andel tror at informasjonen om dem kan bli brukt til et annet formål enn det var samlet inn til. Likevel svarer over halvparten at de bruker et sosialt nettsamfunn hver uke, og mindre enn én av fem leser personvernerklæringene når de gir fra seg informasjon på nett.

Nedenfor vil vi først gi en oppdatert oversikt over lovverket, inkludert EUs nye lovverk for personvern. Deretter vil vi se på tilgang og eierskap til stordata, og utfordringer for personvern.

3.1 Hvilke lover og retningslinjer gjelder?

Lovverket ligger i bunn når stordata brukes i forskning og av myndigheter eller andre. Det er strenge krav til at dataene skal anonymiseres. Dersom de inneholder sensitive opplysninger må man søke konsesjon hos Datatilsynet av de type opplysningene man skal behandle. Det er store forskjeller mellom ulike lands lovgivning for personvern knyttet til innsamling, informasjon og lagring av digitale data. Dette skaper forskjeller knyttet til hvordan aktører kan få tilgang til å bruke slike data (Steen-Johnsen og Enjolras 2015, 135). EUs nye forordning for personvern (GDPR) som innføres i mai 2018, vil harmonisere lovverket i europeiske land.

3.1.1 Lovverk for personvern

Lovverket for personvern er laget for å beskytte retten til et privatliv og retten til å bestemme over egne personopplysninger. Anonymiserte data utfordrer i prinsippet ikke personvernet. Derfor vil lovverket som regel ikke hindre innsamling og analyse av data som

har informert samtykke eller er anonymisert. Lovverket i EU er strengere enn det i USA. En grunnleggende forskjell er at det amerikanske lovverket er sektorspesifikt, mens EUs lovverk for personvern er universelt – det gjelder på tvers av sektorer og aktører som lagrer personsensitive data (Kitchin 2016). I EU er det mer eksplisitte krav til formulering av informert samtykke enn det amerikansk lov krever. I tillegg er EUs lovverk mer restriktivt når det gjelder innsamling, bruk og formidling. Aktørene må ha et rettslig grunnlag for å lagre og analysere personlige data. I USA kan slike data vanligvis analyseres dersom loven ikke spesifikt forbyr det (Solove 2013).

EU vedtok i 2016 et nytt lovverk for personvern, som innføres i mai 2018. Det tidligere personverndirektivet stammer fra 1995. Der det tidligere direktivet har gitt medlemsstatene rom for tolkning og åpner for nasjonale tilpasninger, vil den nye forordningen redusere statenes handlingsrom på personvernområdet (Datatilsynet 2016a). Det nye lovverket vil også omfatte selskaper som er registrert utenfor EU, men som tilbyr tjenester på nett innenfor EU-området. Dette kan for eksempel være selskaper som selger varer over nett, eller som profilerer EU-borgere på bakgrunn av nettbruken deres (Datatilsynet 2016b).

Med den nye personvernlovgivningen får EU-borgere nye rettigheter knyttet til personvern. Det er i hovedsak fire nye hovedpunkter som står sentralt for EU-borgere (EU-forordning 2016/679):

- Enklere tilgang til personlige data – inkludert forståelig og klar informasjon om hvordan dataene bearbeides
- Rett til å overføre persondata mellom ulike tjenestetilbydere
- Rett til å slette data om seg selv dersom man ikke ønsker behandling av data lenger og det ikke er noen legitim grunn til å lagre dataene
- Rett til å vite når personlig informasjon har blitt hacket eller det har vært datainnbrudd

Personopplysninger skal kun behandles dersom det finnes et tydelig spesifisert formål. Dersom en aktør ønsker å bruke data til et annet formål enn de var ment for, må det i utgangspunktet innhentes samtykke. EU-borgere kan også motsette seg profilering, altså at andre aktører (både statlige og private) kan analysere personopplysninger for å avdekke adferd, preferanser, evner eller behov. Dersom man mener personvernrettighetene er brutt, vil borgere få rett til å klage. Dette gjelder også automatiserte avgjørelser som tas på bakgrunn av profiler som er utarbeidet om enkeltpersoner (Datatilsynet 2016b). Den nye forordningen klargjør det ansvaret som forskningsinstitusjoner allerede har når det gjelder databehandling og personvern. Det er høye krav til transparens og informasjon, og alle forskningsinstitusjoner skal ha en personvernrådgiver. Det er forskningsinstitusjonenes ansvar å foreta risikovurderinger for å sikre at dataene ikke kan reidentifiseres, og at man ikke lagrer mer identifiserbare data enn det man trenger.

3.1.2 Lovverk for forskningsetikk

Forskningsetikkloven trådte i kraft i 2017. Den nye loven er strengere enn den første loven fra 2006. Dersom forskeren har opptrådt uredelig eller uaktsomt kan hun ikke lenger skylde på liten kjennskap til normer og regelverk. Loven fastslår blant annet at institusjonen og forskerne er ansvarlige for at forskning gjennomføres i henhold til anerkjente forskningsetiske normer. Blant annet skal institusjonene drive opplæring av sine ansatte og sørge for at alle som deltar i forskningen er kjent med forskningsetiske normer. Ved uredelighetssaker og brudd på regelverket er det institusjonen som har ansvar for å behandle disse sakene. Det skal opprettes retningslinjer på institusjonsnivå for hvordan dette skal gjennomføres, og det skal etableres et utvalg som behandler slike saker lokalt.

Det finnes nasjonale forskningsetiske komiteer som er rådgivende organ for forskningsetikk. For medisinsk og helsefaglig forskningsetikk finnes det i tillegg regionale komiteer.

3.1.3 Etiske prinsipper

Den teknologiske utviklingen skjer så fort at lovverket ikke kan adressere alle utfordringer som kan oppstå når stordata benyttes i forskning. På den ene siden er det viktig at forskningen holder seg innenfor det gjeldende regelverket for personvern, for å sikre at mennesker kan delta i samfunnet uten å risikere straffeforfølgelse eller diskriminering. På den annen side er det viktig å sikre at god forskning kan gjennomføres innenfor dette rammeverket, til nytte for samfunnet.

OECD utarbeidet i 2016 en rapport om forskningsetikk og nye typer data i samfunnsforskning. I denne rapporten kommer de med følgende anbefalinger knyttet til spesielle problemstillinger som oppstår når stordata brukes i forskning (OECD 2016, 8-11):

1. Personvern. De etiske prinsippene som ligger til grunn for personvern er respekt, hensyn til konsekvenser og rettferdighet. En viktig del av dette er å gi personer mulighet til å definere, utvikle og opprettholde sine egne identiteter. Personvern er komplekst både rettslig og etisk, og må vurderes i hvert enkelt tilfelle.

2. Informert samtykke. Når det gjelder analyse av stordata er ikke informert samtykke alltid mulig eller hensiktsmessig. Forskere bør alltid vurdere om samtykke kan innhentes, men dersom det ikke er mulig må forskningens potensielle risiko og nytte veies mot hverandre. Informasjon om hvorfor samtykke ikke var mulig og vurderinger av dette, bør gjøres offentlig tilgjengelig.

3. Anonymitet og avidentifisering. Avidentifisering er ikke nødvendigvis tilfredsstillende dersom flere datasett kobles sammen. Det er fem betingelser som bør tas hensyn til for å sikre trygg behandling av stordata: Personer, prosjekt, data, omgivelser og resultater. Det er behov for mer arbeid knyttet til hvordan anonymitet bør ivaretas.

4. Videresalg av data. Samarbeid mellom offentlige og kommersielle sektorer for å få nytte av data med høy kvalitet er økende. Det er viktig at alle parter følger høye etiske og vitenskapelige standarder. Samtidig er det viktig å informere om hvordan disse transaksjonene gjennomføres når forskningsresultatene rapporteres.

5. Sikkerhet ved deling av data. Det er viktig å sikre at visse kriterier er oppfylt ved deling av data – samtykke, personvern, eierskap og forskningsintegritet. Det er viktig å etablere retningslinjer for hvordan forskere kan innhente data og offentliggjøre hvilke metoder som brukes. Samtidig må potensialet for reidentifisering evalueres.

6. Offentlig forpliktelse. Informasjon og begrunnelse for studien er viktig for å unngå offentlig mistillit. Derfor bør forskere gjøre publikum bevisst på bruk av stordata i samfunnsforskning og legitimere bruk og fremgangsmåte.

3.2 Tilgang og eierskap til data

I det nye digitale landskapet oppstår det nye skillelinjer, og maktbalansen mellom aktørene endres. Det er oppstått et nytt hierarki mellom de som bevisst eller ubevisst genererer data, de som har verktøyene til å innhente data og de som har ekspertisen til å analysere dem (Manovich 2011, 470). Det nye hierarkiet gir flere implikasjoner for forskning.

Forskere og nasjonale myndigheter hadde tidligere eksklusiv tilgang på data som andre aktører ikke hadde, ved å ha ressurser til å samle inn data gjennom spørreundersøkelser og intervjuer. I dag er dette endret ved at private selskaper har tilgang på data som forskningsinstitusjoner enten må kjøpe seg tilgang til, eller bruke ressurser på å samle inn. Disse selskapene har ikke et ansvar for å gjøre disse dataene tilgjengelige, og har full kontroll over hvem som får tilgang til dem (Boyd og Crawford 2012). Dette skaper et misforhold både mellom private aktører og forskningsinstitusjoner, men også mellom akademiske institusjoner som har ulik tilgang på ressurser til å skaffe til veie slike data og kompetanse til å analysere dem (Steen-Johnsen og Enjolras 2015, 134).

Samtidig er det en trend i retning av å gjøre visse typer stordata åpent tilgjengelig. Forskere kan innhente noen av disse dataene gjennom såkalte APIer[5], som er et sett av kommandoer for å hente ut data som er lagret i selskapers databaser. Dette gir på ingen måte tilgang til komplette datasett som selskapene besitter, men kan likevel være nyttig. Nettverket Smarte Byer Norge har i løpet av de siste årene vært en pådriver for en bedre tilrettelegging og utnyttelse av åpne data[6]. Flere forskningsbidrag har bakgrunn i API-data fra for eksempel Flickr og Twitter (Manovich 2011, 464; Larsson 2015, 149). Selskaper som Facebook og Twitter har nå begynt å ta betaling for noen typer API-data. Full tilgang har en prislapp som de fleste akademiske institusjoner i dag ikke har mulighet til å betale. Likevel, dersom forskere fikk full tilgang til dataene, er en annen utfordring at de ville være bearbeidet og ikke «rådata», noe som ikke nødvendigvis er nyttig for formålet med forskningen (Larsson 2015, 150-151). Den desentraliserte tilgangen på digitalt utstyr gjør det også i større grad mulig for forskere å samarbeide med sivilbefolkningen om innhenting av data, for eksempel om forsøpling, kriminalitet, luftforurensning. Denne typen aktiv «borger-forskning» representerer på mange måter et motstykke til det som gjøres i de store næringslivsaktørene (Townsend 2016).

Private selskaper må også forholde seg til lovverket om personvern, noe som kan innebære at analyseavdelingen i selskapet ikke nødvendigvis får tilgang til alle data eller fritt spillerom til å kombinere data som de vil (Manovich 2011, 464). Private selskaper spør ofte forbrukerne om tillatelse til å bruke personlige data ved at de må akseptere vilkår og betingelser for bruk av en tjeneste. Denne tillatelsen gir slike aktører en privilegert posisjon når det gjelder å bruke data til analytiske og kommersielle formål – de trenger ikke overholde de samme etiske retningslinjene som forskere er forpliktet til (Steen-Johnsen og Enjolras 2015, 135).

Forskningsaktivitet i dag skjer ikke nødvendigvis innenfor de tradisjonelle forskningsinstitusjonene. Digitale verktøy gjør at man ikke trenger ressurser for innsamling av data, men kan analysere data knyttet til selskaper eller organisasjoner. På mange måter er det slik at 'alle kan gjøre forskning'.Slik vil forskning ofte måtte konkurrere med fremstillinger fra enkeltpersoner, organisasjoner eller analysebyråer (Steen-Johnsen og Enjolras 2015, 132). Det krever betydelig kompetanse å analysere stordata. Ved bruk av data fra selskaper må forskere være bevisst på dataenes kontekst og bakgrunn, og dermed

[5] Application Programming Interface

[6] www.smartebyernorge.no

hvilke svar dataene kan gi. Meldinger på sosiale medier er ikke nødvendigvis autentiske utsagn, men ofte gjennomtenkt og basert på hvordan man ønsker å fremstå (Manovich 2011). Samtidig er det viktig å være bevisst på avmakt hos forbrukeren, som får sin kontroll over egne data redusert. Det kan være vanskelig å ha kunnskap om fremtidig bruk av data som man bytter bort for å være medlem av et nettsamfunn (Steen-Johnsen og Enjolras 2015, 132). I neste avsnitt vil vi se nærmere på utfordringer for personvernet som bruk av stordata fører med seg.

3.3 Utfordringer for personvernet

Overvåking og personvern er en mer aktuell problemstilling enn noen gang før, likevel er vi storforbrukere av applikasjoner og nettjenester. Informert samtykke og anonymitet er grunnleggende for hvordan myndigheter, selskaper og forbrukere forholder seg til personvern. Det er viktig å diskutere hvorvidt disse prinsippene begrenser de potensielle konsekvensene av utveksling av stordata. Vil de faktisk beskytte de verdiene som står på spill når nye applikasjoner med stordata kan true med å krenke personvernet (Barocas og Nissenbaum 2014)?

3.3.1 Informert samtykke

Informert samtykke har blitt kritisert fordi det har flere grunnleggende svakheter (Nissenbaum 2011; Solove 2013; Hull 2015). Imidlertid betyr ikke dette at informert samtykke som prinsipp bør forlates, det kan være det beste vi har foreløpig. Nissenbaum (2011) peker på to årsaker til hvorfor informert samtykke har blitt omfavnet av myndigheter og selskaper: For det første er informert samtykke definert som en rett til å selv kontrollere personsensitiv informasjon gjennom valgfrihet. For det andre er informert samtykke forenlig med konkurranse i et fritt marked ved at selgere og kjøpere bytter tjenester til markedsbestemte priser. Kjøpere blir informert om selgerens fremgangsmåter ved innsamling og bruk av personlig informasjon, og kan selv bestemme om prisen er rett.

Det er mange grunnleggende utfordringer med prinsippet om informert samtykke som bør tas på alvor. Et grunnleggende etisk spørsmål er hvorvidt personer *egentlig* står fritt til å velge å gjøre en transaksjon, gitt valgenes kontekst og hva kostnadene vil være ved å velge bort en nettside, en handel eller et sosialt nettverk. Dersom forbrukeren opplever at kostnadene ved å velge bort disse tjenestene er for store, kan det stilles spørsmål ved hvor frivillig det egentlig er at personlig informasjon byttes bort mot tjenester (Nissenbaum 2011). Et annet grunnleggende problem er at samtykke ofte blir meningsløst, fordi forbrukeren ikke kan vite hvordan dataene kommer til å brukes i fremtiden, på det tidspunktet hun gir sitt samtykke (Hull 2015). Disse utfordringene er kognitive ved at personer vanskelig kan ta informerte valg, og strukturelle fordi utformingen av reelle valg er mangelfull (Solove 2013).

