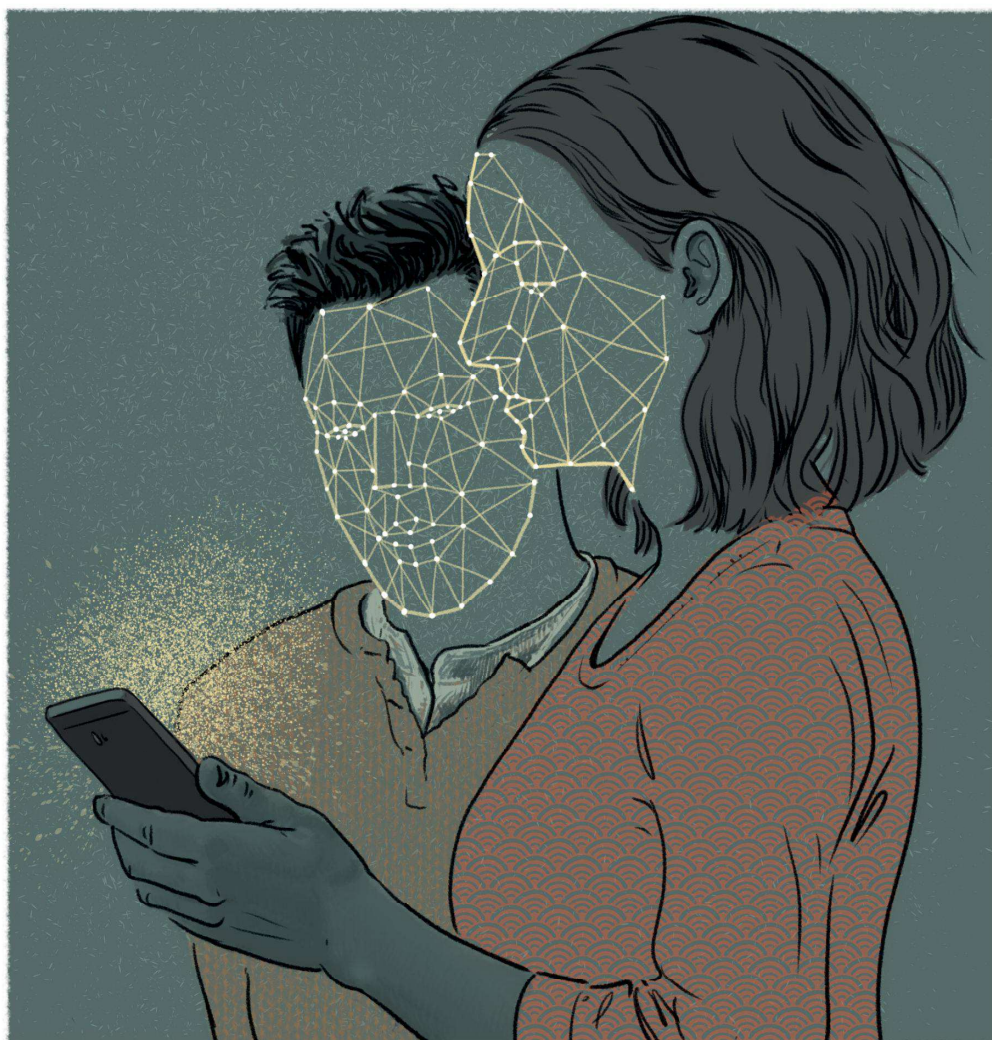




PERSONVERN 2018

TILLIT OG FØLELSER

JANUAR

NY PERSONOPPLYSNINGSFORSKRIFT

I januar trer den nye personopplysningsforskriften i kraft. Dette innebærer blant annet at virksomheter ikke lenger trenger å melde inn kameraovervåkning til Datatilsynet.

MARS

TINDER SNUR ETTER NORSK PRESS

Etter at norske forbrukermyndigheter anklaget Tinder for å ha ulovlige brukervilkår, endret Tinder vilkårene. Blant annet står det ikke lenger at de kan bruke bilder til markedsføringsformål uten brukernes samtykke.

MAI

NRK-AVSLØRING OM HELSE SØR-ØST

NRK avslørte at IT-arbeidere i blant annet Øst-Europa og Asia hadde hatt tilgang på sensitive pasientopplysninger til nesten tre millioner nordmenn. I oktober ga Datatilsynet ni helseforetak et overtredelsesgebyr på 800.000 kroner hver for å ikke ha oppfylt pliktene til sikkerhetsledelse, risikovurderinger og tilgangsstyring i forbindelse med tjenesteutsetting av IKT-Drift til utlandet.

SEPTEMBER

HALVE USA RAMMET AV DATAINNBREDD

Kredittbyrået Equifax ble frastjålet personopplysninger om over 140 millioner amerikanske innbyggere. Den stjålne informasjon inkluderte blant annet fødselsdato, adresser, kredittkortnummer og personnummer.

MARS

ALEXA BLIR VITNE I DRAPSSAK

Smarte assistenter blir stadig mer vanlige, og så lenge disse er påslått lytter de til alt som blir sagt i rommet, slik at de kan reagere på kommandoer. I forbindelse med en drapsetterforskning i USA ba politiet om innsyn i alle logger til en av Amazon's smarte assistenter for å se om det fantes lydopptak som kan hjelpe etterforskningen.

MAI

99 LAND RAMMET AV DATAANGREP

Over 200.000 maskiner i over 150 land ble utsatt for et hackerangrep som gjorde at maskinen deres ble låst. Det ble framsatt et løsepengekrav i form av Bitcoins for å åpne maskinene igjen. En svakhet i Windows var hovedårsaken til at angrepet lyktes. Angrepet rammet blant annet flere britiske sykehus.

AUGUST

IT-SKANDALE FØRER TIL STATSRAÅDVGANG

Det ble avslørt at sjefen i Transportstyrelsen ikke hadde tatt vare på sensitiv informasjon på en sikker måte. Dataene, som hemmelig forsvarsinfo, kom på avveie i utlandet. Dette førte blant annet til at Transportstyrelsens sjef måtte gå av og betale en bot. Senere har flere statsråder måtte gå av.

SEPTEMBER

TELEFON ÅPNES MED ANSIKTSJENNING

FaceID vil gjøre ansiktsgjenkjenning til "allemannseie" når Apple inkluderer teknologien i sin nyeste Iphone. Apple sier at den biometriske informasjonen om ansiktene bare skal lagres lokalt, og ikke sendes til skyen.

PERSONVERN 2018

TILLIT OG FØLELSER

ISBN 978-82-92447-92-5 (trykket utgave)
ISBN 978-82-92447-93-2 (elektronisk utgave)

Utgitt: Oslo, januar 2018

Omslag: Simon J-Eide

Trykk:

Copyright © Teknologirådet

Elektronisk publisert på: www.teknologiradet.no

FORORD

For sjette året på rad markerer Datatilsynet og Teknologirådet den internasjonale personverdagen. Det har blitt en tradisjon at vi denne dagen setter dagsaktuelle temaer i skjæringspunktet mellom teknologi og personvern på agendaen.

I fjorårets personvernrapport vendte vi blikket mot kunstig intelligens i finanssektoren og i offentlig sektor. Vi så på hvordan persontilpassing og forutseende tjenester kan gi oss bedre og mer brukervennlige tjenester, samtidig som data om oss brukes på nye måter.

For personverndagen 2018 har ikke kunstig intelligens blitt mindre relevant, og preger en rekke av sakene vi ser på i år også. Samtidig var året som gikk preget av en rekke hendelser som gjør det naturlig å ta et ekstra blick på sikkerhet.

I årets rapport skriver Datatilsynet om tillit: Hvem kan vi stole på med dataene våre? Stoler vi på at offentlige og private aktører tar gode valg ved tjenestetilsetting til utlandet? Forbrukerelektronikk blir stadig mer tilkoblet, og det er vanskelig å vite hvor data sendes. Kinesiske selskaper kommer på banen med betalingstjenester som kan være interessante for nordmenn, men kan vi stole på at de ivaretar personvernet vårt?

Teknologirådet tar for seg tre trender som kan gjøre seg gjeldende for personvernet fremover: *Emosjonell overvåking* medfører at ny teknologi, for eksempel for ansiktsgjenkjenning, brukes for å komme nærmere følelsene våre. *Smart mobilitet* innebærer både selvkjørende biler og nye og mer personlige transporttjenester. Forsvinner muligheten til å reise anonymt? I tillegg vil vi ta for oss *blokkjeden*, en teknologi som lover å løse utfordringer med tillit og sikkerhet. Men er det nødvendigvis godt nytt for personvernet?

Tusen takk til prosjektlederne hos Datatilsynet og Teknologirådet for godt arbeid med rapporten.

30. januar 2018

Tore Tennøe
Direktør i Teknologirådet

Bjørn Erik Thon
Direktør i Datatilsynet

INNHold

TEKNOLOGITRENDER	9
EMOSJONELL OVERVÅKING	10
SLIK MÅLES FØLELSENE DINE.....	11
HER BRUKES EMOSJONELL OVERVÅKING.....	12
HVA SYNES FOLK?	18
KUNSTIG INTELLIGENS MØTER EKTE FØLELSER	19
FREMTIDENS TRANSPORT: SELVKJØRENDE, SMART OG SPORBAR	21
REISEN BLIR DIGITAL.....	21
SELVKJØRENDE BILER: DATAMASKINER PÅ HJUL	22
EN STRØMMETJENESTE FOR TRANSPORT	27
SKAL VI HA OVERVÅKNINGSØKONOMIEN MED I BAGASJEN?.....	30
BLOKKJEDEN OG PERSONVERNET	31
HVA ER BLOKKJEDER?	32
SIKKER HÅNDBTERING AV DATA	33
ANONYMITET OG PSEUDONYMITET	34
MER KONTROLL TIL BRUKERNE	35
SIKRE TRANSAKSJONER OG UTVEKSLING AV DATA.....	36
UFORGLEMMELIGE MULIGHETER	37

TILLIT	39
TILLIT TIL TJENESTEUTSETTING	40
INFORMASJONSSIKKERHET OG TILLIT	41
LITE TILLIT I BEFOLKNINGEN	42
DEBATT OG KONTROLL FRA MYNDIGHETER	43
VIL DU HA TILLIT, MÅ DU HA KONTROLL.....	44
KAN VI STOLE PÅ DINGSENE?	46
FOR DÅRLIG SIKKERHET I TINGENES INTERNETT	46
BRYR FOLK SEG OM SIKKERHETEN I DINGSER?	47
VEKSTEN I TINGENES INTERNETT ER AVHENGIG AV TILLIT	49
HVA MÅ TIL FOR AT VI KAN STOLE PÅ TINGENES INTERNETT?	50
FORBRUKEREN KAN IKKE STÅ ALENE.....	50
KINAS DIGITALE KJEMPER	52
ALT I ETT	52
ET MARKED UTEN PERSONVERNREGULERING.....	54
LAV TILLIT TIL UTENLANDSKE BETALINGSTJENESTER	56

TEKNOLOGITRENDER

Digitaliseringen berører livene våre på mange forskjellige måter. I årets rapport kartlegger vi hvordan teknologien kommer oss nærmere inn på livet overalt hvor vi ferdes, men også at den kan gjøre oss mer usynlige.

Den første trenden har vi med et nytt begrep kalt «emosjonell overvåkning». Kunstig intelligens og maskinlæring kan ikke bare brukes til å bli best i sjakk, men også til å skille et falskt smil fra et ekte, eller dårlig humør fra en depresjon. Når er det greit at det brukes? Vi har både spurt oss selv og et statistisk utvalg av nordmenn.

I 2018 blir det lov å prøve ut selvkjørende biler i Norge. Biler som er fullpakket med sensorer og intelligens vil sannsynligvis kartlegge oss og omverdenen i en helt annen grad enn før. Kan bildeling og smart kollektivtransport være et bedre alternativ – eller blir det en overvåkningsøkonomi på hjul?

Bitcoin og blokkjeder handler om anonymitet, sikre data og at mellommannen forsvinner. Det høres ut som oppskriften på godt personvern. Kan vi tro på hypen?

EMOSJONELL OVERVÅKING

Teknologi som brukes for å komme nærmere følelsene våre blir mer utbredt. Dette kan brukes til å bedre elevers læring eller forebygge depresjon. Men ønsker vi at datamaskiner har tilgang til følelseslivet vårt?

I mai 2017 fikk IT-ingeniøren Jeff Newman et glimt av fremtiden da han besøkte Peppes Pizza på Oslo S. På grunn av en feil i programvaren viste ikke den digitale reklameskjermen lenger fristende bilder av pizza, men en logg over hvem som hadde sett på skjermen: kjønn, alder, utseende og humør var blant kategoriene. Da han nærmet seg for å ta et bilde av dette, dukket en ny linje opp som beskrev ham selv: «male», «young adult», «glasses» og «smile: 0»¹.

Formålet med slike reklameskilt er å tilpasse innholdet bedre til personen som ser på. Hos Peppes Pizza ble menn vist bilder av pizza med biff, mens kvinner fikk se sunne salater.

Den nye emosjonelle overvåkingen gir datamaskinene innblikk i reaksjonene, humøret og følelsene våre. Da løgndetektoren ble oppfunnet i 1921, ble det mulig å måle noens følelser gjennom kompliserte tester og spesialutstyr. Nå kan målingene skje på avstand og uten at vi legger merke til det, for eksempel gjennom ansiktsuttrykk, tale, kroppens signaler og sosiale medier, og ved bruk av alminnelige webkameraer, mikrofoner og sensorer.

¹ Dette indikerte at han ikke smilte.

SLIK MÅLES FØLELSENE DINE

Til nå har utviklingen innen kunstig intelligens vært rettet mot å trene opp maskiner til å løse logiske oppgaver, som å spille sjakk eller stille medisinske diagnoser. Nye fremskritt gjør at maskiner nå også kan analysere følelsene dine:

- **Ansiktsgjenkjenning:** Utviklingen innen ansiktsgjenkjenning har gjort datamaskiner bedre på å fange opp og tolke ulike ansiktsuttrykk. I dag er for eksempel maskiner bedre enn mennesker på å skille et falskt smil fra et ekte.² Bedriften Affectiva utvikler teknologi som kan fange opp ulike følelser ved å fokusere på 33 punkter i ansiktet: sinne, forakt, vemmelse, frykt, overraskelse, tristhet og glede.³
- **Taleforståelse:** De siste årene har datamaskiner blitt langt bedre på å gjenkjenne og forstå tale, som har ført til at talestyrte assistenter som Siri og Alexa har blitt mer utbredt. Men assistene lytter kun til *hva* du sier, ikke *hvordan* du sier det. Dette er nå i endring. Ved å analysere blant annet stemmeleie og volum, kan datamaskiner også tolke følelsene dine mens du snakker.⁴
- **Sensorer på kroppen:** Treningsarmbånd og smartklokker samler kontinuerlig inn data om hvordan vi har det. Kroppsnær teknologi kan blant annet måle puls og bevegelse, og fuktighet og temperatur i huden. Mye av informasjonen en tradisjonell løgndetektor måler, kan nå registreres ved hjelp av et enkelt armbånd. Over tid kan analyser av kroppens signaler fortelle mye om hvordan en person har det.
- **Hva vi gjør på nettet:** Det meste vi gjør på nettet registreres og analyseres. Psykolog Michal Kosinski har vist hvordan folk kan analyseres i detalj kun ved hjelp av Facebook-aktiviteten deres. Han kom frem til at kun 10 likerklikk kunne si mer om en person enn den jevne kollega, og 300 likerklikk mer enn livspartneren⁵. Men det er ikke bare hva vi

² <http://news.mit.edu/2012/smile-detector-0525>

³ <https://developer.affectiva.com/metrics/>

⁴ <https://www.technologyreview.com/s/601654/amazon-working-on-making-alex-a-recognize-your-emotions/>

⁵ <https://nrkbeta.no/2017/02/04/dataene-som-snudde-verden-pa-hodet/>

liker som analyseres. Hvordan vi bruker sosiale medier og hva vi klikker på skjer ofte impulsivt. Dermed kan også underbevissthetsen vår måles og brukes for å få oss til å tilbringe mer tid på plattformen.⁶

HER BRUKES EMOSJONELL OVERVÅKING

Når et program eller en algoritme først er utviklet, kan den enkelt skaleres opp og tas i bruk for å omfatte mange mennesker. Mens hele 2% av befolkningen i Øst-Tyskland var ansatt i Stasi for å overvåke en befolkning på litt under 20 millioner, kan én algoritme hos Facebook følge med på følelsene til over 2 milliarder brukere.

De følgende eksemplene illustrerer hvor og hvordan følelsene våre overvåkes. Teknologien kan i mange tilfeller brukes til å hjelpe folk, for eksempel fange opp og forebygge depresjon, gi bedre tilpasset læring på skolen, eller bidra til at folk i kritiske situasjoner får hjelp i tide. Samtidig kommer den emosjonelle overvåkingen ofte tett innpå oss som privatpersoner. Dette kan skje uten at vi har gått med på det, og noen ganger med formål som er uklare.

I HELSETJENESTEN: FOREBYGGE DEPRESJON OG BEDRE NØDSAMTALER

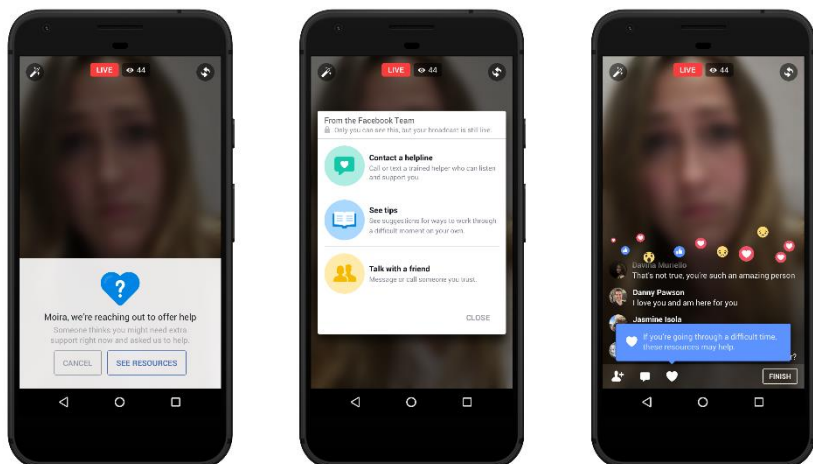
Forskningsprosjektet Intromat ved Haukeland universitetssykehus skal utvikle løsninger som kan bidra til forebygging, behandling og oppfølging av mentale lidelser. De utvikler en app som kan overvåke humørsvingninger hos personer med bipolar lidelse, og forutse depressive eller maniske episoder. Ved bruk av en smartklokke kan endringer i søvn, aktivitet, pulsvariasjon, og fuktighet og temperatur i huden måles. Appen kan i tillegg analysere tonefallet til brukeren under telefonsamtaler. Dersom symptomer oppdages, kan et varsel sendes til brukeren, familien og legen. Formålet er å fange opp symptomer i god tid før personen vanligvis ville ha oppsøkt hjelp selv, og dermed forebygge alvorlige tilbakefall.⁷

I Danmark brukes kunstig intelligens som beslutningsstøtte under samtaler på nødtelefonen. Programmet Corti analyserer hvilke ord og uttrykk som brukes, men også innringers stemmeleie, pustemønster og bakgrunnsstøy. På jakt etter

⁶ Galloway, S. (2017) The Four: The Hidden DNA of Amazon, Apple, Facebook and Google.

⁷ <http://intromat.no/cases/bipolardisorder/>

mønstre sammenlignes dataene med flere millioner andre nødsamtaler. Dette skal gi en raskere og mer presis vurdering av alvorlighetsgraden og hva som er galt. Formålet er at personer i kritiske og stressede situasjoner, og som kanskje har vanskelig for å formulere seg, skal kunne få hjelp raskere.⁸



Facebook Suicide Watch: En brukers direktestrøm har blitt flagget, og hun oppfordres til å søke hjelp (bilde: Facebook).

FORHINDRE SELVMORD

Ifølge Verdens helseorganisasjon er selvmord den nest største dødsårsaken globalt i aldersgruppen 15-29 år.⁹ Ved å følge med på brukeraktivitet kan Facebook Suicide Watch identifisere personer med selvmordstanker og oppfordre dem til å søke hjelp. Algoritmen skanner innlegg på jakt etter ord eller bilder som signaliserer at brukeren er i faresonen, og kommentarer som «trenger du hjelp?» og «går det bra?».¹⁰ Når et innlegg flagges av algoritmen varsles Facebooks empati-team, og brukeren kan sendes informasjon om psykisk helse og få tilbud om å kontakte en hjelpetelefon. I neste rekke kan venner og lokale ressursentre varsles.