Det er usikkert om det i det hele tatt er mulig å gi forbrukeren fullstendig informasjon slik at hun kan ta informerte valg. Det er to store kognitive utfordringer: Informasjon til brukerne og kompleksiteten i de avgjørelsene som må tas. Grunnsteinen i informert samtykke er nettopp at personer skal informeres om hva slags data som samles inn om dem og hvilket formål dataene skal brukes til. For at et samtykke skal gi mening, må forbrukeren vite hva hun samtykker til. Forbrukere leser ofte ikke samtykkeerklæringer eller endrer standardinnstillingene på nettsidene de besøker, eller nettsamfunnene de er medlem av, fordi de er for lange og vanskelige å forstå. Det er vanskelig å utforme et meningsfullt

samtykke, samtidig som det skal være kort og enkelt å forstå (Solove 2013; Barocas og Nissenbaum 2014).

Fremtidig bruk av dataene er en annen utfordring. Selv om forbrukerne prioriterer å lese samtykkeerklæringer, så mangler de kunnskap om potensiell fremtidig bruk og videreformidling av dataene de deler (Solove 2013). Det er vanskelig å se for seg hvordan dataene kan brukes i fremtiden, av hvem og til hvilket formål. De fleste dataene som samles inn i sanntid gjennom mobiltelefoner, apper og sensorer i dag, samles i store datasett uten at vi som brukere vet så mye om det (Prabhu 2015). Det kan være vanskelig å få innsikt i hvordan dataene brukes og transformeres til nye datasett (Kitchin 2016). Richards og King (2013) problematiserer mangelen på transparens, når stordata ifølge optimistene skulle gjøre verden mer transparent. De kritiserer at overvåkningen foregår «i hemmelighet» uten at brukerne har innsikt i hvilke avgjørelser som tas og hvilke data som lagres. I automatiserte systemer er det vanskelig å vite bakgrunnen for de avgjørelsene som tas. Mangel på transparens gjør at individer ikke har mulighet til å rette opp i eller slette data om seg selv, de vet ikke en gang hvem de skal henvende seg til. De vet ikke hvordan data som er samlet inn om dem blir brukt eller om handlinger basert på dataene er rettferdige. De har heller ikke mulighet til å holde datakontrollører ansvarlige for det som skjer (Kitchin 2016).

Det er vanskelig for enkeltpersoner å ha oversikt over ulike vilkår og betingelser for personvern knyttet til ulike tjenester. Selv om hver enhet ga brukere klare anvisninger for hvordan man kan beskytte personsensitiv informasjon, er det i sum altfor mange enheter som samler inn og bruker personlige data. Gjennomsnittspersonen har ikke nok tid eller ressurser til å administrere alle enhetene som har tilgang på personlig informasjon (Solove 2013). I tillegg har selskapene insentiver til å ha utydelige vilkår og betingelser for bruk av en tjeneste, slik at de kan tilpasses fremtidige behov. I 2014 sjekket Datatilsynet et ikke-representativt utvalg på 72 apper, hvorav litt over halvparten var norske. De fant at to tredjedeler av appene ba om én eller flere tilganger til persondata. Posisjon var mest etterspurt (Datatilsynet 2014). I noen tilfeller er det logisk hvilke tilganger appen ber om. For eksempel må en karttjeneste ha tilgang til posisjonen din, om du skal få hjelp til å finne veien. Av de appene som ba om tilganger i Datatilsynets utvalg, ba knapt halvparten om tilganger som det var vanskelig å forstå at de trengte (Datatilsynet 2014, 14).

For å oppsummere, er det flere utfordringer med informert samtykke. De to grunnleggende spørsmålene er om individet egentlig har et reelt valg ved å avstå fra samtykke og dermed tjenestene som tilbys, og om informerte valg overhodet er mulig.

3.3.2 Anonyme data

Anonyme data betyr at forbindelsen til enkeltindivider fjernes slik at dataene i utgangspunktet ikke utgjør noen trussel mot personvern. Et viktig spørsmål er om det i enkelte tilfeller er mulig å anonymisere data på en god nok måte. Forskning viser at data ofte kan deanonymiseres dersom de kobles til andre datasett. En annen utfordring er hvorvidt egenskaper ved en persons liv og identitet brukes til å gjøre slutninger om henne, selv om dataene i seg selv inneholder personsensitive opplysninger.

En av de viktigste måtene å sikre personvern på er å anonymisere data, blant annet gjennom å strippe data for personlig informasjon, bruk av pseudonymer eller aggregering av data (Prabhu 2015; Kitchin 2016). Mange selskaper anonymiserer data slik at de kan selges videre til tredjeparter. Dataene kan brukes videre på mange ulike måter som ikke nødvendigvis har noe å gjøre med den originale årsaken til innsamlingen, og uten noe krav om samtykke fra dem dataene omhandler. Det har oppstått et marked rundt kjøp og salg av data (Kitchin 2016). Det er imidlertid ofte mulig å identifisere enkeltpersoner i slike data.

Selv om dataene er anonyme isolert, kan det være mulig å identifisere personer dersom man kombinerer data med ulike informasjonskilder (Prabhu 2015). Flere forskningsbidrag viser hvordan det er mulig å identifisere individer i anonymiserte datasett. Et av de mest kjente bidragene er fra Narayana og Shmatikov (2008), som identifiserte 80 prosent av Netflix-brukere ved å koble et anonymisert datasett fra Netflix med en IMDB[7]-database.

Det er også mange bidrag som viser hvordan ulike metoder kan identifisere enkeltindivider i mobilitetsdata (for eksempel CDR-data eller GPS-data), se Gambs mfl. (2014) for et sammendrag. Gambs mfl. (2014) bruker en modell som beregner sannsynligheten for en persons mobilitetsmønster basert på tidligere posisjoner, for eksempel 'hjemme' og 'arbeid'. Det er spesielt steder en person besøker jevnlig og bruker en viss tid på, som utgjør grunnlaget for modellen. Dersom mobilitetsmønsteret til individer i et datasett observeres over en viss periode, og dermed kobles til et annet datasett med noen av de samme individene, så kan personene i stor grad (opp mot 45 prosent) re-identifiseres. Dette gjelder selv om mobilitetssporene aggregeres ved å gjelde hvert 2. minutt i stedet for hvert 10. sekund (Gambs mfl. 2014). Bruk av pseudonymer i et datasett er gjerne ikke nok for å bevare anonymitet, fordi mobilitetsmønstre inneholder informasjon som er unik og kan kobles tilbake til enkeltpersoner (Gambs mfl. 2014). For å unngå muligheter for identifisering, betyr det at man må fjerne både direkte personlige indikatorer og informasjon som har høy korrelasjon med personlige indikatorer. I hvilken grad dette gjøres når data deles med tredjeparter er usikkert (Kitchin 2016, 34).

Kommersielle aktører har ofte ikke behov for å vite identiteten din, men ønsker å drive målrettet reklame basert på hva slags person de *tror* du er. Det betyr at de bruker anonyme stordata til å lage profiler basert på data om egenskaper og oppførsel som kan knyttes til deg, uten å avsløre din faktiske identitet (Barocas og Nissenbaum 2014). Det kan være problematisk å gjøre slutninger om personer basert på deres handlinger, fordi det kan generere uriktige karakteristikker av personer som blir hengende ved dem (Kitchin 2016). Det kan krenke individuell autonomi og sosial rettferdighet dersom dette resulterer i ulik behandling av mennesker og styrer valgene som mennesker tar (Barocas og Nissenbaum 2014). I forlengelse av dette oppstår en utfordring som Barocas og Nissenbaum (2014) kaller for «mindretallets tyranni». Dersom noen få mennesker er villige til å gi fra seg personlig informasjon, kan dette innebære at det trekkes slutninger om de mange som deler visse observerbare egenskaper med dem. For eksempel kan det dine venner kommuniserer i sosiale nettverk brukes til å gjøre slutninger om deg som person. Et annet eksempel er hvordan et selskap registrerte handlevanene til kvinner som hadde fått barn i perioden før fødsel. Dette ble brukt til å trekke slutninger om at dersom andre personer hadde lignende handlevaner, ventet de sannsynligvis barn (Barocas og Nissenbaum 2014, 62).

For å oppsummere, er det to hovedutfordringer med anonymisering av stordata. For det første er det en fare for at slike data kan deanonymiseres ved å koble dem mot andre datasett. For det andre kan stordata tross anonymisering brukes til å gjøre slutninger om en person basert på egne handlinger eller handlingene til et mindretall. Det kan føre til diskriminering og begrense egne livsvalg.

3.4 En kontekstuell tilnærming til personvern

Det er et paradoks at de fleste verdsetter personvern høyt, men likevel er villige til å bytte bort personlig informasjon for å få tilgang til enkle tjenester som en applikasjon eller

[7] Internet Movie Database, en offentlig database for å rangere og anbefale filmer og TV-serier

nettside (Hull 2015). En forklaring på dette er at brukernes forventninger til personvern er avhengig av kontekst. Det er for eksempel forståelig at et navigasjonsprogram trenger å få tilgang til telefonens GPS-plassering, men ikke at et kalkulatorprogram skal ha en slik tilgang. Normene for personvern varierer med andre ord fra kontekst til kontekst.

Et teoretisk rammeverk som får økende oppslutning blant forskere er Nissenbaums (2010) kontekstuelle tilnærming til personvern[8]. Teorien om kontekstuell integritet tar utgangspunkt i at det finnes normer for hvordan informasjon deles med andre i ulike situasjoner. Den kontekstuelle integriteten opprettholdes når disse normene blir respektert, men den krenkes når normene blir brutt. Normer for hvordan informasjon deles med andre er basert på hva man mener *bør* gjøres, altså hva som er sosialt akseptert. Normene er ofte innebygd i systemer og må alltid vurderes i sammenheng med konteksten de fungerer i. Hvorvidt man aksepterer å dele personlig informasjon med en annen styres av fire verdier, kalt *informasjonsnormer*: Kontekst, roller, informasjonstype og overføringsprinsipper.

Kontekst: Det finnes et mangfold av ulike sosiale kontekster som har ulike regler og normer for informasjonsutveksling. Disse sosiale kontekstene utgjør et bakteppe for hvordan informasjonsnormene fungerer.

Roller: I en informasjonsutveksling er det minst to aktive aktører med ulike roller: Sender og mottager av informasjonen. Den tredje rollen definerer temaet for informasjonen, i en personvernsammenheng den personen man deler informasjon om. Det er viktig å spesifisere i hvilken kontekst aktørene handler. Normene som gjelder vil for eksempel være helt annerledes i informasjonsutveksling mellom lege og pasient enn om det dreier seg om en resepsjonist og en hotellgjest. Slike kontekster er kritisk når man skal vurdere hvorvidt personer mener personvernet er krenket eller ikke.

Informasjonstype: Informasjonens egenskaper, type og natur er viktig i en informasjonsutveksling. Typen informasjon som deles er kontekstavhengig: En lege kan spørre deg ut om din fysiske tilstand, men det ville oppfattes som upassende dersom sjefen din gjorde det samme.

Overføringsprinsipper: Informasjonen inneholder ofte begrensninger når den utveksles mellom aktører. Et overføringsprinsipp er konfidensialitet, som forhindrer mottager i å dele informasjonen videre. Andre prinsipper kan handle om at man fortjener å få informasjon, er berettiget til det, har mandat til det eller trenger det. Overføringsprinsipper kan også dreie seg om at man deler data frivillig og krever at avsender er klar over informasjonsutvekslingen og gir sitt samtykke til det. Det kan også innebære kjøp og salg av informasjon innenfor de reglene som finnes på det kommersielle markedet. I et vennskap deles for eksempel personlig informasjon frivillig, men det vil bli sett på som et svik dersom man røper denne informasjonen til andre eller snikleser vennens dagbok.

Stordata utgjør et nytt element som utfordrer den etablerte informasjonsflyten. Når man skal vurdere konsekvensene av dette for etablerte verdier, betyr det å undersøke hvorvidt den nye praksisen flytter oss nærmere eller lengre bort fra de etablerte informasjonsnormene. Det innebærer om bruk av stordata fremmer våre interesser, generelle moralske og politiske verdier og kontekstspesifikke mål, formål og verdier (Barocas og Nissenbaum 2014, 48).

[8] Dette perspektivet er videreutviklet av Martin (2012; 2016) som ser på forståelser av personvern som en form for sosial kontrakt.

4 Panelundersøkelse i Oslo og Tallinn

Teorien om kontekstuell integritet tar utgangspunkt i at det finnes normer for hvordan informasjon deles med andre i ulike situasjoner. Den kontekstuelle integriteten opprettholdes når disse normene blir respektert, men den krenkes når normene blir brutt. Normene er del av en uformell sosial kontrakt som innebærer hva slags informasjon som kan deles med andre i ulike situasjoner, og på hvilken måte det kan deles (Nissenbaum 2009; Martin 2012). Normene for hva som er akseptabelt er altså ikke nødvendigvis enhetlige på tvers sosiale situasjoner, relasjoner, geografi osv. Opprettholdelsen av slike normer er avgjørende for å ivareta tillitsforholdet innenfor sosiale fellesskap og mellom brukere og tilbydere av tjenester.

Bruk av store data for å utvikle smarte byer bør ikke bryte med grunnleggende normer for informasjonsdeling, personvern og kontroll. Nytteverdien av å dele data om bevegelsesmønstre, må stå i forhold til risikoen for uønsket overvåking og kontroll. Det er derfor viktig å ha innsikt i hva befolkningen forventer og aksepterer. Brudd på de generelle eller mer spesifikke normene for personvern vil i de fleste tilfeller ha betydelige negative konsekvenser. Tilliten mellom de involverte partene vil reduseres og kan i sin tur påvirke mer generell tillit til teknologiske systemer og samfunnet (Braun mfl. 2018).

I dette kapittelet skal vi undersøke nærmere hvordan innbyggerne i Oslo og Tallin oppfatter utfordringer knyttet til personvern og mobilitetstjenester. Vi vil spesielt rette oppmerksomheten mot de forventningene og holdningene som finnes for bruk av slike data i ulike kontekster, og hvilke forskjeller vi finner mellom byene. Først vil vi imidlertid si noe om landenes status når det gjelder digitalisering av offentlige tjenester og befolkningens tilgang på og bruk av internett.

4.1 Norge og Estland i et komparativt perspektiv

4.1.1 Digitalisering av offentlige tjenester

Estland er i en særklasse når det gjelder nasjonale strategier for digitalisering. Da Estland ble et selvstendig land i 1991, måtte alle systemer bygges opp på nytt. Dette ble sett på som en gyllen anledning til å effektivisere og digitalisere den offentlige forvaltning. Estland har den høyeste andelen av antall innbyggere som bruker offentlige tjenester på nett i Europa (78 prosent) (EDPR 2017). Til sammenligning er andelen innbyggere som bruker offentlige tjenester på nett drøyt 60 prosent i Norge (Johnsen mfl. 2018).

Norge er på mange områder kommet langt i å digitalisere den offentlige forvaltningen. Mange av prinsippene for den norske digitaliseringen er de samme som brukes i Estland (se faktaboks), for eksempel innlogging med en unik identitetskode. ID-porten som en felles løsning for innlogging til tjenester har hatt en kraftig økning i antall brukere, og Altinn som ble åpnet i 2003 har bidratt til økning i elektroniske skjemaer. Selvangivelsen er nå nesten fullstendig digitalisert, og NAV har økt antall digitaliserte henvendelser kraftig. Resepter er nesten full-digitalisert, mens flere tjenester for helseopplysninger vil prøves ut de neste årene (Meld. St. no. 27, 2015-2016).

Helseopplysninger er sensitive opplysninger, som man i Norge ikke har klart å få inn i et felles datasystem. I Estland er helseopplysninger en del av det offentlige datasystemet. Standardinnstillingen er at leger får tilgang til pasientens helseopplysninger, men alle har mulighet til å nekte tilgang til ulike deler av sine helseopplysninger til alle eller noen deler av helsevesenet (Priisalu og Ottis 2017). En av regjeringens hovedprioriteringer i IKT-politikken, som Estland allerede har gjennomført, er at informasjon til forvaltningen kun skal leveres en gang. Dette innebærer også at den enkelte skal få informasjon om hvilke instanser som lagrer, behandler og utveksler opplysninger om dem, til hvilke formål (Meld. St. no. 27, 2015-2016).

Tabell 4.1: Faktaboks: Digitalisering av offentlige tjenester i Estland.

I Estland er digitaliseringen av offentlige tjenester ganske avansert - man kan gjøre nesten alt over internett bortsett fra tre transaksjoner: Utstede ID-dokumenter, registrere ekteskap, og selge eiendom. Digitaliseringen av offentlige tjenester i Estland bygger på tre hovedpilarer (Priisalu og Ottis 2017):

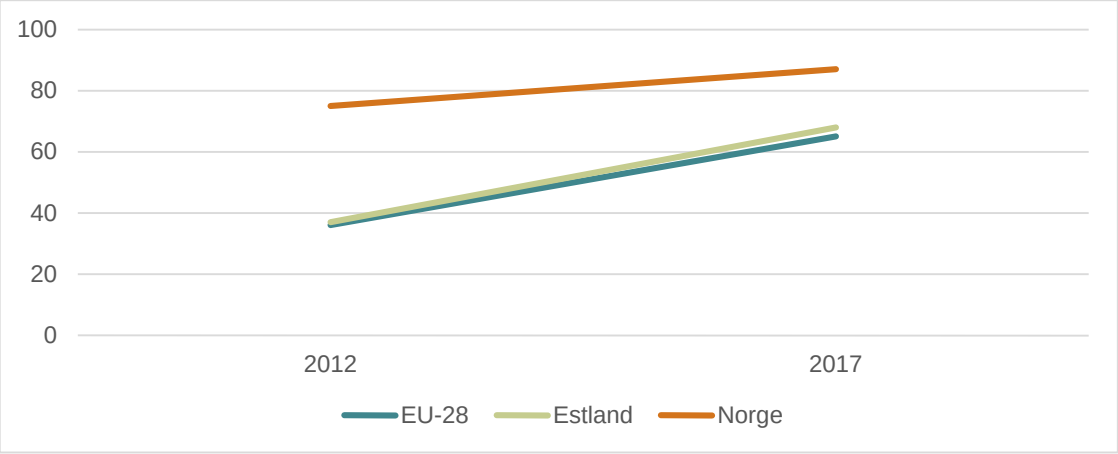
(1) Innføringen av en unik identitetskode (fødsels- og personnummer) for hver innbygger, slik vi også har i Norge.

(2) Sikre at alle innbyggerne har oversikt og kontroll over den personlige informasjonen som lagres i systemet. En digital signatur i form av et elektronisk ID-kort, brukes når innbyggerne kommuniserer med ulike deler av forvaltningen. Dette sikrer at uvedkommende ikke kan lage falske påstander på vegne av andre innbyggere. Eieren av den digital signaturen vil alltid kunne kontrollere datainnholdet under signaturen, og ID-kortet kan kryptere informasjon som kun eier vil ha mulighet til å dekryptere. Slik kan personen koble sine data fra institusjonell kontroll.

(3) Sikre rett bruk og organisering av data. Systemet kalles «X-road». Et underliggende prinsipp for innføringen av dette systemet er et visst nivå av gjensidig tillit mellom offentlige myndigheter og befolkningen. Innbyggerne må ha tillit til at myndighetene ikke misbruker informasjonen, mens myndighetene må ha tillit til at innbyggerne oppgir korrekt informasjon i systemet. Et annet prinsipp er prinsippet om at innbyggerne ikke skal bli forespurt å oppgi samme informasjon til ulike formål. Adresse, for eksempel, fylles automatisk inn i ulike elektroniske skjemaer ved behov. Innbyggerne vil ha oversikt over hvilken etat som har innhentet personlig informasjon om dem. Dersom noen har innhentet informasjon uten samtykke, kan dette meldes inn. Det har vært offentlige saker om offentlig ansatte som har gått inn på personlig informasjon om innbyggere uten å ha en legitim grunn for det.

4.1.2 Befolkningens tilgang på og bruk av internett

Innbyggerne i Norge har bedre tilgang på og bruker internett mer enn innbyggerne i Estland. Men det er spesielt bruk av internett via håndholdte enheter utenfor hjem og arbeid, hvor nordmenn skiller seg ut. Knapt 90 prosent av de spurte nordmenn bruker nett via håndholdte enheter, mens dette gjelder kun knapt 70 prosent av befolkningen i Estland, som er på linje med snittet av EUs befolkning (se Figur 4.1).



Figur 4.1: Individer som brukte en håndholdt enhet til å gå inn på internett utenfor hjem og arbeid i 2012 og 2017 (kilde: Eurostat)

4.1.3 Tillit og personvern

En forskjell som kan ha betydning for personvern knytter seg til i hvor stor grad befolkningen har tillit til hverandre og til statsapparatet. Norge er, som de øvrige skandinaviske landene, kjent for å ha høy grad av mellommenneskelig tillit og til politikere og offentlige organer (Andreasson 2017; Julsrud 2018). Dette anses ofte å være et viktig element i den nordiske samfunnsmodellen, der folk flest har tillit til hverandre og samfunnsinstitusjonene. Det er også en potensielt viktig faktor når det gjelder aksept for å gi fra seg personinformasjon til myndigheter, selskaper eller offentlige institusjoner. Norge utviklet en relativt restriktiv praksis når det gjelder tillatelse til å samle inn og analysere data som potensielt kan true personvernet

Estland har ikke spesielt høy score på eksisterende rangeringer av generell tillit i befolkningen, men denne har likevel vært økende i perioden 2010-2014[9]. Den er likevel markert sterkere enn det en finner i de øvrige baltiske landene. Kvantitative målinger tallfester andelen i befolkningen med høy generell tillit til 40% i Estland, mot 77 % i Norge.[10] Tilliten til politiske myndigheter er også lavere i Estland enn i Norge, men den har vokst seg sterkere siden årtusenskiftet (Puuranen 2016). Ulikheter på dette feltet vil naturlig nok kunne ha mange årsaker, og man kan tenke seg at befolkningens erfaringer fra tiden da de var innlemmet i Sovjetunionen (1940-1991) kan ha hatt negativ betydning for tillit til statsapparat og myndigheter. På den annen side kan det hende at dagens ledere sees på som representanter for et nytt system som står i motsetning til det kommunistiske regimet. Den stigende tilliten til myndigheter og forvaltning etter årtusenskiftet kan tyde på at dette er tilfelle.

Et tredje forhold er at Estland har innført et digitalt system for behandling av informasjon mellom offentlige myndigheter og privatpersoner, som mange har gode erfaringer med (Se Tabell 4.1). Det digitale systemet for tilgang til offentlig informasjon ble i 2007 utsatt for et omfattende cyber-angrep, som ledet til omfattende diskusjoner om sårbarhet, sikkerhet og personvern. I ettertid ble myndighetenes åpne og inkluderende debatt om sikkerhet knyttet til dette vurdert som positiv og tillitsbyggende (Priisalu and Ottis 2017).

[9] http://www.worldvaluessurvey.org/wvs.jsp

[10] Tallet indikerer andelen i befolkningen som er enig i et utsagn om at «folk flest er til å stole på».

4.1.4 Hypoteser

På bakgrunn av de forskjellene vi kjenner til, kan vi utlede følgende hypoteser om holdninger og normer for bruk av mobilitetsdata og personvern mellom befolkningen i Oslo og Tallinn:

1. Befolkningen i Oslo vil ha høyere institusjonell tillit enn befolkningen i Tallinn, og dermed ha større aksept for bruk av mobildata for å registrere mobilitet
2. Befolkningen i Oslo har høyere bruk av mobilkommunikasjon og applikasjoner og vil derfor være mer opptatt av at slike opplysninger beskyttes enn befolkningen i Tallinn
3. Befolkningen i Tallinn vil ha større tillit til at offentlige myndigheter behandler personlige opplysninger på en god måte sammenlignet med befolkningen i Oslo
4. Aksept for bruk av mobildata, og behov for beskyttelse, vil variere i henhold til brukersituasjon, i tråd med en kontekstuelle forståelsen av personvern.

4.2 Resultater fra spørreundersøkelsen

Nedenfor presenterer vi resultatene fra undersøkelsen som vi gjennomførte blant befolkningen i Oslo og Tallinn i desember 2017. Undersøkelsen tok for seg temaer knyttet til interesse for personvern, tillit i befolkningen, bruk av kommunikasjonsteknologi, tiltro til myndigheter og andre institusjoner, oppfatninger av risiko og sårbarhet, aksept for bruk av data, samt holdningsvariasjoner og holdningsfaktorer.

4.2.1 Interesse for personvern

Interessen for personvern ble kartlagt gjennom spørsmålet: Hvor opptatt er du av personvern, altså lover og regler som beskytter mot at informasjon om deg eller din familie blir benyttet av utenforstående uten at du selv ønsker det? Svarene indikerer en moderat interesse i begge byer, og en signifikant høyere interesse i Oslo, hvor om lag 3 av 4 i stor eller svært stor grad har interesse for personvernspørsmål (tabell 4.2). Det er ingen spesielle ulikheter knyttet til utdannelse, kjønn eller alder.

Andelen som har hørt om den nye personvernforordningen i EU som skjerper regelverket for personvern, er også høyere i det norske utvalget (tabell 4.3). Forskjellene her er imidlertid ikke like sterke. I Oslo-utvalget sier om lag halvparten at de har hørt om dette. Det er tydelige forskjeller i utvalget, ved at de med høyere utdannelse i større grad har hørt om forordningen.

*Tabell 4.2: Interesse for personvern, Oslo og Tallinn***. Prosent.*

	I svært liten grad	I liten grad	I verken liten eller stor grad	I stor grad	I svært stor grad	Vet ikke	Totalt
Oslo	1	5	20	46	27	0	100
Tallin	8	25	30	31	4	3	100
Sum	4	14	25	39	16	1	100

*** p<.001

Tabell 4.3: Kjennskap til EUs nye dataforordning. Oslo og Tallinn. Prosent.*

	Ja	Nei	Totalt
Oslo	49	50	100
Tallinn	45	55	100
Sum	**47**	**53**	**100**

* p<.05

4.2.2 Tillit i befolkningen

I mange tilfeller benyttes et dikotomt spørsmål for å måle dette, der en spør om folk flest er til å stole på, eller om en ikke kan være forsiktig nok i omgang med andre (Inglehardt and Weltzel 2005).

I tråd med hva man kan forvente ut fra tidligere internasjonale undersøkelser, er tilliten signifikant høyere i utvalget fra Oslo sammenlignet med utvalget fra Tallinn[11] (tabell 4.4). Forskjellene vedvarer når vi ser på tillit på et lavere nivå, såkalt inn- og utgruppe tillit (tabell 4.5). Inngruppe-tillit betegner i hvilken grad man har tillit til personer som man kjenner og har et etablert forhold til. Utgruppe-tillit betegner om man har tillit til personer utenfor den umiddelbare bekjentskapskretsen (Delhey and Weltzel 2012). Nivået for inngruppe-tillit er relativt likt for begge utvalgene, men det er sterkere tillit til familiemedlemmer i Estland. Det norske utvalget har signifikant høyere utgruppe-tillit.

Tabell 4.4: Generell tillit i Oslo og Tallinn. Prosent.

	De fleste er til å stole på***	Man kan ikke være forsiktig nok i omgang med andre mennesker	Total
Oslo	69	31	100
Tallinn	45	55	100

*** p < 0.001

Tabell 4.5: Inn- og utgruppe tillit Oslo og Tallinn. Prosent.

		Oslo	Tallinn
Inngruppe	Personer i familien din***	94	99
	Naboer***	48	50
	Personer du kjenner personlig***	87	81
Utgruppe	Personer du møter for første gang***	14	8
	Personer med en annen religion***	21	12
	Personer med en annen nasjonalitet***	24	19

*** p < 0.001

[11] Sett i sammenheng med WVS undersøkelsen fra 2014 kan det late til at tillitsnivået har styrket seg i Estland i løpet av de siste årene (fra 40-45%) men blitt svekket i Norge (fra 77 til 69%).

Det er tydelige forskjeller mellom byene når det gjelder tillit til sine respektive statsapparater. (Tabell 4.11). I Tallinn er andelen med tillit til nasjonalforsamling og politikere halvparten av det den er i Oslo.

Tabell 4.6. Andelen som har stor/svært stor grad av tillit til sentrale samfunnsinstitusjoner. Oslo og Tallinn. Prosent

	Regjeringen***	Politiske partier***	Stortinget***	Domstolene***	Offentlige myndigheter
Oslo	41	18	50	78	53
Tallinn	31	9	23	66	53

*** $p < 0.001$

4.2.3 Bruk av kommunikasjonsteknologi

Bruk av mobilkommunikasjon er et viktig grunnlag for registrering av mobilitet i befolkningen. Den viktigste kilden til kommunikasjon er mobiltelefoner med internett («smarttelefoner») som har GPS-posisjonering og kan innhente datamengder i en annen skala enn eldre modeller. Slik bruk fordrer mobiltelefoner med bedre datakapasitet enn tidligere modeller, samt mobilnettverk med tilstrekkelig overføringskapasitet. Registrering av mobilitet via mobiltelefoner kan gjøres «passivt» ved at abonnenter i et telefonnett posisjoneres romlig gjennom operatørenes basestasjoner. Det kan også gjøres «aktivt» ved at mobilbrukerne laster ned applikasjoner og aktivt registrerer og deler lokasjonsinformasjon med andre.

Befolkningen i de to byene har i de fleste tilfeller god tilgang til mobiltelefon med internett. I Oslo er penetrasjonen på 94 prosent (tabell 4.7). I Tallinn er andelen smarttelefonbrukere noe lavere (80 prosent). Dette er likevel en høy andel i europeisk sammenheng. Mobilbruk er blitt universelt, og kun to informanter oppgir at de ikke har mobiltelefon, begge bosatt i Oslo. Det er betydelige forskjeller knyttet til *alder* når det gjelder tilgang til smarttelefoner (Tabell 4.8). Dette er særlig fremtredende i Tallinn der knapt 40 prosent av de over 60 har smarttelefon. I Norge er tilsvarende andel 16 prosent. Dette viser at mange eldre ikke vil kunne benytte mobilitetstjenester gjennom apper, lokasjonsdata o.l.

Tabell 4.7 Tilgang til mobiltelefontyper og alder. Oslo og Tallinn. Prosent.

	Telefon med internett	Telefon uten internett	Total
Oslo***			
15-59	99	1	100
60 og eldre	83	16	100
	94	6	100
Tallinn***			
15-59	91	9	100
60 og eldre	61	40	100
	81	19	100
Alle	87	13	100

*** p<.001

Et stort flertall mener at mobiltelefonen er svært viktig for dem i deres hverdag – over 70 prosent i Oslo – og her er det signifikante forskjeller både knyttet til alder og kjønn (tabell 4.9). De yngre brukerne mener dette er mer viktig enn de eldre, og i Oslo er det kvinner som setter mest pris på mobiltelefonen.