En måned etter lansering erklært Facebook-direktør Mark Zuckerberg at algoritmen hadde hjulpet over 100 personer.¹¹ Men med funksjonen følger en rekke utfordringer, og brukerne har heller ikke mulighet til å velge den bort (opt-out).

⁸ <http://www.corti.ai/2650-2/howitworks/>

⁹ http://www.who.int/mental_health/prevention/suicide/suicideprevent/en/

¹⁰ <https://www.wired.com/2017/03/artificial-intelligence-learning-predict-prevent-suicide/>

¹¹ <https://www.weforum.org/agenda/2018/01/can-ai-algorithms-help-prevent-suicide/>

Facebook vil ikke ta i bruk denne teknologien i Europa, grunnet det de hevder er for strenge regler for personvern. I Teknologirådets undersøkelse oppgir 43 prosent at de er negative til at Facebook tar i bruk dette i Norge, mens 23 prosent er positive.

PÅ SKOLEBENKEN: LÆRING OG FØLELSER

Læring er tett knyttet opp mot følelser, som nysgjerrighet, fascinasjon, forvirring og frustrasjon. En god lærer vil oppdage slike tegn hos elevene, og følge dem opp på en god måte. Flere forsøker nå å integrere slike funksjoner i digitale læremidler. På plattformen Remote Laboratory har de for eksempel utviklet en maskinlærings-algoritme som kan fange opp ulike ansiktsuttrykk gjennom et webkamera, ved å spore 70 punkter i ansiktet.¹² Algoritmen kan måle grad av sinne, tristhet, overraskelse eller glede, som kan indikere om studenten har forstått et konsept eller har behov for hjelp.

Hong Kong-selskapet Find Solution har utviklet programmet 4 Little Trees, som analyserer elevers ansiktsuttrykk gjennom kameraet på et nettbrett.¹³ Programmet måler endringer i følelsene hos elevene mens de løser en oppgave, for eksempel i matematikk. Om eleven ser ut til å slite eller miste motivasjonen, dukker det opp en pop-up med lyder, animasjoner og hint. Analysene sendes også til læreren, som kan tilpasse undervisningen til den enkelte eleven. Om programmet erfarer at eleven ikke har det så bra, kan et mental helse-varsel sendes til foreldrene.

I en undersøkelse gjennomført av Teknologirådet spurte vi folk om hva de synes om ulike bruksområder for teknologi som analyserer følelsene dine. Et av spørsmålene dreide seg nettopp om digitale læringsprogrammer som ved hjelp av innebygget kamera i PC eller nettbrett kan registrere reaksjoner, humør og følelser mens en elev løser oppgaver. Resultatene viser at 24 prosent er positive til at dette tas i bruk for å bedre barns læring, mens 38 prosent er negative. Aldersgruppene 30-39 år og 40-49 år, de som mest sannsynlig kan ha barn i skolealder, var mest positive (hhv. 33 og 30 prosent).

PÅ KONTORET: VEILEDE ANSATTE

På kontoret kan stemmeanalyse brukes for å vurdere hvordan en ansatt utfører arbeidet sitt. Dette kan for eksempel gjelde for noen som jobber med salg eller

¹² Khalfallah, J. og Slama, J. B. H. (2015) «Facial expression recognition for intelligent tutoring systems in remote laboratories platform». *Procedia Computer Science* 73, s. 274-81.

¹³ <https://www.findsolutionai.com/4littletrees>

kundeservice. Basert på analysene kan programmet gi tilbakemeldinger og tips. I Teknologirådets undersøkelse spurte vi folk om hva de synes om at denne typen teknologi blir tatt i bruk for å gi bedre veiledning til ansatte. Resultatene viser at 23 prosent er positive og 42 prosent er negative til dette bruksfeltet.

TREFFSIKKER MARKEDSFØRING

Hvem du er og hva du gjør på Facebook bidrar til at du profileres. På denne måten kan reklameselskaper betale for akkurat din oppmerksomhet. I 2016 lanserte Facebook en funksjon som også gir selskapet bedre innsikt i følelsene dine. Dette var i form av seks animerte emoji'er: Liker, Kjærlighet, Haha, Wow, Trist og Sint. Med innsikt i følelsesreaksjonene dine på ulike typer innlegg kan Facebook skreddersy nyhetsstrømmen din slik at du vises mer innhold som engasjerer deg, noe som kan bidra til at du tilbringer mer tid på Facebook. Du kan også få se mer treffsikker reklame, og annonsørene kan få mer informasjon om dine reaksjoner.¹⁴

Facebooks patentsøknader kan gi en indikasjon på selskapets fremtidige planer. De fikk nylig innvilget patent på en funksjon som kan lese ansiktsuttrykket ditt gjennom kameraet på PC-en eller telefonen din mens du bruker plattformen, og tilpasse innholdet du vises til reaksjonene og humøret ditt. Et annet patent kan forutsi og tilføre emosjonell kontekst til meldingene dine, som skriftstørrelse og -type, blant annet basert på hvor fort du skriver og hvor hardt du trykker på skjermen.¹⁵

Facebook eksperimenterte med brukernes humør

I 2014 kom det frem at Facebook hadde manipulert nyhetsstrømmen til flere hundre tusen brukere ved å fjerne alt positivt eller alt negativt innhold, for å se hvordan det påvirket humøret deres. Det viste seg at brukerne som ble utsatt for negativitet la ut mer negativt innhold selv, mens det motsatte skjedde med de som ble vist positivt innhold.¹⁶ Et lekket dokument fra 2017 avslørte også at Facebook kategoriserte tenåringer som følte seg verdiløse eller usikre. Selskapet benektet imidlertid at dataene ble brukt til markedsføringsformål.¹⁷

¹⁴ <https://www.forbes.com/sites/amitchowdhry/2016/02/29/facebook-reactions/#24722e451a62>

¹⁵ <https://www.forbes.com/sites/curtissilver/2017/06/08/how-facebook-wants-to-capture-your-emotions-facial-expressions-and-mood/amp/>

¹⁶ <https://www.theguardian.com/technology/2014/jun/29/facebook-users-emotions-news-feeds>

¹⁷ <https://arstechnica.com/information-technology/2017/05/facebook-helped-advertisers-target-teens-who-feel-worthless/>

REKLAMESKILT SOM VURDERER DEG

Reklameskiltet for Peppes Pizza som ble beskrevet innledningsvis stammer fra det amerikanske selskapet Kairos, som spesialiserte seg på ansiktsgjenkjenning innen varehandel. Den irske bedriften Orb Screen tilbyr tilsvarende skilt, og kan tilpasse reklamer basert på følgende kriterier: antall personer som ser på, hvor lenge de ser på, alder, kjønn, ansiktstrekk (som skjegg eller briller) og humør.

I vår undersøkelse spurte vi folk om hva de synes om at reklameskilt på gaten bruker kameraer for å tilpasse innholdet til deg, dersom dette gjør at du får mer relevant informasjon. Hele 68 prosent var negative til denne teknologien, mens kun 10 prosent var positivt innstilt. Den yngste aldersgruppen (18-29 år) var mindre negativ enn snittet, hvor 17 prosent av de yngste oppga å være positive.

POLITISK PÅVIRKNING

Cambridge Analytica har blitt kjent for sin rolle i Donald Trumps valgkampanje og «Leave.EU»-bevegelsen i Storbritannia. Firmaet baserer sin markedsføring på psykologiske modeller, stordataanalyse og persontilpassede annonser.

Like før det amerikanske valget i 2016 erklærte firmaets konsernsjef at de hadde profilert personligheten til alle USAs velgere — 220 millioner mennesker¹⁸. De hadde knyttet folks digitale fotspor opp mot en psykologisk modell som kan gi en relativt nøyaktig profil av personligheten din og hvordan du trolig vil oppføre deg. Tusenvis av datapunkter om alt fra handlevaner, klubbmedlemskap og avisabonnementer, til hva du liker og deler på Facebook, ble i kombinasjon omgjort til personers følelser, bekymringer og behov.

Profilene ble brukt for å skreddersy politiske budskap til enkeltpersoner. For eksempel kunne velgere med høy score på nevrotisme og planmessighet vises annonser med budskap om innbrudd i hjemmet og våpeneierskap som trygghetstiltak, med bilde av en innbruddstyv i det han knuser et vindu¹⁹. Mer introverte velgere kunne vises et bilde av far og sønn på andejakt, med budskap om tradisjon og familieverdier. Dørbankere tok også i bruk en app som oppga hvem som kunne være mottakelige for Trumps budskap, personlighetsprofilene til beboerne, og retningslinjer for hvordan samtalen skulle føres.

¹⁸ <https://www.youtube.com/watch?v=6bG5ps5KdDo>

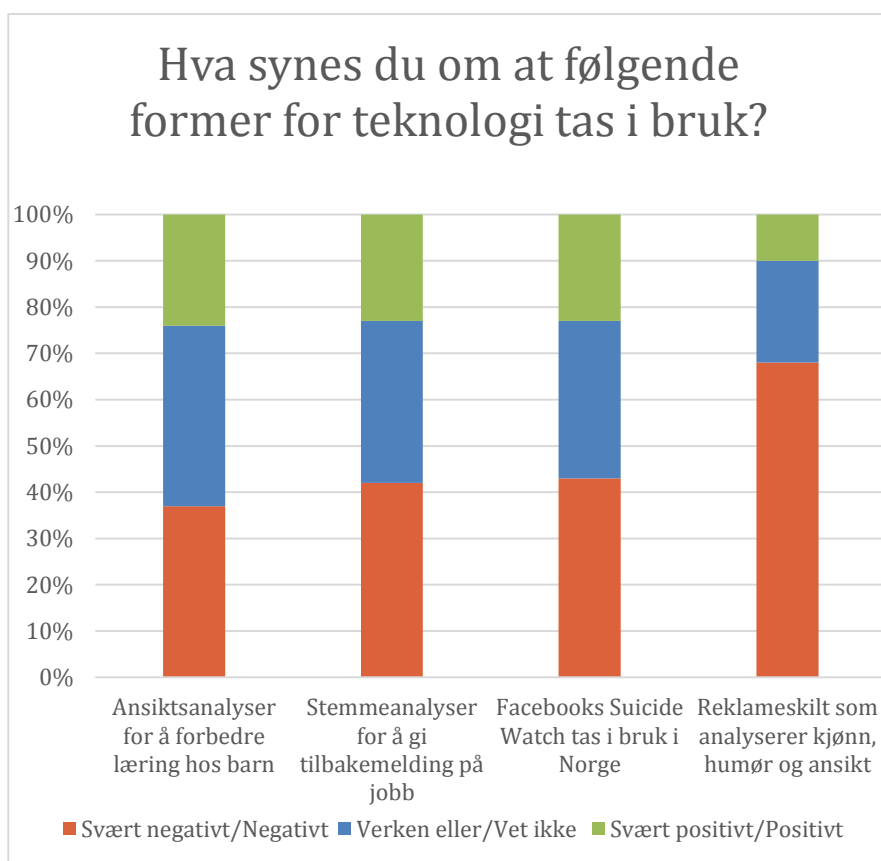
¹⁹ <https://nrkbeta.no/2017/02/04/dataene-som-snudde-verden-pa-hodet/>

Clinton-kampanjen kombinerte også store data og målrettet annonsering, men skal ha vært mer orientert rundt demografi og meningsmålinger. Dermed tilførte den psykologiske profileringen et ekstra lag til Trump-leirens analyser²⁰. I hvor stor grad dette ga utslag på valgresultatet er imidlertid omstridt.