Tabell 4.8. Respondentenes vurdering av mobiltelefonens betydning i dagliglivet og alder. Oslo og Tallinn. Prosent

	Veldig viktig	Litt viktig	Ikke viktig	Total
Oslo***				
15-59	78	19	2	100
60 og eldre	56	36	88	100
	71	24	4	100
Tallinn*				
15-59	56	39	5	100
60 og eldre	43	49	7	100
	51	43	6	100
Alle	61	33	5	100

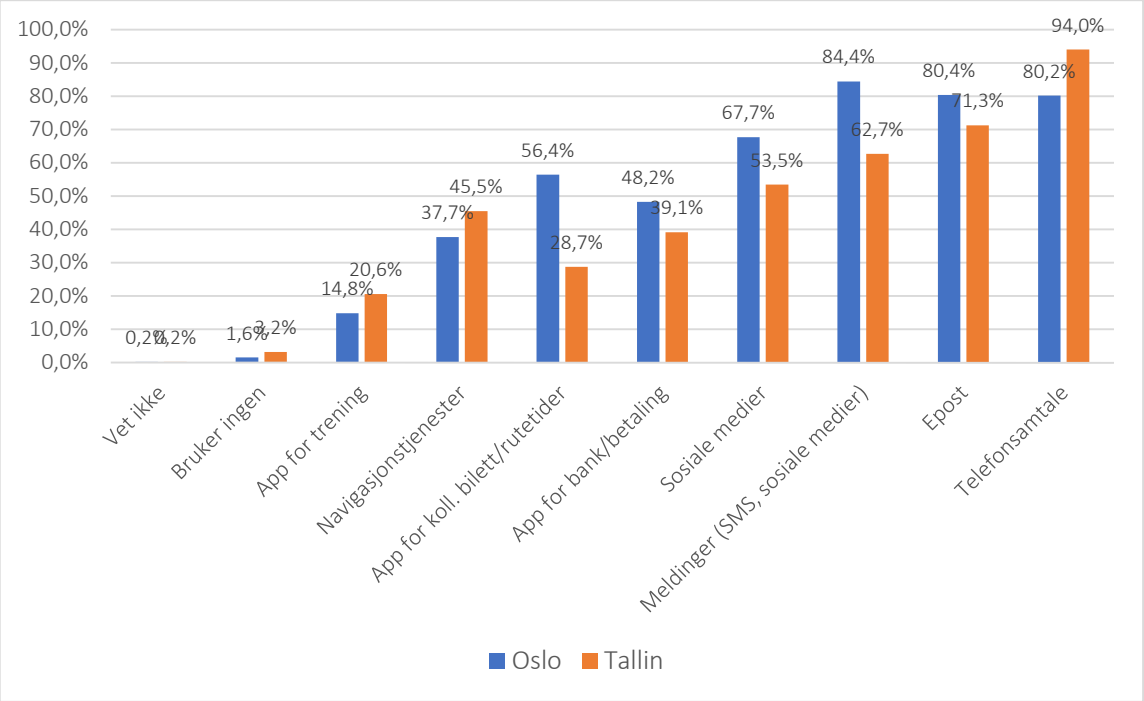
*** p<.001

Tabell 4.9. Respondentenes vurdering av mobiltelefonens betydning i dagliglivet og kjønn. Oslo og Tallinn. Prosent

	Veldig viktig	Litt viktig	Ikke viktig	Total
Oslo**				
Menn	62	30	6	100
Kvinner	77	20	3	100
	70	*24*	*4*	*100*
Tallinn**				
Menn	52	37	9	100
Kvinner	50	46	3	100
	51	*43*	*6*	*100*
Alle	61	33	5	100

Smarttelefonen har gitt de reisende mulighet til å benytte en lang rekke tjenester, der man i større eller mindre grad benytter geografisk posisjonering av seg selv og andre tilbud eller kommunikasjonspartnere. Applikasjoner som benytter posisjoneringsfunksjoner knytter dette ofte opp til andre typer data som kart og veidata, register over kommersielle tjenestetilbud, reiseinformasjon, mm. Denne typen tjenester gjør det i økende grad mulig for applikasjonsleverandører og nettleverandører å registrere og lagre mobilitetsmønster. Kopling mot ulike andre data gjør at anonymitet og personvern kan bli svekket.

Det er spesielt telefonsamtaler, meldinger og epost som benyttes av informantene i Oslo og Tallinn (figur 5.2). Meldingstjenester kan gjøres via sosiale medier eller som en mobiltjeneste (SMS), og i det norske panelet er dette mer populært enn taletelefoni. Generelt er de norske informantene mer orientert mot bruk av datatjenester enn de estiske, noe som selvsagt også betinges av tilgangen på mer avanserte mobiltelefontyper. Den største forskjellen ligger i bruk av apper for å kjøpe billett og sjekke rutetider, der andelen som bruker dette daglig er dobbelt så høy i Oslo. Navigasjonstjenester, som for eksempel GoogleMaps, benyttes av 46 prosent av utvalget i Tallinn mot 38 prosent i Oslo.



Figur 4.2. Digitale tjenester på mobiltelefonen som benyttes daglig, Oslo og Tallinn. Prosent.

Det er tydelige forskjeller mellom hvilke tjenester menn og kvinner foretrekker i de to byene (tabell 4.8). Sosiale medier er begge steder mer benyttet blant kvinner, og det samme gjelder meldingstjenester. Kvinner er også mer aktive brukere av apper for kollektivbilletter og ruteinformasjon, mens navigasjonstjenester benyttes uavhengig av kjønn.

Tabell 4.10. Digitale tjenester på mobiltelefonen som benyttes daglig og kjønn, Oslo og Tallinn. Prosent

	Oslo		Tallinn	
	Menn	Kvinner	Menn	Kvinner
Sosiale medier***	59	74	47	58
Navigasjonstjenester	38	38	49	43
Epost	79	82	72	71
Meldinger (SMS, sosiale medier)***	77	89	56	67
Telefonsamtale	85	77	93	95
App for bank/betaling	50	47	43	37
App for koll. billett/rutetider***	48	62	24	32
App for trening	12	17	22	20
Bruker ingen	3	1	3	3

4.2.4 Tiltro til myndigheter

Vi spurte informantene om hvilke aktører de mener har innflytelse på personvernet deres. I Oslo er tiltroen til myndighetenes innflytelse sterkere enn i Tallinn. Her er det derimot flere som mener at den enkelte har mest innflytelse, samt virksomhetene som forvalter slike data (tabell 4.11). Totalt sett legges det i begge byer størst vekt på de enkelte virksomheter. De markerte ulikhetene mellom utvalgene i de to byene er interessant, og som vi skal se senere i undersøkelsen finnes det lignende ulikheter på andre områder.

Tabell 4.11 Vurdering av ulike aktørers innflytelse over personvernet. Prosent

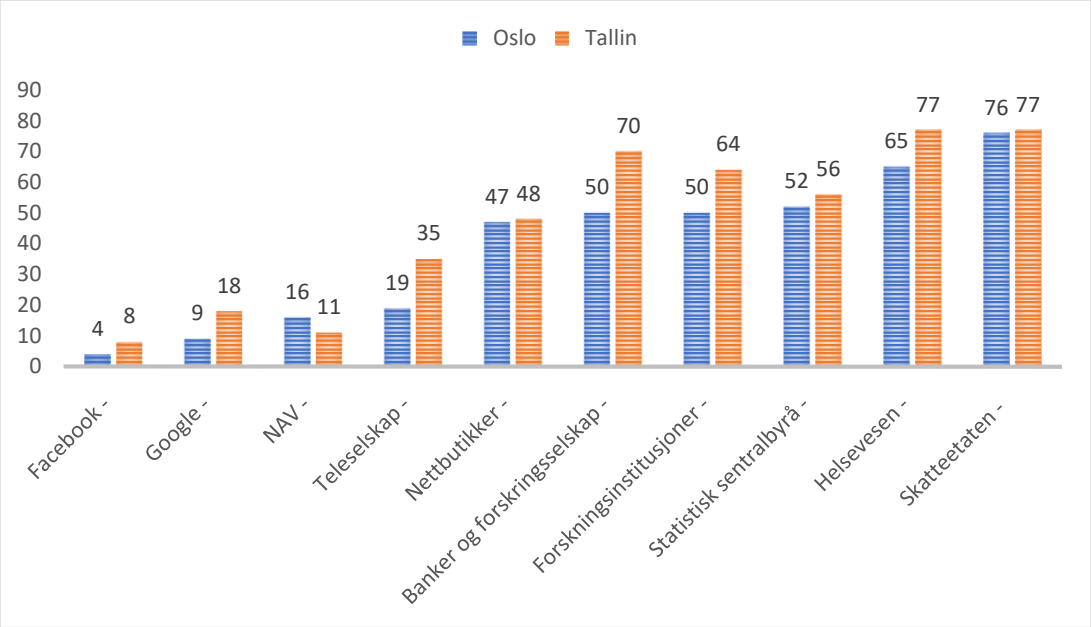
	Svært liten innflytelse	Liten innflytelse	Hverken eller	Stor innflytelse	Svært stor innflytelse	Na	Vet ikke	Totalt
*Myndighetene som forvalter regelverket****								
Oslo	1	3	18	40	30	1	8	100
Tallinn	5	7	21	26	30		12	100
Total	3	5	20	32	30	0	10	100
*Den enkelte gjennom egne valg****								
Oslo	1	5	17	36	29	10	4	100
Tallinn	4	5	13	23	49		5	100
Total	2	5	15	30	39	5	4	100
*Virksomheter som har personvernopplysninger****								
Oslo	2	4	14	31	42	1	6	100,0
Tallinn	1	4	11	23	57		5	100,0
Total	2	4	12	27	49	1	5	100,0

*** p<.001

Den generelle tilliten til regjering, politiske partier, storting og domstoler er som vist tidligere betydelig høyere i Oslo enn i Tallinn. Tilliten til institusjonenes evne til å håndtere personvern i er imidlertid sterkere i Tallinn (Figur 4.3). Dette gjelder for alle institusjoner med unntak av NAV (som i Estland har mindre tillit enn Google). Forskjellene er særlig store for teleselskap og banker/forsikringsselskap og forskningsinstitusjoner.

Det later altså til at det norske panelet har sterk generell tillit til statsapparatet og det politiske systemet, men lavere tillit til at offentlige og private aktører kan håndtere personvern på en god måte. I Tallinn er forholdet motsatt. En mulig årsak er at de i

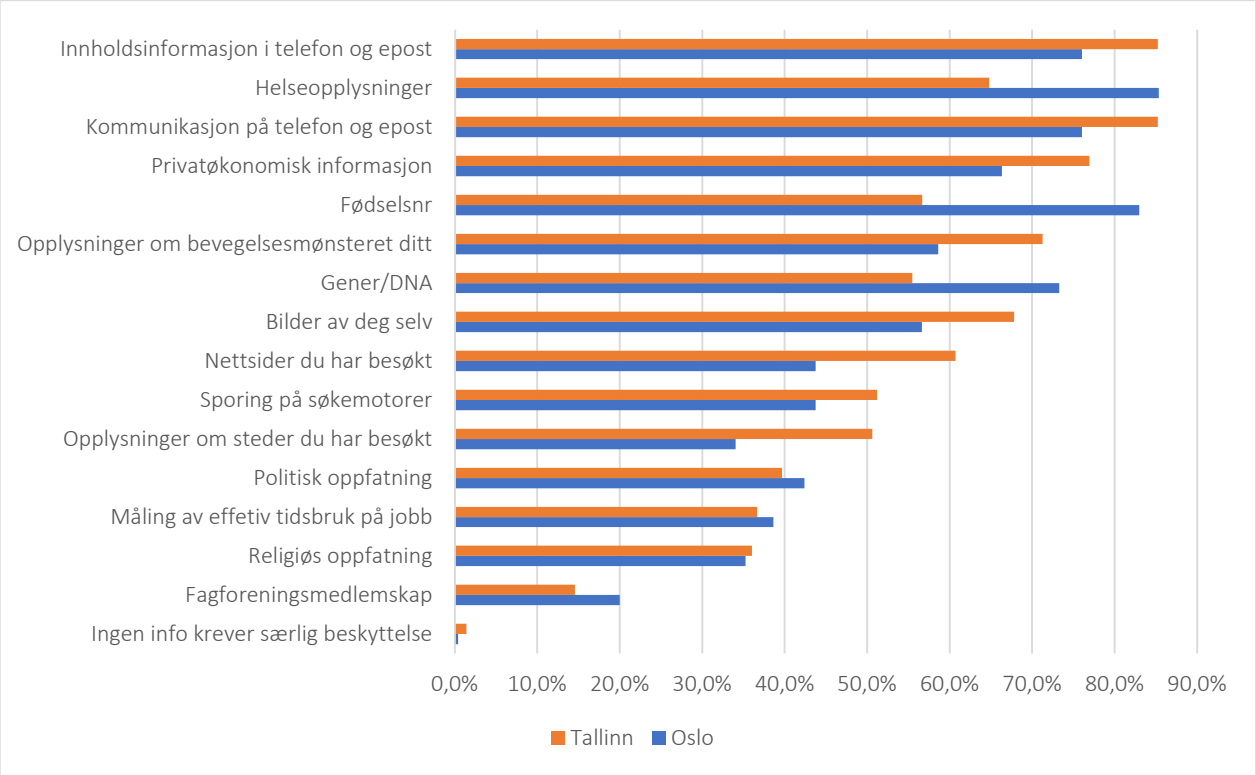
Estland har innført et digitalt system for behandling av informasjon mellom offentlige myndigheter og privatpersoner, som mange har gode erfaringer med. At tilliten til det politiske systemet er lavere behøver ikke å berøre disse forholdene. Nettselskaper som Facebook og Google har generelt svært lav tillit i begge byer, og det samme gjelder for NAV og teleselskap. I Oslo har halvparten av respondentene stor eller svært stor tillit til forskningsinstitusjoner når det gjelder håndtering av personvern.



Figur 4.3 Institusjoner respondenter har stor eller svært stor tillit til når det gjelder personvern. Oslo og Tallinn. Prosent.

4.2.5 Oppfattet risiko og sårbarhet

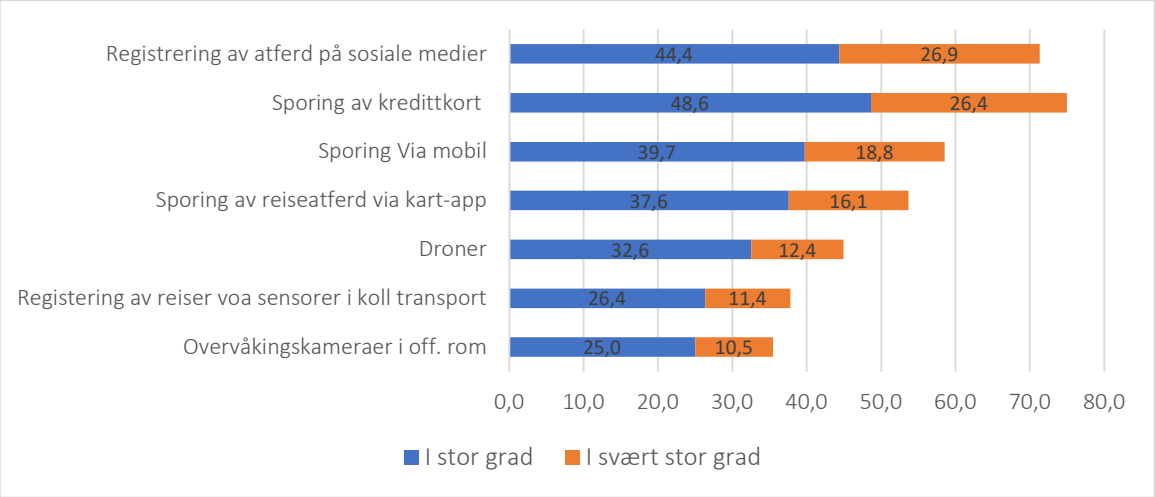
Informasjon om bevegelsesmønster oppfattes som en type personlig informasjon som bør lovbeskyttes. Dette mener et flertall av innbyggerne i begge byer, og i Tallinn er andelen som er enig i dette på over 70 prosent (Figur 4.4). Denne typen informasjon anses som like sensitivt som for eksempel informasjon om genmateriale og fødselsnummer. Mest sårbart, og med mest behov for beskyttelse, er innholdsinformasjon i epost og mobilkommunikasjon, samt helseopplysninger.



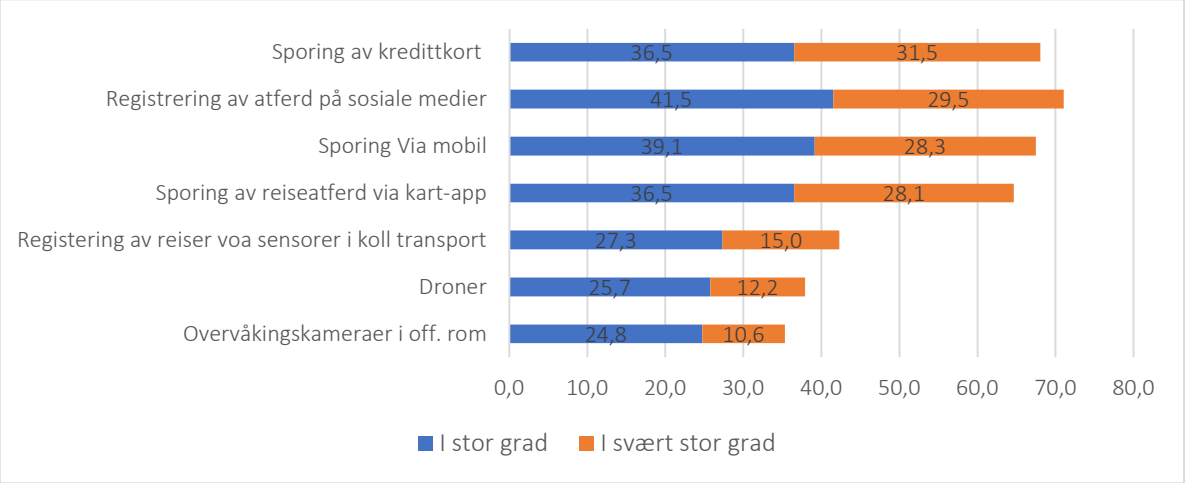
Figur 4.4 Personlig informasjon som innbyggerne mener lovverket særlig bør beskytte mot innsamling og analyse. Oslo og Tallinn. Prosent

Sett i forhold til den relativt høye andelen som benytter sosiale medier og navigasjonstjenester daglig, er det interessant at registrering av atferd på sosiale medier og sporing via kart-apper samtidig anses som viktige trusler mot personvernet. Kanskje er det slik at den høye bruken har initiert en ny type bekymring rundt dette de senere årene.[12] Sett i lys av den økende interessen for å kartlegge befolkningens mobilitet via teleoperatørers mobildata (CDR), er det verdt å merke seg at 40 prosent av borgerne i Oslo og Tallinn mener dette i stor grad truer personvernet (Figur 4.5).

[12] Undersøkelsen ble foretatt samtidig som det ble kjent at data fra Facebook hadde blitt videresolgt til selskaper som benyttet dette til å spre falske nyheter og påvirke valgresultater i blant annet USA. Dette kan ha påvirket resultatene på dette spørsmålet.

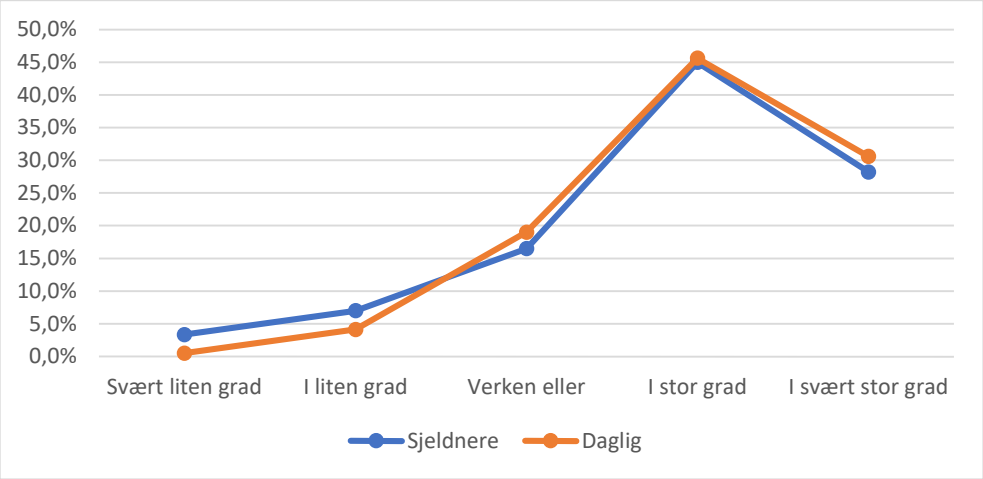


Figur 4.5. Digitale tjenester som respondentene mener truer personvernet i stor og svært stor grad, Oslo. Prosent

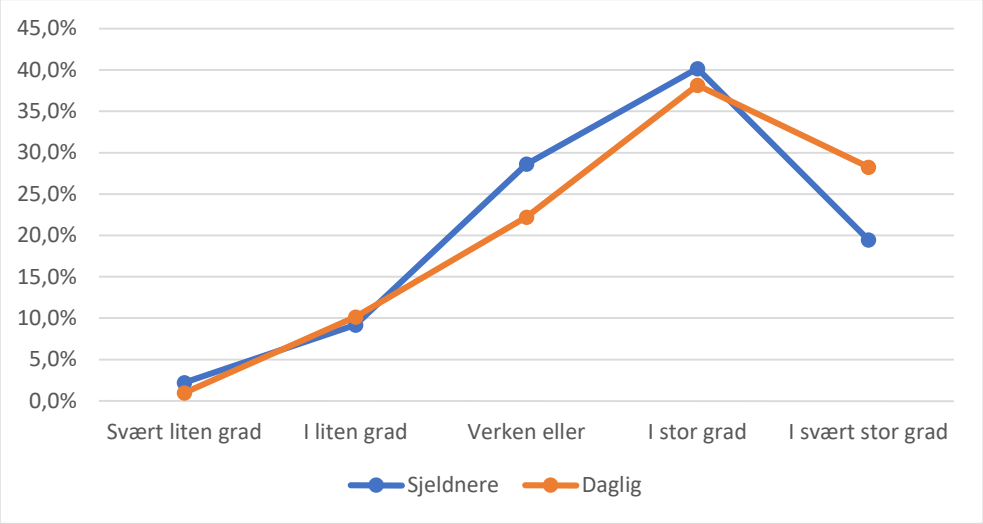


Figur 4.6. Digitale tjenester som respondentene mener truer personvernet i stor og svært stor grad, Tallinn. Prosent

Det er lite som tyder på at de som er aktive brukere av sosiale medier er mer bekymret for personvernhensyn enn de som bruker det i mindre grad. Som vist i figur 4.7 og 4.8 er ikke de aktive brukerne av disse teknologiene mer bekymret enn andre.

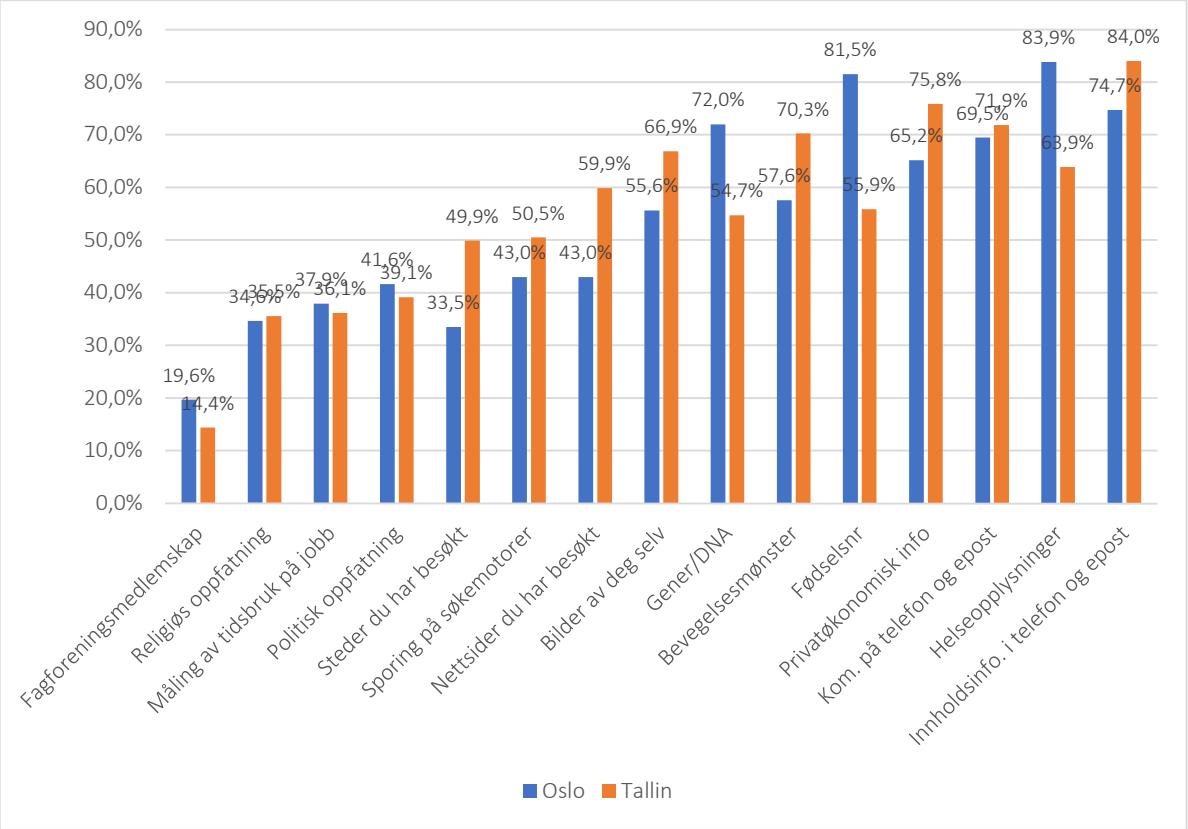


Figur 4.7. Bruk av sosiale medier og i hvilken grad sporing fra atferd på sosiale medier utgjør en trussel. Oslo og Tallinn. Prosent



Figur 4.8. Bruk av navigasjonstjenester (for eksempel GoogleMaps) og i hvilken grad sporing fra kart-applikasjoner anses å utgjøre en trussel. Oslo og Tallinn. Prosent

Hvilke typer informasjon er det respondentene mener lovverket bør beskytte oss mot? Øverst på listen står «innhenting og analyser av personlige samtaler og meldinger på telefon og epost» (Figur 4.9). Helseopplysninger og fødselsnummer anses som særlig viktig i det norske utvalget. Om lag 60 prosent av det norske utvalget mener videre at det er viktig at lovverket beskytter mot innhenting av informasjon/analyser av bevegelsesmønster. I Tallinn er dette ti prosentpoeng høyere. Som det fremgår av figuren er dette på nivå med informasjon om personlig genmateriale. Totalt sett anser panelene at informasjon om bevegelsesmønster har mer behov for beskyttelse enn spor og «bevegelser» som er gjort på nett.



Figur 4.9. Typer personlig informasjon som respondentene mener lovverket særlig bør beskytte mot innsamling og videre bruk. Oslo og Tallinn. Prosent.

4.2.6 Aksept for bruk av data

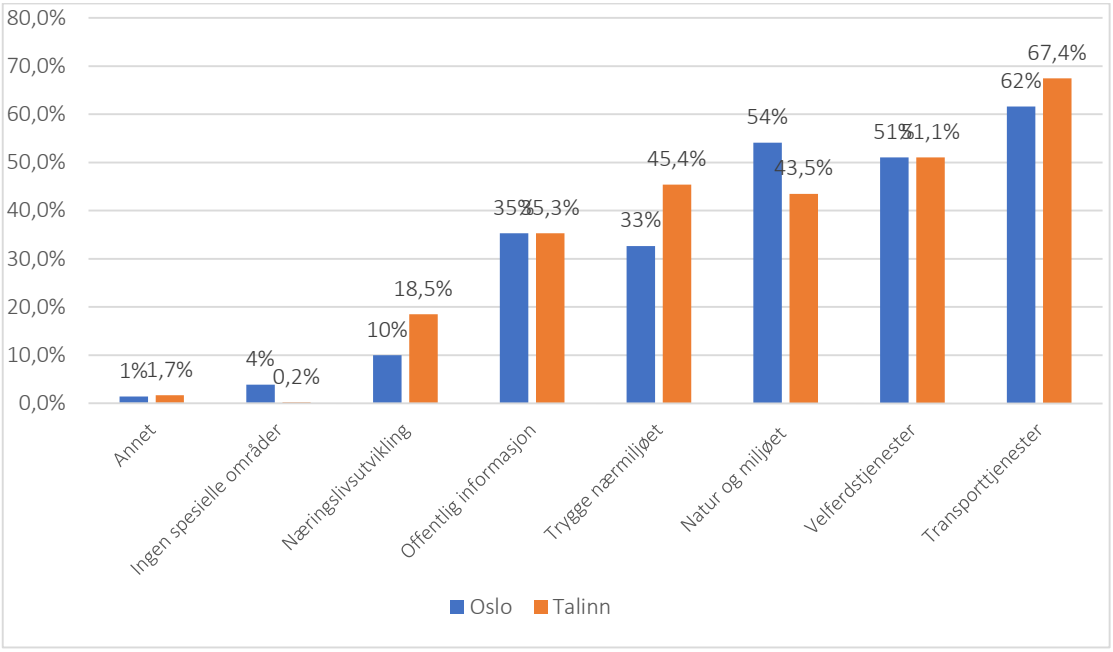
Smarttelefoner kan benyttes for å spore mobilitet, og det kan være områder der dette er mer akseptabelt enn andre, slik det er blitt beskrevet i den kontekstuelle tilnærmingen beskrevet ovenfor.

Tabell 4.12 viser at det er størst aksept for å bruke denne typen data for å forebygge terror og kriminalitet. Dette er det eneste feltet der det er et flertall som sier seg helt eller delvis enig i at dette er akseptabelt. Dernest kommer forbedring av transportsystemene, som drøyt halvparten synes er akseptabelt i stor eller svært stor grad. I Oslo er det 18 prosent som synes at det er akseptabelt å bruke slike data for å utvikle kommersielle produkter. Generelt er aksepten for bruk av slike data noe høyere i Tallinn enn i Oslo, men det er ingen tydelige skiller mellom kjønn eller alderskategorier.