²⁰ <https://www.ft.com/content/bee3298c-e304-11e6-9645-c9357a75844a>

HVA SYNES FOLK?

I januar 2018 gjennomførte Teknologirådet en undersøkelse der vi spurte folk om hva de synes om fire ulike bruksområder for teknologi som samler inn og analyserer data om følelsene våre²¹. Resultatene viser at folk er mer negative enn positive til emosjonell overvåking. Allikevel er det ikke helt entydig: 23-24 prosent er positive til tiltak som har et uttrykt formål om å hjelpe, ved å forbedre elevers læring, veilede ansatte eller forhindre selvmord. Utvalget vi spurte er tydelig skeptisk til reklameskilt som analyserer hvem du er: 68 prosent er negative til denne bruken, mens kun 10 prosent er positive.



²¹ Undersøkelsen ble gjennomført av Norstat i januar 2018. 1017 respondenter i et landsrepresentativt webpanel har besvart undersøkelsen.

Kan en datamaskin avsløre seksuell legning?

En studie fra Stanford på om homofile har spesielle ansiktstrekk fikk mye oppmerksomhet høsten 2017. Ved hjelp av kunstig intelligens kunne forskerne med 70-90 prosent sikkerhet identifiserer hvilket ansikt som tilhørte en homofil person, hvis valget stod mellom ansiktet til én heterofil og én homofil person. For mennesker som gjorde det samme, lå treffsikkerheten rundt 55-60 prosent.

Ved å hente bilder av 36,630 menn og 38,593 kvinner fra nettdatingsider hvor brukerne selv hadde skrevet hvilket kjønn de var interessert i, trente de et nevralt nettverk til å finne en matematisk sammenheng mellom seksuell legning og ansiktstrekk. Modellen fant 500 variabler, som blant annet kunne måle at homofile menn hadde større panner og smalere kjever, mens homofile kvinner hadde smalere panner og større kjever.²²

Studien har i ettertid blitt kritisert for unøyaktighet, så vel som etisk uforsvarlighet.

Det har blant annet blitt bemerket at forskjellene i ansiktsform kan ha blitt plukket opp fra måten bildene er tatt på: om pannen er lent mot eller fra kameralinsen, eller hvordan ansiktstrykket er i det man tar bildet. Et annet poeng er at algoritmen kun fungerer når den må velge mellom to bilder som er satt opp mot hverandre, hvor den fra før av vet at en person er heterofil og den andre homofil. Den har ingen betydelig presisjon hvis den skal plukke ut fra et større utvalg.²³

Gitt de riktige kriteriene er likefullt datamaskinene bedre enn mennesker til denne typen bildeanalyser. Dersom forskningen gjør ytterligere fremskritt, kan det være dårlig nytt både for retten til privatliv og for personer i land hvor homofile forfølges.

KUNSTIG INTELLIGENS MØTER EKTE FØLELSER

Kunstig intelligens har fått en vårløsning. De siste års diskusjoner har stort sett dreid seg om at maskiner nå kan løse kompliserte logiske oppgaver bedre enn oss, mens sosiale relasjoner og følelser er områder fortsatt forbeholdt mennesker. Det som diskuteres mindre er, som vi har vist her, at teknologien også kan brukes til å få bedre innsikt i følelseslivene våre.

Følelsesanalyser ved bruk av kunstig intelligens kan fungere som et verktøy innen psykisk helse, i nødsamtaler og i skolen. Det kan også brukes for å avsløre private følelser og løgner, og for å påvirke oss til å kjøpe produkter eller politiske budskap.

²² <https://www.economist.com/news/science-and-technology/21728614-machines-read-faces-are-coming-advances-ai-are-used-spot-signs>

²³ <https://theoutline.com/post/2248/how-to-navigate-the-coming-a-i-hypestorm>

Et viktig skille er at det nå er lettere å observere folk på avstand, uten at de vet om det. Store aktører er ute etter informasjon om deg som du ikke ønsker å vise, eller kanskje ikke engang er klar over selv. Denne utviklingen vil trolig skyte fart fremover, etter hvert som vi utstyres oss med flere sensorer i det daglige og genererer mer personlige data.

Den emosjonelle overvåkingen medfører en rekke viktige spørsmål for personvernet:

- **Er det bevisst og frivillig?** Om følelsene dine analyseres uten at du er klar over det, kan du heller ikke samtykke. For at aktører skal kunne bruke data om følelsene dine for å profilere deg bør det være et aktivt samtykke, og mulighet for å velge det bort (opt-out). Selv i tilfeller hvor informasjonen ikke lagres eller selges til tredjeparter, kan det oppleves ubehagelig å bli kategorisert basert på utseende og emosjoner.
- **Hva er formålet?** Emosjonell overvåking kan brukes for å hjelpe oss, for eksempel i kritiske helsesituasjoner. Men de samme dataene har også stor påvirkningsverdi, og kan brukes til kommersielle og politiske formål uten at du har gitt fra deg informasjonen bevisst eller til det formålet. Da er det særlig problematisk om personen profileres som å være i en sårbar livssituasjon.
- **Hvem vil vi ha hjelp fra?** Facebook har tilgang til enorme mengder data om oss. Dersom informasjonen de sitter på kan redde liv, kan man argumentere for at det er bedre at de griper inn enn at de unnlater å gjøre noe. Samtidig er det en uheldig rolleblanding om de samme dataene som brukes til å redde liv, også brukes til målrettet markedsføring. Dette forsterker et allerede skjevt maktforhold mellom brukere og plattformer.

FREMTIDENS TRANSPORT: SELVKJØRENDE, SMART OG SPORBAR

Smarttelefonen er for mange viktigere enn bilnøkkelen for å komme seg fra A til B. Selvkjørende biler er på vei, og måten vi organiserer transport er i ferd med å endres. Vil dette også medføre at alle våre reiser vil spores?

REISEN BLIR DIGITAL

Vi har lenge kunnet være gjerrige på informasjon når vi har vært på reise, og vi har hatt frihet til å velge anonyme alternativer. Bilen har gitt oss mulighet til å bevege oss fritt i et land preget av store avstander, og har for mange vært et frihetssymbol.

Nye utfordringer gjør at vi må tenke nytt om hvordan vi reiser: Økende lokal forurensing og økt befolkning har gjort at Stortinget har erklært et mål om at de største byene ikke skal ha vekst i personbiltransport frem mot 2030. Målet innebærer at veksten i persontransporten i byområdene skal tas med kollektivtransport, sykkel og gange. I tillegg til at trafikken skal bli mer miljøvennlig, skal den også bli digitalisert. Vil det da bli mulig å ferdes anonymt?

Elbilveksten i Norge har vært et stort steg for miljøutfordringer, men den gir ikke færre biler på veiene. Vi ser nå to teknologiske trender som kan bidra til å løse utfordringer knyttet til fremtidens transport, men de kan også bidra til at vi blir mer sporbare:

- **Selvkjørende biler:** Fra i år blir det lov å teste selvkjørende biler på norske veier. Teknologiselskaper som Tesla og Google er lengst fremme i utviklingen. Google-selskapet Waymo lanserer taxitjeneste i Arizona, og Tesla lover at dagens biler skal kunne oppgraderes til å bli fullstendig selvkjørende. For å kunne sanse like godt som eller bedre enn et menneske, må en bil utstyres med sensorer og kameraer. Dette gjør at den vil samle inn informasjon, både om omgivelsene og passasjerene.
- **Deling og digitalisering:** Vi har allerede sett en endring i hvordan folk koordinerer seg i forbindelse med reiser. De siste årene har selskaper som Uber og Lyft vært med på å utfordre etablerte forretningsmodeller ved å koordinere tilbud og etterspørsel direkte mellom enkeltpersoner. Nå ser vi flere nye forretningsmodeller komme til: Mobilitet som tjeneste innebærer at alle transporttjenester kan koordineres på én plattform, slik at samme app brukes til buss, tog, t-bane, sykkel og taxi. Slike plattformer vil trenge mye data for å kunne tilby persontilpassede tjenester.

Bilene blir en del av tingenes internett og vil etterspørre data fra brukerne for å levere personlig og sømløs transport. Personvernet for fremtidens transport er med andre ord i støpeskjeen.

SELVKJØRENDE BILER: DATAMASKINER PÅ HJUL

I 2004 utlyste det amerikanske forsvaret The DARPA Grand Challenge: en konkurranse om å lage en selvkjørende bil som kunne kjøre en 240 kilometer lang løype i ørkenen. Vinneren kom bare 12 kilometer før den kjørte i en sanddyne. Siden den gang har utviklingen av selvkjørende biler skutt fart. Waymo (tidligere Google) sine selvkjørende testbiler har nå tilbakelagt omlag 6,4 millioner kilometer i amerikanske byer, og biler med autopilot er allerede på markedet. Store teknologiske fremskritt de siste årene har ført til at massiv datakraft og sofistikerte sensorer nå kan integreres i en bil.