Tabell 4.12 Områder der respondenter i stor eller svært stor grad aksepterer bruk av sporingsdata fra mobiltelefoner. Prosent.

	Utvikle nye kommersielle tjenester og produkter	Forskning	Forbedre transport-systemene	Forebygge terror og kriminalitet	M
Oslo	18	44	52	63	44
Tallinn	17	49	55	67	47

Ny teknologi kan benyttes til å utvikle byer på mange ulike felter. Presentert for en liste med definerte områder, indikerer befolkningen i Oslo og Tallinn at transporttjenester er det viktigste området å satse på, fulgt av velferdstjenester, og natur og miljørettede tiltak (Figur 4.10). Disse områdene anses totalt sett som viktigere enn å forbedre offentlig informasjon eller næringsutvikling.



Figur 4.10 Områder respondenter mener det er viktig å forbedre ved bruk av ny teknologi (angivelse av 1-3 områder per respondent). Oslo og Tallinn. Prosent.

4.2.7 Holdningsvariasjon

Vi har benyttet et batteri med spørsmål for å kartlegge holdninger og normer for bruk av mobilitetsdata og personvern i de to byene. Vi skal her gå igjennom hovedtrekk og undersøke noen sentrale mønstre i svarene.

Generelt er mange positive til å utnytte digitale data. Spesielt anser mange at faren for kriminalitet og terror gjør overvåking av befolkningen mer nødvendig (tabell 4.12). Tiltroen til at offentlige myndigheter ikke skal misbruke informasjon er høy i Oslo, og det er også troen på at denne typen data vil komme de reisende selv til gode. Sett under ett støtter godt halvparten av panelet i Oslo delvis eller helt disse utsagnene. Optimismen rundt

mulighetene er ikke mindre i Tallinn, selv om det også her er en svakere tillit til myndigheter og offentlige etater.

Tabell 4.13. Andel som er litt eller helt enige i utnyttelse av digitale data til samfunnsformål. Oslo og Tallinn, Prosent

	Vi må akseptere en større grad av overvåking for å kunne bekjempe kriminalitet og terrorisme***	Offentlige etater bør fritt kunne utveksle informasjon og data for å kunne utvikle best mulig tjenester***	Jeg stoler på at myndigheter ikke misbruker informasjon som er generert gjennom digitale medier og andre kilder***	Teknologiske systemer som registrerer befolkningens reiser vil hjelpe oss med å utvikle byer som er bedre å bo i	Registrering av reiseatferd via elektroniske data kommer også de reisende selv til gode
Oslo	68	46	64	51	59
Tallinn	76	54	52	53	57
Alle	72	50	58	52	58

*** p< .001

Ser vi på de mer kritiske utsagnene, støtter tre av fire i Oslo utsagnet om at digitale data har gjort samfunnet mer sårbart (tabell 4.14). Godt over halvparten er bekymret for at sporingsdata skal komme på avveie, spesielt i utvalget fra Tallinn. Det er interessant at så mange som 64 og 69 prosent av befolkningen i Oslo og Tallinn er enig i at de føler seg tvunget til å gi fra seg informasjon for å få tilgang til nødvendige tjenester. Det foreligger altså et betydelig «press» fra systemleverandører og andre ved bruk av mobile tjenester. Det kan også være at brukerne anser de digitale tjenestene som så attraktive at de likevel går med på å gi fra seg informasjon. Hvor viktige tjenestene i realiteten er kan være vanskelig å si, men de er trolig mer prekære i Tallinn der større deler av interaksjon med offentlige myndigheter skjer på digitale plattformer. Generelt er andelen som gir uttrykk for kritiske forhold knyttet til bruk av digitale data noe høyere enn de positive aspektene nevnt ovenfor. Dette behøver ikke å bety at panelet er delt i en positiv og negativ fraksjon, men at forhold knyttet til aksept og tiltro veies opp med like deler skepsis og ønske om varsomhet ved bruk av digitale data.

Det er stor aksept for å innføre restriksjoner og bestemmelser for personvern, og i Oslo mener over 80 prosent at det er bra at personvernlovene blir strengere (Tabell 4.15). Når godt over halvparten av informantene mener at det bør innføres strengere restriksjoner for å regulere bruken av data som inneholder bevegelsesmønstre, tyder dette på at mange mener at den i dag er svak eller fraværende.

Tabell 4.14 Andel som er litt eller helt enige i kritiske forhold knyttet til bruk av digitale data. Oslo og Tallinn

	Jeg føler med tvunget til å gi fra meg informasjon for å få tilgang til nødvendige tjenester**	Avhengigheten av digitale data har gjort samfunnet sårbart for terrorhandlinger, ulykker og katastrofer**	Jeg er bekymret for at data og informasjon om hvor jeg beveger meg er på avveie og vil kunne misbrukes i fremtiden	Kopling av digitale persondata vil i økende grad bli benyttet av politiske partier eller organisasjoner for å overvåke politiske motstandere**
Oslo	64	75	55	52
Tallinn	69	69	60	61
Alle	66	72	58	58

*** p< .001 ** p< .01

Tabell 4.15. Andel som er litt eller helt enige i legale restriksjoner. Oslo og Tallinn. Prosent

	Det bør innføres strengere tiltak for å regulere bruken av data der en registrerer folks personlige reisemønster ***	Det er bra at lovene for personvern blir strengere **
Oslo	57	83
Tallinn	55	74
Alle	56	79

*** p< .001 ** p< .01

4.2.8 Holdningsfaktorer

En faktoranalyse gir muligheter for å finne frem til underliggende mønstre i holdningsdataene, noe som kan forenkle tolkningen av svarene. I denne studien har vi benyttet prinsipal komponentanalyse (PCA) på 13 holdningsutsagn om bruk av digitale data, personvern og mobilkommunikasjon.

Dersom det er bakenforliggende faktorer som skaper varians i dataene kan dette skape problemer i en faktoranalyse. En KMO test viser en verdi på 0,787 noe som anses som tilstrekkelig. Bartletts test bør være signifikant på et nivå lavere enn .05, noe som er tilfelle for holdningsdataene i denne undersøkelsen (sig. = 0,000) Dette tilsier at de valgte variablene i undersøkelsen er egnet for å gjennomføre en faktoranalyse. Basert på en Varimax rotasjon fremkommer fire faktorer med en egenverdi på over 1. Ettersom tre av faktorene står for over 50 prosent av variasjonen i materialet vil vi benytte disse i den videre analysen.

Tabell 4.16 Komponentmatrise basert på Prinsipal komponentanalyse (PCS) og Varimax-rotasjon. (Kun verdier over 0,4 er inkludert).

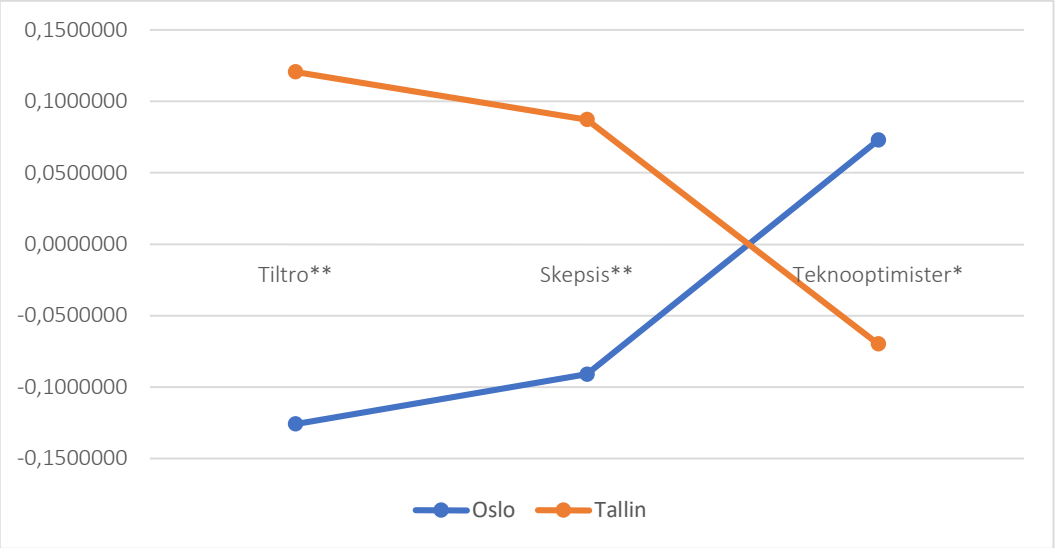
Rotated Component Matrixa			
	Component		
	Tiltro	Kritiske	Tekno optimister
Bare de som har noe å skjule har behov for personvern	0,758		
Vi må akseptere en større grad av overvåking for å kunne bekjempe kriminalitet og terrorisme	0,721		
Frykten for overvåking er overdrevet	0,716		
Offentlige etater bør fritt kunne utveksle informasjon og data for å kunne utvikle best mulig tjenester	0,506		0,470
Jeg stoler på at myndigheter ikke misbruker informasjon som er generert gjennom digitale medier og andre kilder	0,489	-0,432	
Kopling av digitale persondata vil i økende grad bli benyttet av politiske partier eller organisasjoner for å overvåke politiske motstandere		0,761	
Jeg er bekymret for at data og informasjon om hvor jeg beveger meg er på avveie og vil kunne misbrukes i fremtiden		0,677	
Jeg føler meg tvunget til å gi fra meg personlig informasjon for å få tilgang til nødvendige tjenester		0,628	
Avhengigheten av digitale data har gjort samfunnet alt for sårbart for terrorhandlinger, ulykker og katastrofer		0,491	
Teknologiske systemer som registrerer befolkningens reiser vil hjelpe oss med å utvikle byer som er bedre å bo i			0,898
Registrering av reiseatferd via elektroniske data kommer også de reisende selv til gode			0,882
Det er bra at lovene for personvern blir strengere -			
Det bør innføres strengere tiltak for å regulere bruken av data der en registrerer folks personlige reisemønster			

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 10 iterations.

Den første og viktigste variabelen forklarer nær 30 prosent, deretter 15 og 9 prosent for henholdsvis faktor 2 og 3. Den roterte komponentmatrisen viser hvilke variabler som inngår i faktorene (komponenter) (tabell 4.16). For å skille disse fra hverandre er disse gitt navn som søker å reflektere noe av meningsinnholdet i disse.

Den første og viktigste kjennetegnes av stor grad av *tiltro* til offentlige myndigheter, og at det er nødvendig med stor grad av informasjonsdeling og overvåking. De som skårer høyt på denne faktoren har i stor grad aksept for overvåking og tillit til at offentlige institusjoner tar hånd om dette på en måte som unngår misbruk. Den andre faktoren er derimot preget av en *skepsis* til myndigheters bruk av digitale data, blant annet på grunn av fare for utilbørlig overvåking og risiko for misbruk av dataene. Den siste faktoren – *teknologioptimister* – preges av en oppfatning om at ny teknologi er sentralt for å utvikle nye byer og bedre transportsystemer for brukerne.



Figur 4.11 Faktor-score befolkningen i Oslo og Tallinn. Gjennomsnittsverdier

I begge byene er tiltro-dimensjonen sterkest blant de eldste (60+), og signifikant lavere for yngre årsklasser. I Norge er skepsisen høyest blant middelaldrende, og her er også tiltroen lavest. Teknologioptimisme har mindre variasjon mellom årsklassene. Ser man på ulikheter mellom byene generelt, er tekno-optimismen sterkest i Oslo, mens innbyggerne i Tallinn har høye verdier både på dimensjonene for tiltro og skepsis (Figur 5.11). Dette indikerer muligens en sterkere grad av polarisering av holdningene i Estland.

Ikke overraskende er det også slik at det er sterke sammenhenger mellom tillit til samfunnsinstitusjoner og de holdningene man har til bruk av digitale data (tabell 4.17). Mistillit til de politiske institusjonene er forbundet med en skeptisk holdning til bruk av slike data. En teknologi-optimistisk innstilling korrelerer med en sterkere grad av institusjonell tillit.

Tabell 4.17 Korrelasjoner mellom faktorscore og tillit til samfunnsinstitusjoner. Oslo og Tallinn

	Oslo				
Faktorer	Tillit				
Holdningskategori	Regjeringen	Politiske partier	Stortinget	Domstolene	Offentlige myndigheter
Tiltro	,151**	0,052	0,042	0,025	0,075
Mistillit/skepsis	-,181**	-,277**	-,220**	-,200**	-,264**
Tekno optimisme	,135**	,192**	,228**	,319**	,266**

	Tallin				
Faktorer	Tillit				
Holdningskategori	Regjeringen	Politiske partier	Stortinget	Domstolene	Offentlige myndigheter
Tiltro	,197**	,163**	,172**	,110*	,259**
Mistillit/skepsis	-,191**	-,171**	-,109*	-,227**	-,158**
Tekno optimisme	,207**	,141**	,209**	,140**	,217**

4.3 Oppsummering

Estland har kommet svært lang i å ta i bruk digitale data for å koordinere og effektivisere interaksjon mellom offentlige myndigheter og enkeltpersoner. Samtidig er dette et land der det liberale demokratiske systemet er av nyere dato enn i Norge, og der det generelt er lavere tillit til myndigheter og det politiske systemet, noe som også kommer til uttrykk i denne undersøkelsen. Utviklingen i Tallinn ser likevel ikke ut til å ha drevet frem noen sterk motstand mot innsamling og bruk av persondata, men snarere en normalisering og aksept på mange områder. Sammenlignet med Oslo har befolkningen høy tillit til at offentlige og private virksomheter kan håndtere personvern.

I begge byer ser vi imidlertid at bekymringen for misbruk av disse dataene er betydelig og tidvis overgår de positive forventningene og tiltroen til at de offentlige myndighetene klarer å beskytte mot misbruk. Det ser ut som at det i Tallinn har vært en polariserende utvikling der aksept og nyttevurderinger verdsettes, samtidig som skepsisen også har blitt styrket. Det er verdt å merke seg at godt over halvparten av borgerne i begge byer er bekymret for at sporingsdata skal komme på avveie.

Bekymringen mot de risikable sidene ved bruk av mobile tjenester som kan spores, har tilsynelatende ikke lagt noen demper på bruken. De som er mest aktive brukere av sosiale medier og navigasjonstjenester på sine reiser er ikke mindre bekymret for personvern enn andre. En forklaring er at mange føler at de er nødt til å bruke disse mobile tjenestene i sin

hverdag, eller at de ikke mener at risikoen overgår fordelene. Det er interessant at så mange som 64 og 69 prosent av befolkningen i Oslo og Tallinn er enig i at de de føler seg tvunget til å gi fra seg informasjon for å få tilgang til nødvendige tjenester.

Den utbredte skepsisen til bruk av denne type data forklarer hvorfor det også er forståelse for tiltak som kan regulere bruken. Et stort flertall i begge byene mener det er bra at personvernlovgivningen blir strengere. Vi kan gjenfinne ulike oppfatninger av bruken av mobildata og personvern i utvalget. For det første en innstilling preget av *tiltro* til offentlige myndigheter, og at det er nødvendig med en stor grad av informasjonsdeling og overvåking. Samtidig er det en tydelig grunnholdning preget av *skepsis* til myndigheters bruk av digitale data, blant annet på grunn av fare for utilbørlig overvåking og risiko for misbruk av dataene. En tredje holdningstype preges av sterke forventninger om at *ny teknologi* vil bidra til å utvikle bedre transportsystemer for brukerne. Disse holdningene deler utvalget i tre ulike holdningssegmenter, selv om det også er mye overlappende holdninger.

Bruk av mobile data for å registrere mobilitet er avhengig av tillit til de som henter inn disse dataene. Det er derfor ikke overraskende at det er sterk sammenheng mellom tillit til samfunnsinstitusjoner og de holdningene enkeltpersoner har til bruk av digitale data. Tillit til politiske institusjoner er forbundet med tiltro til databehandling, mens mistillit er forbundet med en mer skeptisk holdning til data og personvern.

I første del av dette kapittelet fremsatte vi noen *hypoteser* som vi nå er bedre i stand til å vurdere. Den første av disse postulerte at befolkningen i Oslo ville ha høyere institusjonell tillit enn befolkningen i Tallin, og dermed større aksept for bruk av mobildata. Denne hypotesen ble ikke understøttet. Tillitsnivået til de politiske institusjonene er høyere i Norge, men den generelle aksepten for bruk av mobildata var likevel høyere i Tallinn enn i Oslo. Årsaken synes å være at befolkningen i den estiske hovedstaden har sterkere tillit til de operative samfunnsetatene, selv om tilliten til det politiske systemet er lav. Vi kan anta at det her også ligger en generelt høy grad av tillit til de tekniske systemene som håndterer personvernet i disse institusjonene, og erfaringen brukerne har med disse.

Den andre hypotesen postulerte at befolkningen i Oslo ville være mer opptatt av at data fra mobile enheter beskyttes enn befolkningen i Tallinn, på grunn av høyere bruk av mobilkommunikasjon og applikasjoner underveis. Det er imidlertid ingen sammenheng mellom bruk av mobilkommunikasjon og skepsis til personvernet som følge av slik bruk. Det er heller ikke slik at de norske brukerne er mer opptatt av å verne om mobildata enn de estiske, selv om nordmenn generelt har en sterkere interesse for personvernspørsmål. Denne hypotesen blir dermed ikke støttet av våre data.

Vi antok videre at befolkningen i Tallinn vil ha større tillit til at offentlige myndigheter behandler personlige opplysninger på en god måte sammenlignet med befolkningen i Oslo, på grunn av de generelt gode erfaringene befolkningen har med utnyttelse av persondata i det offentlige tjenestetilbudet. I Oslo har befolkningen noe større tillit til at personvernlovgivningen håndheves av myndighetene. Tilliten til institusjonenes evne til å håndtere personvern er imidlertid sterkere i Tallin. Dette tyder på at digitaliseringen av disse tjenestene har bidratt til å styrke tilliten til disse etatene. Denne hypotesen kan derfor støttes, selv om kausalmekanismene er uklare.

Vi antok også at aksept for bruk av mobildata, og behov for beskyttelse, ville variere i henhold til brukersituasjon. Resultatene viste at aksept for bruk av mobildata i stor grad var betinget av brukssituasjon og formål. I tilknytning til kriminalitet og terror og forbedring av transportinfrastruktur er aksepten for bruk størst. Denne hypotesen ble dermed understøttet.

5 Utfordringer og muligheter ved bruk av mobildata

Visjonen om utvikling av smartere byer er bygget på en grunntanke om at aktiv utnyttelse av teknologi kan bidra til å skape byer som vil gi bedre livskvalitet og levekår for innbyggerne. Det er sterke forventninger om at en mer radikal og integrert bruk av teknologi vil bidra til å løse mange av de utfordringer som verdens byer står ovenfor (Glasmeier and Nebiolo 2016). Registrering av befolkningens reiseatferd via mobiltelefoner antas å være en viktig del av det nye digitale økosystemet som i sum skal frembringe nye tjenester, blant annet innenfor transportsektoren (Steenbruggen, Tranos and Nijkamp 2014).

En bred bruk av mobildata er imidlertid betinget av at befolkningen aksepterer slik bruk, og at de har tillit til at de som henter inn denne typen data bruker det på måter som ikke går utover deres personvern. Litteraturen om smarte byer har så langt i liten grad vært rettet mot befolkningens opplevde behov og ønsker, men futuristiske visjoner om smarte og bærekraftige byer eksisterer side om side med dystopiske visjoner om byer preget av overvåking, undertrykking og kontroll (Vanolo 2016; Boyd og Crawford). Innhenting av personlige mobildata knytter an til både positive og negative forestillinger om fremtidens byer. En overdreven, eller feilaktig bruk av denne typen teknologi kan få betydelig negative konsekvenser, som bidrar til å underminere muligheten for å utvikle byer med bedre livskvalitet og levekår. En slik utvikling vil også på sikt kunne bidra til at den tilliten til sentrale samfunnsinstitusjoner brytes ned.

5.1 Sentrale utfordringer

Registrering og utnyttelse av mobildata begrenses til en viss grad av eksisterende lover og regler. Sentralt her er prinsipper om informert samtykke og anonymisering, slik at innhentet data ikke skal kunne tilbakeføres til enkeltindivider. Reglene for bruk er blitt skjerpet gjennom EUs nye personvernforordning som ble implementert våren 2018.

Utnyttelse av mobilitetsdata styres av et sett med uskrevne sosiale normer mellom personer, grupper og institusjoner. Dette er kontekstavhengige «regler» for bruk og deling av informasjon som er utviklet over tid og som styrer forventningene til personvernhensyn. Brukerne av digitale systemer og mobile applikasjoner forventer at myndighetene og tjenestetilbyderne handler i samsvar med disse normene. Dette handler ikke bare om hvilke typer data som registreres, men også til hvilket formål de benyttes, hvordan de behandles og hvem de skal deles med. Når en part bryter med denne sosiale kontrakten, vil dette rokke ved tilliten og stabiliteten til det sosiale systemet som det er en del av, og vil påvirkes negativt.

Omfattende bruk av ny teknologi som brukerne oppfatter at bryter med rutiner og normer for personvern, kan bidra til å svekke legitimiteten til private selskaper, institusjoner og myndigheter. Et eksempel på dette fikk vi når det våren 2018 ble kjent at Facebook hadde videresolgt data om sine brukere til et selskap som utvikler personprofiler til

markedsføringsselskaper og politiske PR-byråer[13]. Facebooks praksis for bruk av persondata ble senere beklaget av selskapet, men skandalen har bidratt til en skjerpet debatt om hvordan sosiale medier utnytter sensitive persondata.

Vi har i våre undersøkelser funnet klare tegn på det som ofte omtales som et «personvernparadoks», nemlig at personer ofte tilsynelatende handler i strid med egne holdninger når det gjelder teknologibruk (Marwick og Boyd 2014; Hull 2015). Til tross for en uttrykt bekymring om misbruk, fortsetter mange å benytte teknologien som før. Én forklaring kan være at brukerne oppfatter det som komplisert og vanskelig å få innsikt i disse prosessene, slik at de i stedet «satser på» at dette blir tatt hånd om av myndigheter eller andre. Alternativt kan det tenkes at den opplevde nytteverdien overgår de oppfattede risikoelementene. I situasjoner der mulighetene eller evnene til egen kontroll og oversikt svekkes, vil det være naturlig å legge større vekt på de generelle normene som gjelder.

5.2 Veien videre

Denne rapporten har vist hvordan det i dag eksisterer en viss aksept for bruk av mobildata i befolkningen, spesielt i forbindelse med å bekjempe kriminalitet og terror og utbygging av et bedre transporttilbud. Brukeraksept styres av formål, men også de aktuelle situasjonene der dette tas i bruk. Når det gjelder kommersiell bruk av slike data er det lav aksept, med mindre det er eksplisitt forståelse av nødvendigheten av dette (for eksempel i forbindelse med apper som benyttes til navigasjon).

Resultatene har vist at over halvparten av befolkningen i Oslo mener at mobildata i stor eller svært stor grad truer personvernet. Dette tyder på at det eksisterer en betydelig usikkerhet rundt hvordan slike data brukes i dag, og om dette er i tråd med etablerte prinsipper for personvern. Derfor bør en videre bruk av disse dataene gjøres med forsiktighet. Bruk av denne typen data i kommersielle sammenhenger vil kunne oppfattes som brudd på eksisterende normer. Et brudd på normene rammer selskapene som henter inn data (teleoperatører), men også institusjoner og selskaper som bestiller og utnytter seg av disse.

Offentlige etater som ønsker å utnytte denne typen data i en videre utvikling av transporttilbudet bør sikre seg at dette gjøres i samsvar med de normer, forventninger og ønsker som finnes i befolkningen. Utnyttelse av denne typen teknologi bør søke å involvere innbyggerne (som skal bruke systemene) slik at man utvikler løsninger som er tilpasset en gitt geografisk kontekst. På denne måten kan man også inngå i dialog om hvilke normer og forventninger som bør være gjeldende på dette feltet fremover (Konsti-Laakso and Rantala 2017). Innenfor forskning bør forskere være særlig påpasselige med å informere om hvorfor data innhentes og hvordan de vil bli benyttet. De forskningsetiske retningslinjene som gjelder for bruk av store data bør ligge til grunn for alle typer prosjekter hvor denne typen data tas i bruk (OECD 2016). Implikasjonene av de nye personvernforordningene i EU (GDPR) bør også avklares nærmere.

[13] https://www.bbc.com/news/technology-43649018

6 Litteratur

Andreasson, Ulf. 2017. "Tillit - det nordiske guldet." edited by Nordic Council of Ministers Secretariat Nordic Council of Ministers. København.

Barocas, S. og Nissenbaum, H. (2014). Big data's end run around anonymity and consent, i Lane, J., Stodden, V., Bender, S. og Nissenbaum, H. (red), Privacy, big data and the public good, Cambridge University Press, New York.

Boyd, D. og Crawford, K. (2012). Critical questions for big data. Provocations for a cultural, technological, and scholarly phenomenon. Information, Communication & Society Vol. 15, No. 5, s. 662-679.

Datatilsynet (2016a). EUs personvernreform. Publisert 20.2.2012, sist endret 19.2.2016.

Datatilsynet (2016b). Hva blir nytt med forordningen? Publisert 18.2.2016.

Datatilsynet (2014). Appenes informasjon og tilgang til personopplysninger. En kartlegging, oktober 2014.

Delhey, Jan, and Christian Weltzel. 2012. "Generalizing Trust. How Outgroup-Trust Grows Beyond Ingroup-Trust." *World Values Research* 5(3):46-69.

EDPR (2017). Europe's Digital Progress Report (EDPR) 2017 Country Profile Estonia.

EU (2015). Special Eurobarometer 431 "Data protection". Rapport Juni 2015. DOI: 10.2838/552336.

Gaffney, C. og Robertson, C. (2016). Smarter than Smart: Rio de Janeiro's flawed emergence as a smart city. Journal of Urban Technology, 1466-1853.

Gambs, S., Killijian, M.-O. og Cortez M.N.P. (2014). De-anonymization attack on geolocated data, Journal of Computer and System Sciences, Vol. 80 (8), 1597-1614.

Glasmeier, Amy K., and Molly Nebiolo. 2016. "Thinking about Smart Cities: The Travels of a Policy Idea that Promises a Great Deal, but So Far Has Delivered Modest Results." *Sustainability* 8(1122; doi:10.3390/su8111122).

Gregersen, F. og Weber C. (2016). Big Data eller spørreskjemaer? Ja takk! Samferdsel 24.11.2016.

Grossi, G. and Pianezzi, D. (2017). Smart cities: Utopia or neoliberal ideology? Cities 69, 79-85

Hjorthol, R., Engebretsen Ø. og Uteng T.P. (2014). Den nasjonale reisevaneundersøkelsen 2013/14 – nøkkelrapport. TØI-rapport 1383/2014.

Hollands R. G. (2008). "Will the real smart city please stand up?", City 12 (3), 303-320

Hull, G. (2015). Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data. Ethics Inf Technol Vol. 17, s. 89-101.

Inglehardt, Ronald, and Christian Weltzel. 2005. Modernization, Cultural Change, and Democracy. The Human Development Sequence. London: Cambridge.

Julsrud, Tom Erik. 2018. Organisatorisk tillit. Grunnlaget for samarbeid i nettverkenes tid. Bergen: Fagbokforlaget.

Kitchin, R. (2016). Getting smarter about smart cities: Improving data privacy and data security. Data Protection Unit, Department of the Taoiseach, Dublin, Ireland.

Kitchin, R. (2015). The real-time city? Big data and smart urbanism. GeoJournal Vol. 79, s. 1-14.

Kitchin, R. (2013). Big data and human geography. Opportunities, challenges and risks. Dialogues in Human Geography Vol. 3, s. 262-267.

Konsti-Laakso, Suvi, and Tero Rantala. 2017. "Managing community engagement: A process model for urban planning." *European Journal og operational Research* InPress.

Lombardi, P., Giordano S., Farouh H., Yousef W. (2012). Modelling the smart city performance, Innovation: The European Journal of Social Science Research, 25 (2): 137-149.

Larsson, A.O. (2015). Studying Big Data – ethical and methodological considerations, i Fossheim H og Ingierd H (red), Internet research ethics, Cappelen Damm Akademisk.

Manovich, L. (2012). Trending: The promises and the challenges of big social data, i Gold, M. K. (red), Debates in digital humanities, University of Minnesota Press, Minneapolis, London.

Martin K. (2016). Understanding privacy online: Development of a social contract approach to privacy. J Bus Ethics 137, 551-569.

Martin, K., Shilton K. (2016). Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices. The Information Society 32 (3), 200-216.

Meld. St. 27 (2015-2016). Digital agenda for Norge. Kommunal- og moderniseringsdepartementet.

Mora, L., Bolici R., Deakin M. (2017). The First Two Decades of Smart-City Research: A Bibliometric Analysis. Journal of Urban Technology 24 (1): 3-27.

Narayanan, A. og Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets. Proceedings of the IEEE Symposium on Security and Privacy, Washington, DC, USA (2008), pp. 111-125

Nissenbaum, H. (2011). A contextual approach to privacy online, Dædalus, the Journal of the American Academy of Arts & Sciences, Fall 4.

Nissenbaum H. (2010). Privacy in Context – Technology, Policy and the Integrity of Social Life. Stanford: Stanford University Press.

OECD (2016). Research Ethics and New Forms of Data for Social and Economic Research, OECD Science, Technology and Industry Policy Papers, No. 34, OECD Publishing, Paris. http://dx.doi.org/10.1787/5jln7vnpxs32-en

Pew Research Centre (2016). Mobile fact sheet. Survey conducted Sept. 29- Nov. 6 2016.

Prabhu, R. (2015). Big data – big trouble?, i Fossheim H og Ingierd H (red), Internet research ethics, Cappelen Damm Akademisk.

Priisalu, J., og Ottis, R. (2017). Personal control of privacy and data: Estonian experience, Health and Technology 17(4):441–51

Puranen, B. 2016. Similarities and differences in values aming Baltic and Nordic countries. Presentation, Tallinn 23/8-16, Inst. for Future Studies. https://www.eetika.ee/sites/default/files/www_ut/similarities_and_differencies_in_values_among_baltic_and_nordic_countries_bi_puranen.pdf

Richards, N.M. og King, J.H. (2013). Three Paradoxes of Big Data. Stanford Law Review Online Vol. 66, No. 41, s. 41–46.