I november 2017 startet også Waymo å teste sine selvkjørende biler uten å ha en sikkerhetssjåfør bak rattet, i vanlig trafikk i en forstad utenfor Phoenix i Arizona. De vil nå gradvis utvide til å tilby en kommersiell taxitjeneste i hele byområdet.²⁴ Flere av de største selskapene jobber også med dette, og noe av det interessante her er at teknologiselskaper, slik som Waymo, Tesla og Baidu, leder an. De tradisjonelle bilselskapene som BMW, Ford og Mercedes er hakk i hæl, og sier at de vil ha selvkjørende biler på markedet i 2021, men da som en del av en transporttjeneste.

Den selvkjørende bilen lover oss først og fremst en sikrere transport: Over 90 prosent av dagens bilulykker skyldes menneskelige feil, og selvkjørende biler kan bidra til en reduksjon i ulykker dersom de innføres på en forsvarlig måte. Selvkjørende biler kan dessuten gjøre bilkjøring tilgjengelig for flere, ikke bare de som har førerkort.

Flere land har allerede endret lovverket for å kunne tillate testing av selvkjørende biler. I Norge trådte lovendringen i kraft i 2018, og de største transport-selskapene, som Ruter og Kolumbus, har planer om å teste selvkjørende busser på veiene det kommende året.²⁵

HVORDAN FUNGERER DEN?

En selvkjørende bil bruker sensorer til å gjøre en rekke oppgaver som mennesker må gjøre i dag:

- **Sanse:** Sensorer og kameraer registrerer alt som foregår rundt bilen. LiDAR er en type laserscanner som gir detaljert informasjon om avstand til ulike objekter. Signaler fra alle de forskjellige sensorene kombineres for å fungere best mulig under alle værforhold.
- **Vite hvor den er:** Kart, GPS og bevegelsessensorer brukes for at bilen skal vite hvor den befinner seg.
- **Ta beslutninger i trafikken:** Programvare og kunstig intelligens brukes for å kjenne igjen objekter, ta beslutninger i trafikken og manøvrere trygt fra A til B.

²⁴ <https://waymo.com/journey/>

²⁵ <https://e24.no/bil/trafikk/se-planene-i-disse-byene-kan-foererloese-busser-komme-foerst/24149182>



Bilde: Waymo

1. **LiDAR** bruker lasermåling for å lage et detaljert bilde av omgivelsene.
2. **Kamera og bildegjenkjenning** identifiserer skilt og objekter i veibanen.
3. **Radar** ser objekter i bevegelse, og fungerer i all slags vær.
4. **Ekstra sensorer** rundt bilen brukes for å unngå blindsoner.
5. **GPS** angir posisjon. De fleste biler har også backup-systemer i tilfelle signalet faller ut.
6. **Kraftige datamaskiner og kunstig intelligens** tolker signaler fra sensorene og tar beslutninger i trafikken.

HVILKEN INFORMASJON SAMLER EN SELVKJØRENDE BIL INN?

Ved å lagre all kartinformasjon lokalt kan en selvkjørende bil i prinsippet fungere fullstendig offline, uten å sende eller ta imot signaler fra omverdenen som sier hvor den befinner seg. Waymo-bilene kommuniserer ikke med omverdenen for å navigere, blant annet for å sikre seg mot hacking.²⁶ Likevel er det sannsynlig at en bestillingstjeneste vil lagre data om hvor folk reiser til og fra.

Det kan være et viktig prinsipp å skille mellom hvilke data som er nødvendig å samle inn for at reisen skal være trygg, versus informasjon som kan være verdifull å selge til tredjeparter. I tillegg kan man skille mellom informasjon bilen

²⁶ <https://www.ft.com/content/8eff8fbe-d6fo-11e6-944b-e7eb37a6aa8e>

samler inn om omgivelsene og hvilken informasjon som samles inn om passasjerer:

- **Data fra omverdenen:** En selvkjørende bil må bruke kamera for å orientere seg. Ved ulykker må mye av denne informasjonen lagres, dersom det blir en forsikringssak eller etterforskning. I loven om utprøving av selvkjørende kjøretøy blir ikke bildene fra kameraene regnet som «vedvarende overvåking», og dermed heller ikke omfattet av reglene om overvåking i personopplysningsloven. Imidlertid kan et kamera på en buss eller bil som går i fast rute regnes som overvåking.²⁷ I Kina nektes utenlandske bedrifter å teste og utvikle selvkjørende biler, i frykt for at detaljert kartlegging og fotografering kan brukes til spionasje.²⁸
- **Data om passasjerene:** I følge Gartner kan 30% av forbrukerinteraksjon med teknologi i 2018 skje via en taleassistert plattform, slik som for eksempel Amazons Alexa.²⁹ Kanskje vil passasjerer ønske å ha denne typen lyttende assistenter integrert i bilene? I den vedtatte utprøvningsloven er det spesifisert at lydopptak ikke vil være lov inne i kjøretøyet, med mindre det er søkt om og alle som er med på lydopptaket har gitt skriftlig samtykke.³⁰

²⁷<https://www.regjeringen.no/contentassets/ba61cdboa68f4325a5d8309f284897d2/no/pdfs/prp201620170152000dddpdfs.pdf>

²⁸ <https://www.ft.com/content/2ba4366c-e08c-11e7-a8a4-0a1e63a52f9c>

²⁹ <https://su.org/tech-scouting-august/>

³⁰ <https://www.stortinget.no/globalassets/pdf/innstillinger/stortinget/2017-2018/inns-201718-032l.pdf> (§12, s. 4)

Tesla: Allerede 75 000 kameraer på norske veier

Tesla-modeller solgt fra høsten 2016 skal kunne oppgraderes til å få autopilot via en programvareoppdatering. For å kunne levere dette er bilene utstyrt med 8 kameraer, en rekke sensorer og en kraftig datamaskin. Et av kameraene er inni bilen, mens de syv andre er utenpå og filmer i alle retninger.³¹

I mai 2017 oppdaterte Tesla brukervilkårene sine, slik at de kan samle inn korte videosnutter fra kameraene for å trene opp programvaren til å gjenkjenne veistriper, skilt og for å utvikle autopilot-funksjonen. Selskapet presiserer at videosnittene ikke vil være knyttet til bilens identifikasjonsnummer og at det ikke vil være mulig å søke opp videoer knyttet til en spesifikk bil.³²

Det finnes i dag rundt 10 704 slike Tesla-modeller i Norge. Det vil si at det allerede finnes 74 928 Tesla-kameraer på norske veier.³³



Tesla-kameraet: Dette er bildene som de ulike kameraene på Tesla samler inn. Kameraene sender tilbake sorthvitt-bilder. De kan sende høydefinerte bilder i farger, men sorthvitt går raskere å prosessere.³⁴

³¹ <https://www.tesla.com/autopilot>

³² <https://electrek.co/2017/05/16/tesla-autopilot-2-0-can-see/>

³³ <http://teslastats.no/>

³⁴ <https://electrek.co/2017/05/16/tesla-autopilot-2-0-can-see/>

EN STRØMMETJENESTE FOR TRANSPORT

Mobilitet som tjeneste (eng. Mobility as a Service, eller MaaS) er et konsept som går ut på at transport kjøpes som en tjeneste, heller enn at man eier et transportmiddel. Sammen med selvkjørende biler og mobiltelefonen kan digital koordinering gjøre at det blir enklere og mer praktisk å komme seg dit man skal uten å eie en bil.

I et slikt scenario forsvinner mye av behovet for parkering, og areal kan frigjøres til for eksempel fotgjengere, parker eller nybygg. Men denne typen endring vil også kreve at folk er villig til å gi slipp på noen av fordelene bileierskap gir. Folk vil være nødt til å legge om sine transportvaner og dele biler med andre.

Helsingfors har satt et mål om at ingen innbyggere skal behøve å eie en bil innen 2025.³⁵ For å nå dette målet satser de på å legge om til at man skal kunne få dekket alle sine transportbehov gjennom mobiltelefonen. Dette vil være en slags strømmetjeneste for transport som kan ligne på Netflix eller Spotify.

Mobilitet som tjeneste er allerede tilgjengelig på markedet i Finland, og folk kan abonnere på transporttilbud tilpasset sine behov. Transportmyndighetene der har lagt om hvordan data utveksles mellom privatpersoner, tjenestetilbyder og det offentlige for å kunne legge til rette for digitale mobilitetsløsninger.³⁶

MAAS OM INFORMASJON

Ved bruk av mobilitet som tjeneste vil det være behov for betydelig utveksling av informasjon mellom forskjellige aktører for å kunne fordele inntektene fra reisene og abonnementene.

Et annet behov for informasjon vil oppstå når reisetilbudet skal tilpasses den enkelte. For å fungere som en personlig reiseassistent, kan denne typen tjenester be om for eksempel data fra kalenderen din, slik at den kan planlegge reisen din før du har tenkt på det selv. Enkelte av funksjonene kan også kreve at tjenesten vet hvor du befinner deg til enhver tid, også når du ikke bruker den.

³⁵ <http://www.helsinkitimes.fi/finland-news/domestic/11062-the-future-resident-of-helsinki-will-not-own-a-car.html>

³⁶ <https://www.lvm.fi/en/mobility-as-a-service>

I Norge har kollektivselskapet Ruter planer om å lansere mer personlige transportprodukter. I et strategidokument foreslår de å lage en mobilitetsassistent som snakker med kalenderen din og er koordinert med vennene dine på Facebook, slik at du kan tilbys samkjøringstjenester.³⁷

Uber sporet brukere – også etter fullførte reiser

Frem til november i fjor lagret Uber informasjon om hvor brukerne befant seg i fem minutter etter at reisen hadde endt. For å kunne bestille reiser mest mulig lettvin, krevde tjenesten tilgang til hvor brukerne befant seg til enhver tid. Kravet om at såkalte stedstjenester skulle være skrudd på til enhver tid ble tatt bort etter at det kom frem at ansatte hos Uber hadde misbrukt systemet til å spionere på eks-kjærester og andre bekjente.³⁸

I en bloggpost i 2012 la de ut statistikk som viste hvordan de kunne analysere hva kunden hadde gjort basert på reisemønstre. Blant annet kunne de vise statistikk over hvor mange kunder som sannsynligvis hadde brukt Uber i forbindelse med en one-night-stand.³⁹

³⁷ <http://m2016.ruter.no/teknologi-og-tjenester-moter-kundebehov/>

³⁸ <https://techcrunch.com/2017/08/29/uber-to-end-controversial-post-trip-tracking-as-part-of-privacy-drive/>

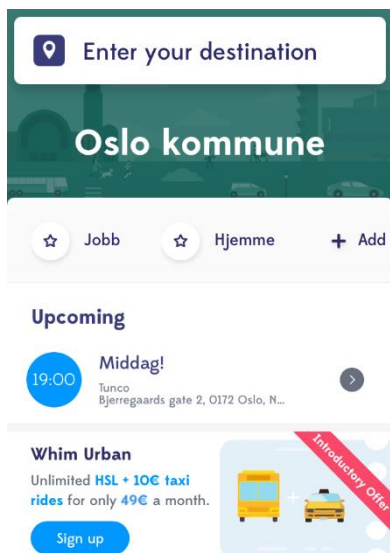
³⁹ <https://gigaom.com/2012/03/26/uber-one-night-stands/>

DENNE INFORMASJONEN VIL WHIM HA

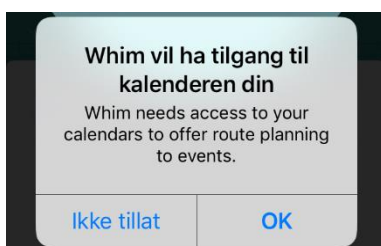
Travel data. We store information about your trips. This includes the start and end points of the trip, the start and end times of the trip, the method of travel, and the cost. This information is associated with your unique user identifier. This information is vital for the functioning of the service, as it allows us to provide the service and to ensure the trip provider is compensated for the trip.