SSB, 2017. Norsk mediebarometer. 05244. Andel som har tilgang til ulike medier og elektroniske tilbud i hjemmet (prosent), etter medietype, statistikkvariabel og år (1991-2017) https://www.ssb.no/statbank/table/05244

Solove, D. J. (2012). Privacy Self-Management and the Consent Dilemma. Harvard Law Review 1880 (2013); GWU Legal Studies Research Paper No. 2012-141; GWU Law School Public Law Research Paper No. 2012-141. Tilgjengelig på SSRN: https://ssrn.com/abstract=2171018

Steenbruggen, John, Emmanouil Tranos, and Peter Nijkamp. 2014. "Data from mobilephone operators: A tool for smarter cities?" *Telecommunications Policy* 39(4-5):335-46.

Steen-Johnsen, K. og Enjolras, B. (2015). Social research and Big Data – the tension between opportunities and realities, i Fossheim H og Ingierd H (red), Internet research ethics, Cappelen Damm Akademisk.

Stopher, P.R. og Greaves S.P. (2007). Household travel surveys: Where are we going?, Transportation Research Part A: Policy and Practice 41 (5), 367-381.

Sun, J., og Yan, J. (2016). Blockchain-based sharing services: What blockchain technology can contribute to smart cities." Financial Innovation 2(26): 1-9.

Tapscott, D., og Tapscott, A. (2018). Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World. London: Penguin Random House.

Townsend, Anthony. 2016. "Green Gadgets? The Smart-Cities Movement and Urban Environmental Policy." Pp. 62-86 in *Remaking the Urban Social Contract. Health Energy and the Environment*, edited by Michael A. Pagano. Chicago: The Universisty of Illionis Press.

Vanolo, A. (2016). Is there anybody out there? The place and role of citizens in tomorrow's smart cities. Futures 82, 26-36.

Vedlegg 1

KANTAR TNS

NORSK GALLUP

Transportøkonomisk institutt

Big Data

Pnr 17101511

29.11.2017

Innhold

1. UNDERSØKELSESDESIGN

1.1 Innledning

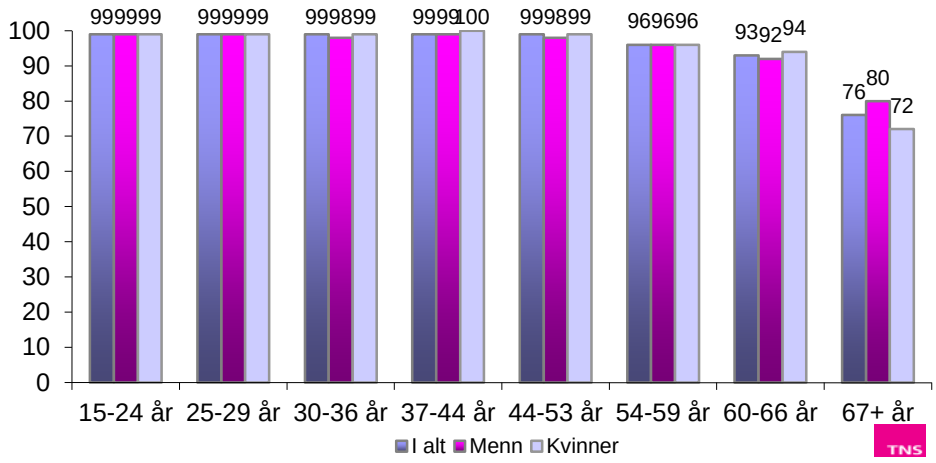
Kantar TNS har gjennomført datainnsamling for Transportøkonomis institutt (TØI), i kartlegging av befolkningens bruk av informasjonsteknologi og holdninger til personvern. Kartleggingen er gjennpomført parallet i Oslo og Tallinn. Informasjonen skal brukes i forsknings- og utredningssammenheng.

1.2 Målgruppe

Målgruppe er befolkningene i Oslo og Tallinn 18 år og eldre, til sammen 548.325 og 297.589 innbyggere henholdsvis.

Populasjons-grunnlaget er Kantars aksesspanel i de to byene. Når undersøkelsen gjennomføres med nettbasert skjema, er det av betydning for utvalgssammensetingen at respondentene har nettilgang. Eksempelvis er nettpenetrasjonen i Norge i aldersgruppen 60-66 år 93%, mens den faller til 76% i aldersgruppen 67 år og eldre (Figur 1).

Figur 1. Internettpenetrasjon etter alder, 2016.



Med uavkortet øvre aldersgrense, er det mulig at deler av målgruppen ikke er tilgjengelig på nett.

1.3 Utvalgsramme

Panelene er et forhåndsrekrutterte utvalg av personer 15 år og eldre som er villige til å delta undersøkelser. Deltagerne (i Norge) er *tilfeldig* rekrutterte gjennom andre telefon- (fast- og mobil) og postale undersøkelser, og utgjør *aktive* paneler.

1.4 Utvalgstrekning

Panelenes størrelse tilsier at det er mulig å trekke representative utvalg fra dem til ulike undersøkelser.

Paneldeltakernes bakgrunnskjennetegn er allerede kartlagt, og brukes til å rette undersøkelsen direkte mot målgruppen. Panelutvalg kan dermed tilrettelegges med større grad av presisjon enn hva som vanligvis er mulig gjennom andre metoder, ettersom paneldeltakernes bakgrunn er kjent på utsendingstidspunktet.

Populasjonen i denne undersøkelsen er forhåndsstratifisert etter alder og kjønn i de to byene (Tabell 1).

Tabell 1. Populasjon etter alder, kjønn og bosted. Prosent.

POPULASJON	Alder				
Oslo, N=548.325	18-29	30-44	45-59	60-89	Total
Kjønn					
Mann	12	17	11	9	50
Kvinne	13	16	11	11	50
Total	25	33	22	20	100
Tallinn, N=297.589					
Mann	3	16	12	12	43
Kvinne	3	17	14	23	57
Total	6	34	26	35	100

Andelen unge personer i aldesgruppen under 29 år er høyere i Oslo enn i Tallinn, særlig på bekostning av personer 60 år og eldre. Samtidig er kvinner noe overrepresentert i Tallinn.

Respondentene er trukket tilfeldig innenfor strataene.

1.5 Utvalgsstørrelse

Ønsket utvalg er 500 respondenter i hver by, til sammen 1.000 respondenter representative for målgruppen.

2. DATAINNSAMLING

2.1 Metode

Undersøkelsen er gjennomført over Internett. Ettersom de fleste etter hvert har fått nettilgang, brukes nettet i stigende utstrekning til intervjuundersøkelser.

Web-basert design gir stor fleksibilitet i utformingen av spørreskjemaet, og tillater for eksempel komplekse spørsmålsbatterier og filterstrukturer (slik tilfellet er i denne undersøkelsen), avspilling av lyd, vising av bilder (logoer) etc. Elektronisk kommunikasjon gir rask gjennomføring til lav kostnad. Særlig koplet mot Aksesspanelet er dette en effektiv metode, både i forhold til utvalgets kvalitet og innsamlingskostnad.

Spørreskjemaet er sendt ut som e-post med invitasjon til deltakelse, sammen med link til spørreskjemaets adresse på Internett.

2.2 Spørreskjemaet

TØI har laget utkast til spørreskjema, som er justert og endelig tilrettelagt i samarbeid med Kantar. Det består av 17 spørsmål – der enkelte spørsmål er integrert i spørsmålsbatterier og andre inngår i filterstruktur.

Ettersom Aksesspanelet inneholder en rekke typer bakgrunnsinformasjon på respondentene, legges disse til databasen i etterkant.

Spørreskjemaet finnes vedlagt (Vedlegg 1). Median intervjutid er 11 minutter, i begge byene.

2.3 Feltperiode

Datainnsamlingen er foretatt i november 2017. Etter prosjektoppstart den 06.11 og en innledende fase knyttet til spørreskjemadesignet, ble undersøkelsen pilotert den 13.11. Blant annet ble det etter hvert kjent at en del av befolkningen i Tallinn er russisktalende. Spørreskjemaet ble derfor oversatt til russisk i tilleg til den opprinnelig planlagte oversettingen til estisk. Pilot ble sendt til TØI for vurdering. Hovedundersøkelsen ble sendt ut den 14.11. Feltarbeidet ble avsluttet den 22.11.2017, etter en påminnelse.

3. ENDELIG UTVALG

3.1 Respons

Responsen i en undersøkelse rettet mot et aksesspanel vil avvike fra andre undersøkelsedesign, ettersom respondentene er forhåndsrekrutterte til å delta.

Undersøkelsen ble sendt ut til 3.617 respondenter (Tabell 2). Utvalget «oversamples» uansett i utgangspunktet ikke, ut over forventet innkomst: Selv om dette vil kunne gi raskere gjennomføring, vil personer som er lett tilgjengelige kunne bli overrepresenterte i utvalget. Tilsvarende er utvalget sendt ut sekvensielt i henhold til faktisk innkomst.

Tabell 2. Respons. Antall.

	Antall respondenter	
Status	Oslo	Tallinn
Utsendinger	1000	2617
Ikke kontakt	457	1973
Kontakt	543	644
Frafall:		
Ufullstendig utfylling	27	19
Vil ikke delta - self screening[1]	-	98
Teknisk feil	-	26
Intervju	516	501

[1] I Norge spores ikke åpning av e-post, da det trigger flere varslings-funksjoner hos respondentene.

Totalt sett er undersøkelsen åpnet av 1.187 respondenter (54% av utsendte i Oslo, 25% i Tallinn). Blant disse har 27 og 19 respondenter henholdsvis ikke returnert fullstendig besvarelse. I Tallinn har 98 respondenter åpnet skjemaet uten å fylle det ut, mens 26 er fjernet av tekniske årsaker. Feltarbeidet ble avsluttet med 2.017 respondenter. Besvarelsene utgjør i Oslo 95% av respondentene som har mottatt det og 52% av de utsendte skjemaene. I tallinn er de tilsvarende størrelsene 78% og 19%.

Ettersom undersøkelsen stenges når ønsket antall respondenter er oppnådd, har de sist ankomne respondentene ikke hatt anledning til å delta, og responsen underestimeres i så fall eventuelt i forhold til totalt antall utsendte skjemaer.

3.2 Endelig utvalg

Gitt utvalgsplanen, kan det endelige utvalget sammenliknes med befolkningskjennetegnene, for å vurdere eventuelle systematiske avvik (Tabell 3).

Tabell 3. Utvalg (uvektet) etter alder, kjønn og bosted. Prosent.

UTVALG			Alder		
Oslo, n=516	15-29	30-44	45-59	60-89	Total
Kjønn					
Mann	2	6	17	16	41
Kvinne	13	18	12	17	59
Total	15	23	29	33	100
Tallinn, n=501					
Mann	8	8	10	15	41
Kvinne	12	16	11	20	59
Total	20	24	21	35	100

Tabellen viser utvalgets fordeling etter kjønn og alder for de to byene, som kan sammenstilles med befolkningsfordelingen (Tabell 1). I Oslo-utvalget er befolkningen yngre enn 44 år noe underrepresentert til fordel for de eldste, samtidig som kvinner ern noe overrepresenterte. I Tallinn er de yngste under 29 år overrepresentert på bekostning av aldersgruppen 30-44 år. Kjønnsbalansen er om lag som i befolkningen.

Vi nevnte ovenfor at internettpopulasjonen har et noe høyere utdanningsnivå enn befolkningen for øvrig. Sammenlikning av utvalgsundersøkelser med offisiell utdanningsstatistikk er imidlertid ikke rett frem. Dels er aldersintervallene og referansetidspunktene ulike, og undersøkelsens begreper er ikke eksakt sammenliknbare med begrepene anvendt i offentlig statistikk (Utdannings-statistikken tar blant annet hensyn til hvilket år utdanningen er avsluttet). Dessuten vil respondentene ha vansker med å plassere seg i forhold til de «offisielle» kriteriene. Endelig tenderer respondentene til å overrapportere eget utdannningsnivå, særlig i forhold til korte utdanninger ut over videregående skole. I Oslo har 51% av befolkningen *16 år og eldre* utdanning på høgskole/universitetsnivå. I utvalget gjelder dette for 69%. Med disse forbeholdene in mente antydes det at personer med høy utdanning overrepresenteres noe.

3.3 Vekting av endelig utvalg

Det endelige utvalget er veiet tilsvarende befolkningsfordelingen, som følger:

1. Først sjekkes det at respondentene har informasjon på alle vektevariablene (alder, kjønn, bosted).
2. Utvalget grupperes i hht vektevariablene og vekter beregnes tilsvarende befolkningsandelene.
3. Vektingen er utført med enkel cellevekting.

Vektene fordeler seg som følger (Tabell 5):

Tabell 5. Vektenes fordeling. Antall og prosent.

vekt

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	,23	59	5,8	5,8	5,8
	,35	41	4,0	4,0	9,8
	,58	82	8,1	8,1	17,9
	,64	87	8,6	8,6	26,5
	,69	86	8,5	8,5	34,9
	,82	74	7,3	7,3	42,2
	,88	63	6,2	6,2	48,4
	,89	91	8,9	8,9	57,3
	1,01	66	6,5	6,5	63,8
	1,05	82	8,1	8,1	71,9
	1,12	102	10,0	10,0	81,9
	1,20	49	4,8	4,8	86,7
	1,32	54	5,3	5,3	92,0
	2,04	40	3,9	3,9	96,0
	2,97	30	2,9	2,9	98,9
	5,52	11	1,1	1,1	100,0
	Total	1017	100,0	100,0	

Vedlegg 1. Spørreskjemaet

Spørreskjemaet er utarbeidet på norsk, og oversatt til henholdsvis Estisk og Russisk. Se eget vedlegg (Excel format).

- I spørsmål om vurdering av lokale institusjoner, er estiske ekvivalenter satt inn.
- For yrke og inntekt er lokale standarder anvendt.

Transportøkonomisk institutt (TØI)

Stiftelsen Norsk senter for samferdselsforskning

TØI er et anvendt forskningsinstitutt, som mottar basisbevilgning fra Norges forskningsråd og gjennomfører forsknings- og utredningsoppdrag for næringsliv og offentlige etater. TØI ble opprettet i 1964 og er organisert som uavhengig stiftelse.

TØI utvikler og formidler kunnskap om samferdsel med vitenskapelig kvalitet og praktisk anvendelse. Instituttet har et tverrfaglig miljø med rundt 70 høyt spesialiserte forskere.

Instituttet utgir tidsskriftet Samferdsel med 10 nummer i året og driver også forskningsformidling gjennom TØI-rapporter, artikler i vitenskapelige tidsskrifter, samt innlegg og intervjuer i media. TØI-rapportene er gratis tilgjengelige på instituttets hjemmeside www.toi.no.

TØI er partner i CIENS Forskningssenter for miljø og samfunn, lokalisert i Forskningsparken nær Universitetet i Oslo (se www.ciens.no). Instituttet deltar aktivt i internasjonalt forskningssamarbeid, med særlig vekt på EUs rammeprogrammer.

TØI dekker alle transportmidler og temaområder innen samferdsel, inkludert trafikksikkerhet, kollektivtransport, klima og miljø, reiseliv, reisevaner og reiseetterspørsel, arealplanlegging, offentlige beslutningsprosesser, næringslivets transporter og generell transportøkonomi.

Besøks- og postadresse:
Transportøkonomisk institutt
Gaustadalléen 21
NO-0349 Oslo

22 57 38 00
toi@toi.no
www.toi.no