13. Advertisements

The Service may include advertisements. Advertisements may be targeted on the basis of the queries you have made through the Service, or on the basis of other information you have provided.



It is also possible that we are able to further simplify your life by providing you with personalised marketing or recommendations, unless you let us know that you do not wish to receive such marketing. If you explicitly agree, by opt-in consent, it is also possible that your data is used for the purpose of providing you with offers from our partners that suit you and your needs.



We need your permission

☐ Location

Whim uses your current location for route planning and for booking taxis and cars. Whim works best if it has access to your location.

☐ Notifications

We use background push notifications to issue tickets quickly and to update bookings in real-time. We will never spam you.

Brukervilkår: Bildene over stammer fra den finske mobilitets-appen Whim. Ved å gi tilgang til kalenderen din, planlegger applikasjonen din neste reise før du har tenkt på det selv. Du kan også gå med på at informasjon om reisene dine brukes til å gi reklame eller persontilpassede reisetilbud.

SKAL VI HA OVERVÅKNINGSØKONOMIEN MED I BAGASJEN?

Vi står foran store endringer for transportsektoren. Ikke bare er bilparken i ferd med å bli elektrisk, den kan også bli både selvkjørende og delt. Men digitaliseringen åpner for at informasjon om hvor vi beveger oss kan samles inn enklere. På internett har vi i praksis gått med på en forretningsmodell hvor våre persondata har blitt en valuta som kan kjøpes og selges.⁴⁰ Skal vi ta med oss overvåkingsøkonomien også når vi reiser?

Selvkjørende biler blir en del av tingenes internett. Fra å etterlate oss spor punktvis, som når vi passerer en bomstasjon, kan det trekkes en kontinuerlig linje etter oss. Men det trenger ikke å bli slik: I prinsippet skal en selvkjørende bil kunne manøvrere sikkert uten å være på nett.

Mobilitet som tjeneste kan for mange erstatte behovet for å eie en egen bil. Ved å ha alle transportalternativer tilgjengelig på telefonen, kan kollektivtransport integreres med mer personlige tilbud. Trolig vil også selvkjørende biler bli et av alternativene man kan velge. For å utvikle produkter som er best mulig tilrettelagt for en persons liv, kan det imidlertid være nødvendig å vite mye om brukeren.

I samarbeid med Datatilsynet har kollektivselskaper utarbeidet en bransjenorm som skal sikre muligheten til å reise anonymt selv om billettene er elektroniske.⁴¹ Men for å ta med muligheten til å reise anonymt inn i fremtiden, er transportaktørene nødt til å legge til rette for det. For eksempel bør det være mulig å opprette en profil som ikke tilknyttes brukerens identitet, uten at det medfører et vesentlig dårligere transporttilbud.

Kun data som er nødvendige for å levere en sikker og effektiv transporttjeneste bør samles inn, og de bør kun benyttes til å levere tjenesten. Mobilitets-apper som Whim peker mot en utvikling hvor informasjon om reisene dine kobles sammen med markedsføring. Dette bør i så fall kun skje når brukeren tydelig velger det selv.

⁴⁰ <https://teknologiradet.no/sikkerhet-og-personvern/hva-er-overvakingsokonomien/>

⁴¹ <https://www.datatilsynet.no/regelverk-og-skjema/lover-og-regler/bransjenormer/bransjenorm-e-billettering/>

BLOKKJEDEN OG PERSONVERNET

Bitcoin har fått mange millioner brukere de siste årene. Teknologien bak denne kryptovalutaen heter blokkjeden og endrer fundamentalt hvordan vi lagrer og utveksler data. Kan den også fikse personvernet?

Det europeiske personvernbarometeret viser at hele to tredjedeler av innbyggerne er bekymret over at de ikke har full kontroll over informasjonen de oppgir på nett. Den største frykten er muligheten for å bli utsatt for svindel.⁴² Det er en kjensgjerning at store databaser med personsensitive data er utsatt for hacking, slik tilfellet var for kredittinformasjonsselskapet Equifax i 2017.

Samtidig er det å kunne dele data og gjøre transaksjoner nødvendig for økonomien, og innovativ bruk av data fra innbyggerne kan fornye mange velferdstjenester. Folks tillit til systemet og til de offentlige virksomhetene som forvalter, drifter og utvikler det, vil være avgjørende. For å sikre denne tilliten, er det flere utfordringer som må håndteres godt:

- Sikker håndtering av data som er samlet inn
- Mulighet til å være anonym
- Kontroll med digitale spor

⁴² http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf

- Trygg utveksling av data

Blockkjeden er en ny teknologi som i prinsippet kan adressere alle disse utfordringene. Skal vi tro på hypen?

HVA ER BLOKKJEDER?

Bitcoin er en digital valuta og betalingssystem som ble introdusert av Satoshi Nakamoto i 2009, og har i dag flere millioner unike brukere over hele verden. Satoshi Nakamoto er et pseudonym og identiteten er ukjent.

Teknologien som Bitcoin baserer seg på kalles *blockchain*, eller på norsk *blokkjede*. Bitcoins blokkjede gjør det mulig for parter som ikke nødvendigvis kjenner hverandre å dele informasjon eller handle direkte med hverandre uten å bruke betrodde tredjeparter som banker.

Det finnes flere varianter av blokkjeder, og de kan brukes på andre områder enn kryptovaluta. Overordnet kan en blokkjede forstås som en digitalisert og delt regnskapsbok som holder oversikt over hendelser. En blokkjede kan potensielt løse en rekke oppgaver, både i privat og offentlig sektor, sikrere og mer effektivt enn dagens løsninger.

Et lovende bruksområde er såkalte smarte kontrakter. I dag er det vanlig at betrodde tredjeparter holder orden på transaksjoner og sikrer at begge parter får det de skal ha. For eksempel brukes ofte en eiendomsmegler for å sikre at selgeren får pengene før huset overføres til ny eier, at kjøper får overført huset til seg når de har betalt pengene, og at salget blir tinglyst i grunnboken. Kjøpet er ikke endelig før alle prosessene er gjort.

Dette er både kostbart og tidkrevende. En blokkjede vil kunne gjøre prosessen mye raskere, og samtidig sikre at ingen av partene får sin del før alle prosessene er utført. Hvis det skjer noe underveis, for eksempel at kjøper ikke får lån og pengene ikke blir utbetalt likevel, kanselleres hele transaksjonen. Dette prøves nå ut i Sverige.⁴³

⁴³ <https://www.lantmateriet.se/contentassets/6874bc3048ab42d6955e0f5dd9a84dcf/blockkedjan-framtidens-huskop.pdf> /

SIKKER HÅNDTERING AV DATA

Det har vist seg vanskelig for databehandlerne å gi dataene nødvendig beskyttelse. Tjenesteleverandørene risikerer store bøter i EU dersom de ikke makter å beskytte kundenes data godt nok, men kan vi likevel stole på at dataene blir ivaretatt på en ordentlig måte og ikke kommer på avveie?

Følgende mekanismer i blokkjeden gjør at det er umulig å endre på innsamlede data når de først er blitt lagt til:

- **Kryptering:** Blokkjeden bygger på etablerte prinsipper for kryptografi. Hver transaksjon krypteres, signeres, lagres fortløpende og samles i en blokk. Flere blokker danner til sammen en kjede, derav navnet.
- **Permanente kjeder:** Hver ny blokk lagres sammen med et «regnestykke» med informasjon fra den forrige blokken. Hvis noen prøver å endre innholdet, vil det oppdages av de neste blokkene fordi «regnestykket» da ikke går opp.
- **Delvis gjennomiktig:** Transaksjonene som skjer i blokkjeden er synlige for alle i systemet. Det gjelder imidlertid ikke selve innholdet, som er kryptert.
- **Distribuert lagring:** En fullstendig kopi av hele blokkjeden befinner seg på flere maskiner. Det betyr at det er mange som beskytter dataene.
- **Regler om konsensus:** Konsensusmekanismen er et sett med regler nettverket bruker for å kontrollere hver transaksjon og for å oppnå enighet om hvilken blokk-versjon som er gyldig. Såkalte bokførere konkurrerer om å føre inn én og én blokk i blokkjeden. Bokførerne må bevise at alle transaksjonene er gyldige og at for eksempel de samme pengene ikke kan brukes flere ganger (*double spending*). Mekanismene sikrer også at ingen bevisst kan hindre noen fra å utføre tjenester (*denial of service*).

Til sammen gjør alle disse elementene blokkjeden til en elegant og robust løsning for sikker håndtering av data om oss. Dette har sammenheng med at teknologien i utgangspunktet er utviklet for å håndtere kryptovalutaen Bitcoin.

Spørsmålet er om dette vil fungere i praksis også på andre områder. For eksempel tar det i gjennomsnitt 10 minutter å godkjenne en Bitcoin-blokk og føre den inn i blokkjeden. Dette vil være et problem når store systemer skal basere seg på blokkjeden, fordi løsningen kan skalere dårlig og bruker mye energi.

Det har derfor blitt utviklet blandingsmodeller som bruker elementer fra Bitcoins blokkjede, og bygger på med egne elementer slik at de kan skalere bedre og bli bedre tilpasset andre bruksområder. Noen slike alternativer er Ethereum, Ripple, Litecoin og IOTA.⁴⁴

ANONYMITET OG PSEUDONYMITET

Hvis vi kan opptre anonymt legger vi ikke igjen digitale spor som kan kobles til vår identitet. Blokkjeden fjerner behovet for å kjenne til identiteten til den andre parten for å kunne samhandle med den. Transaksjoner skjer ved å oppgi egen og den andres adresser i blokkjeden, og foregår dermed uten å referere til noens identitet.

Anonymitet og pseudonymitet kan være viktige verktøy for personvernet. Hvis en transaksjon ikke kan spores tilbake til de involverte individene, berøres heller ikke deres behov for personvern.

Det er imidlertid uenighet om hvorvidt brukerne av Bitcoin er anonyme eller pseudonyme. Bitcoin er ikke anonymt på samme måte som kontanter. Alle transaksjoner loggføres og man er avhengig av å ha en konto. Kontoen fungerer som et pseudonym som kan knyttes til ulike Bitcoin-transaksjoner. Det er med andre ord vanskelig, men ikke umulig, å finne identiteten bak en adresse på blokkjeden.

Det er her risiko for re-identifisering kommer inn. Nettbanker som håndterer en Bitcoin-konto kan lagre brukerinformasjon om IP-adresse, operativsystem og type mobiltelefon. Det er dermed mulig for myndigheter, hackere eller andre å få tak i denne typen brukerdata. De vil imidlertid ikke kunne få tilgang til dataene som befinner seg i blokkjeden.

Et annet problem er at brukeren får mer ansvar og risiko. Dersom man skulle miste eller glemme adresse og passord på blokkjeden, mister man også nøkkelen. Da har man ingen mulighet til å få tak i transaksjonene og informasjonen igjen. Det er mange som ikke har kunnet ta ut verdiene de har i Bitcoin fordi de har glemt dette. Hvis noen uvedkommende får tak i nøkkelen til noen andre på blokkjeden, kan vedkommende nøste seg tilbake til alle transaksjoner som denne personen har gjort.

⁴⁴ http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf (s.9)

En måte å gjøre det vanskeligere for andre å samle spor og avsløre ens identitet er å lage mange adresser på blokkjeden, på samme måte som man kan ha mange e-postadresser med ulike pseudonymer. Det er også mulig å legge til lag over blokkjeden, som kan sikre personvernet ytterligere. Det finnes blant annet en metode som kalles «null kunnskapsbevis» (*zero-knowledge proof*) der en tilbyder kan bevise overfor en annen part at et gitt utsagn er sant uten å røpe noen annen informasjon bortsett fra det faktum at utsagnet faktisk er sant.⁴⁵

MER KONTROLL TIL BRUKERNE

Vi legger igjen mange spor hver gang vi bruker digitale tjenester, og vi har ikke nødvendigvis oversikt over hvem som vet hva om oss. Kan vi stole på at dataene blir brukt til det de er ment til?

Blokkjede-teknologi kan gi brukerne kontroll over bruken av egne data gjennom verktøy for transparens, åpenhet og brukersamtykke. Dette gjør det mulig å løse offentlige tjenester på en ny måte.

Blokkjeden egner seg til å håndtere samtykke, fullmakter, sperringer og reserverasjoner på tvers av ulike registre på en enhetlig og trygg måte. Hvordan brukerne vil dele sine data kan uttrykkes som regler som lagres på en offentlig blokkjede. Dermed vil reglene være transparente og ingen andre enn de som eier dataene kan tukle med disse rettighetene.

Et eksempel er sensitive helsedata. Ved å dele helsedata kan helsetjenesten gi mer presis og personalisert diagnose, behandling og forebygging, samtidig som medisinsk forskning får tilgang på nyttige data. I dag håndterer imidlertid ulike systemer fullmakter forskjellig, og det er vanskelig å ha oversikt.

Tjenesten MyHealthMyData benytter blokkjeden til å gi brukerne mulighet til å gi, nekte eller trekke tilbake tilgang til helsedata fra ulike tilbydere.⁴⁶ Innbyggerne kan altså enklere kontrollere hvem de deler hvilke helsedata med, og hvordan de kan brukes.

⁴⁵ https://en.wikipedia.org/wiki/Zero-knowledge_proof

⁴⁶ <https://ec.europa.eu/digital-single-market/en/blockchain-technologies>

Det EU-finansierte forskningsprosjektet Decode (DEcentralised Citizen Owned Data Ecosystems) foreslår å gå enda lengre. Prosjektpartnerne fra en rekke universiteter og institutter advarer mot at innbyggerne vil slutte å dele personlige data dersom det fortsetter som i dag, hvor noen få store virksomheter både lagrer, prosesserer og kontrollerer tilgangen til våre data.

Konseptet baseres på blokkjede-teknologi og innebærer at kontrollen over dataene flyttes over til brukerne, ved at data lagres lokalt hos hver og en av oss, enten på en PC eller i en privat nettsky, og at brukerne selv bestemmer hvem som skal ha tilgang til hvilke typer data, i hvilken tidsperiode og for hvilke formål. På denne måten må de som ønsker tilgang i større grad argumentere for hvorfor og hvordan de vil bruke dataene.⁴⁷

SIKRE TRANSAKSJONER OG UTVEKSLING AV DATA

Vi ønsker at riktige personer og institusjoner har tilgang til nødvendige data når de trenger det. Dette er for eksempel viktig i helsetjenesten. Men hvordan kan vi unngå at for mange får for mye informasjon om oss?

Blokkjede-teknologien tilbyr et sett med mekanismer som sikrer at transaksjonene utføres i henhold til programmerte regler. Slike regler kan for eksempel være hvordan data utveksles mellom ulike offentlige etater eller mellom land.

Estland har etablert en blokkjede-infrastruktur som gjør det mulig å koble sammen informasjon fra ulike offentlige etater. Selve dataene ligger fremdeles lokalt, men blokkjeden holder rede på hvordan dataene kan deles mellom institusjoner på en sikker måte og i henhold til lovverket. Estland bruker en annen blokkjede-variant enn Bitcoin; den krever blant annet tillatelse fra en tredjepart for å få tilgang (*permissioned*).⁴⁸

Estland har også inngått en avtale med Finland om å bruke blokkjeden for å gjøre helsedata tilgjengelig for helsepersonell og innbyggere i begge land. Dette vil gjøre det mulig å tilby helsetjenester på tvers av land, og for innbyggerne å bruke helsetjenester når de er på reise.⁴⁹

⁴⁷ <https://www.nesta.org.uk/sites/default/files/decode-o2.pdf>

⁴⁸ <http://www.digitalinsuranceagenda.com/96/guardtime-the-worlds-largest-blockchain-company/>

⁴⁹ <https://e-estonia.com/estonia-and-finland-to-start-sharing-patient-data-and-thats-just-the-start/>

Alle innbyggere i Estland kan logge seg inn på sine egne data, for eksempel i helseregisteret, og se hvilke helsearbeidere som har gjort det samme og når. Innbyggerne kan be om en begrunnelse fra offentlige ansatte som har gått inn på sine data uten god grunn, og eventuelt stille dem for retten.⁵⁰

UFORGLEMMELIGE MULIGHETER

Blokkjede-teknologien har snart 10-årsjubileum. Den har hatt en eksplosiv vekst, spesielt som kryptovaluta. Vi har fått prinsipielle bevis for at konseptet også kan forbedre personvernet, spesielt når det gjelder sikker lagring og utveksling av informasjon, og for gi brukerne mer kontroll.

Et annet spørsmål er om den er bærekraftig. Konsensusmekanismen slik den er utformet i dag, krever for eksempel veldig mye regnekraft og energi. Bitcoin har i løpet av 2017 gått forbi det årlige energiforbruket til land som Danmark og Irland, og brukte pr. januar 2017 45 terrawatt per time (*TWh*) årlig, noe som tilsvarer det årlige energiforbruket i Irak.⁵¹ Det reises også spørsmål om en teknologi som baserer seg på anonymitet er sosialt bærekraftig, siden det åpner for omfattende hvitvasking og finansiering av kriminell virksomhet.

Det utvikles imidlertid nye typer blokkjeder som kan vise seg å fungere bra på ulike områder. For noen, som offentlige myndigheter, er behovet for å unngå tredjeparter naturlig nok ikke så viktig.

Teknologirådet har tidligere argumentert for å etablere en tydelig *digital samfunnskontrakt* for samspillet mellom innbyggere og offentlige virksomheter. Å gi innbyggerne reell mulighet til å kontrollere og forme sin digitale profil vil være en viktig del av en slik samfunnskontrakt.⁵² Helsemyndighetene kan for eksempel starte å prøve ut hvordan blokkjeden kan brukes for å styre tilgang til sensitive helsedata.

Det blir viktig å bygge inn personvern hensyn i blokkjede-teknologien fra starten. En personvern-nøtt er for eksempel følgende: Det er i utgangspunktet bare mulig å legge til transaksjoner på blokkjeder. Hvis en transaksjon først er blitt

⁵⁰ <https://medium.com/e-residency-blog/welcome-to-the-blockchain-nation-5d9b46c06fd4>

⁵¹ <https://digiconomist.net/bitcoin-energy-consumption>

⁵² https://teknologiradet.no/wp-content/uploads/sites/19/2013/08/Rapport_Denne-gangen-er-det-personlig.-Det-digitale-skiftet-i-offentlig-sektor.pdf (s. 55).

godkjent og validert på blokkjeden kan den ikke slettes. Dette er et av grunnkonseptene for å få til tilliten i systemet. Det betyr at alle transaksjoner som er blitt utført på en blokkjede siden tidenes morgen ligger lagret, noe som harmonerer dårlig med retten til å bli glemt.⁵³

⁵³ <https://www2.deloitte.com/dl/en/pages/legal/articles/blockchain-datenschutzrecht.html>

TILLIT

Vi må kunne stole på at opplysningene våre blir behandlet på en god og sikker måte. I 2017 ble denne tilliten utfordret, og vi ser her nærmere på tre aktuelle områder - tjenesteutsetting til utlandet, sikkerhet i forbrukerelektronikk og kinesiske aktører bak betalingstjenester.

Skal vi si ja til å dele, trenger vi tillit. Tillit er ikke bare nødvendig når hver og en av oss står overfor et enkeltvalg, som å inngå et kundeforhold eller ikke. Tillit er også viktig i et samfunnsperspektiv, for hvordan samfunnsfunksjoner fungerer, hvordan vi forholder oss til våre omgivelser og vår deltakelse i samfunnet. Tør vi å dele alt med legen vår? Stoler vi på at opplysninger om vår privatøkonomi blir behandlet fortrolig? Våger vi å varsle om kritikkverdige forhold? Kan vi ta i bruk internettbaserte dingser uten å føle oss overvåket?

Tall fra undersøkelsen

I de tre påfølgende kapitlene viser vi tall fra en ny undersøkelse utført av Kantar TNS. Spørreundersøkelsen ble gjennomført medio desember 2017, med 1015 respondenter fra 18 år og oppover fra Kantar TNS' landsrepresentative web-panel.

Nye tjenester og produkter er i økende grad basert på data, og i særlig grad personopplysninger. Digitalisering, effektivisering, produktutvikling og videreutvikling av tjenester avhenger av at folk har tillit til å dele opplysninger. Tillit verken kan eller bør tas for gitt. Offentlige og private må vise seg tillitsverdige. De må evne å vise oss hvorfor vi skal stole på dem.

TILLIT TIL TJENESTEUTSETTING

Tjenesteutsetting - enten det er lagring av data eller drift og vedlikehold av IKT-infrastruktur - er egentlig gammelt nytt. I 2017 ble imidlertid tjenesteutsetting, og helt særlig tjenesteutsetting til utlandet, gjenstand for en fornyet interesse og aktualitet. Primært gjennom avsløringer eller skandaler. Stoler vi på at virksomheter tar gode valg i forbindelse med tjenesteutsetting til utlandet?

Her i Norge er det særlig to saker som har ført til at tjenesteutsetting er satt på dagsorden:

Den saken som har fått størst oppmerksomhet er den såkalte «Helse Sør-Øst-saken», som NRK meldte om for første gang i mai 2017.⁵⁴ IT-medarbeidere i Asia og Øst-Europa hadde fått tilgang til pasientdata fra Helse Sør-Øst, som lagrer pasientinformasjon om halvparten av alle nordmenn. Bakgrunnen var at helseforetakene i Helse Sør-Øst, og deres databehandler Sykehuspartner hadde satt ut tjenester og infrastruktur til den amerikanske IKT-aktøren HPE (senere DXC).

⁵⁴ https://www.nrk.no/norge/helse-sor-ost_innrommer-at-utenlandske-it-arbeidere-har-hatt-tilgang-til-pasientjournaler-1.13478443

Den andre saken ble kalt «Nødnett-saken» etter at NRK omtalte den for første gang i februar 2017. Etter det «NRK kjenner til har deler av Nødnettet i lengre tid vært driftet fra India, av indiske IT-arbeidere som ikke er sikkerhetsklart. ⁵⁵» Og videre, at IT-arbeiderne i India kunne ha stengt ned deler av nødnettet, uten at man fra norsk hold kunne forhindre det. Nødnettet er samfunnskritisk infrastruktur, med brukere som politiet, andre nødetater og Forsvaret.

I tillegg kommer den svært alvorlige IT-skandalen i Sverige, hvor Transportstyrelsens tjenesteutsetting hadde ført til at flere svært beskyttelsesverdige registre var tilgjengelige for utenlandske IKT-teknikere uten sikkerhetsklarering. Flere statsråder måtte gå. ⁵⁶

INFORMASJONSSIKKERHET OG TILLIT

En fellesnevner i sakene er informasjonssikkerhet – hvordan konfidensialitet, integritet og tilgjengelighet blir ivaretatt.

Tjenesteutsetting er et svært personvernrelevant tema. Det handler om hvilke parter som får tilgang og kontroll over personopplysninger. I en slik sammenheng har vi som enkeltmennesker ofte lite informasjon og få valgmuligheter. Trenger du helsetjenester på sykehuset, må du leve med den måten sykehuset organiserer sin IKT-drift på. Vi er i stor grad overlatt til at virksomhetene som har opplysninger om oss, tar gode valg.

Utfordringene ved tjenesteutsetting er imidlertid ikke et spørsmål om sikring av personopplysninger alene. Det kan også handle om sikkerhet i bred forstand. Om sikkerhet for viktig infrastruktur og sentrale samfunnsfunksjoner, og i ytterste konsekvens nasjonal sikkerhet.

De nevnte avsløringene kan svekke befolkningens tillit. Både til aktørene som er involvert, men også til tjenesteutsetting som sådan, og da spesielt til utlandet. Det gir særlig grobunn for uro at de involverte aktørene er store og antatt profesjonelle, der behovet for god informasjonssikkerhet er selvsagt. Hvis dette

⁵⁵ <https://www.nrk.no/norge/driften-nodnettet-ulovlig-fra-india-1.13358591>

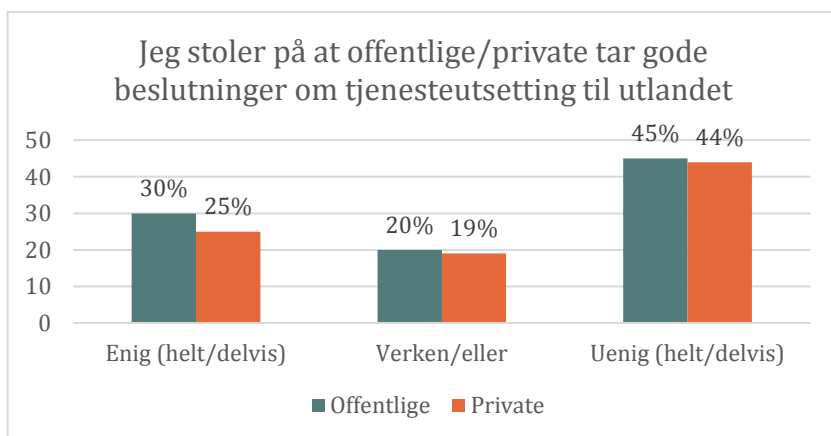
⁵⁶ <https://e24.no/makro-og-politikk/sverige/sveriges-statsminister-stefan-lofven-gaar-ikke-av-etter-it-skandalen/24105295>

kunne skje her, hvordan står det da til hos andre og mindre profesjonelle aktører? En rekke spørsmål melder seg. Både om vårt personvern som enkeltmenneske, men også om situasjonen i et bredere perspektiv:

- Var de nevnte sakene kun sjeldne eksempler, eller står vi i en situasjon hvor mange aktører egentlig mangler oversikt over hva som faktisk skjer, hvilke parter som har tilgang eller kontroll over hva, og hvilken risiko de i praksis opererer med?
- Setter økonomi, effektivitet og behovet for fremdrift i IKT-prosjekter personvern og sikkerhet på sidelinjen?

LITE TILLIT I BEFOLKNINGEN

I en undersøkelse gjennomført av Kantar TNS⁵⁷ spurte vi om tillit til tjenesteutsetting til utlandet:⁵⁸



Svarene viser at tilliten til tjenesteutsetting både i offentlig og privat sektor ikke er god. Det er betydelig flere som svarer at de er helt eller delvis *u*enige i at

⁵⁷ Se introduksjonskapittelet «Tillit».

⁵⁸ Utsagnene lød slik: «Jeg stoler på at offentlige virksomheter i Norge tar gode beslutninger om tjenesteutsettelse til utlandet» og «Jeg stoler på at private bedrifter i Norge tar gode beslutninger om tjenesteutsettelse til utlandet». Undersøkelsen hadde følgende introduksjonstekst til utsagnene: «Offentlige og private virksomheter kan tjenesteutsette (outsource) IKT-drift og vedlikehold, eller lagring av personopplysninger, til utenlandske aktører. Tjenesteutsettelse kan redusere kostnader og være enklere for en del virksomheter, men det innebærer ofte at medarbeidere i utlandet har tilgang til dataene i IKT-systemet.» Andelen for «vet ikke» eller ubesvart er ikke tatt med i diagrammet.

de stoler på at offentlige eller private tar gode valg ved tjenesteutsetting til utlandet, sammenliknet med de som sier seg helt eller delvis enige. Svært få – bare fem (offentlige) eller tre prosent (private) – viser sterk tiltro til at offentlige eller private tar gode valg ved tjenesteutsetting til utlandet (alternativet «helt enig»). Til sammenlikning velger rundt 20 prosent det stikk motsatte alternativet, «helt uenig». Dette er en lite tilfredsstillende situasjon.

Det er noe overraskende at svarene for offentlige og private er så like. Tilliten til det offentlige regnes gjerne som god. En tidligere undersøkelsen fra Datatilsynet viste høyere tillit til behandling av personopplysninger til de offentlige virksomhetene tatt med i undersøkelsen, enn til de private.⁵⁹

DEBATT OG KONTROLL FRA MYNDIGHETER

Sakene folk kjenner fra nyhetene har også brakt med seg noe positivt. Oppmerksomhet i media og oppfølging av relevante myndigheter har rettet søket på krav rundt tjenesteutsetting, det har skapt debatt og forhåpentlig også en større grad av bevissthet.

I oktober 2017 varslet Datatilsynet vedtak om overtredelsesgebyr på kroner 800 000,- for hver av de ni helseforetakene i Helse Sør-Øst. Dette er det høyeste gebyret Datatilsynet har gitt noen gang i en enkelt sak. Helseforetakene fikk gebyr for å ikke ha oppfylt pliktene til sikkerhetsledelse, risikovurderinger og tilgangsstyring i forbindelse med tjenesteutsetting av IKT-drift til utlandet.

I kjølvannet av Helse Sør-Øst-saken, ga Helse- og omsorgsdepartementet i juni 2017 Direktoratet for e-helse i oppdrag å gjennomgå informasjonssikkerheten ved bruk av private leverandører i helse- og omsorgssektoren. Oppdraget inkluderte blant annet å identifisere og foreslå gode rutiner for å sikre informasjonssikkerhet ved bruk av private leverandører. Rapporten⁶⁰ ble levert i november 2017.

I Nødnett-saken igangsatte både Nasjonal kommunikasjonsmyndighet (Nkom) og Nasjonal sikkerhetsmyndighet (NSM) tilsyn. Begge myndigheter

⁵⁹ Personvernundersøkelsen 2013/2014, side 9.

[https://www.datatilsynet.no/globalassets/global/om-](https://www.datatilsynet.no/globalassets/global/om-personvern/rapporter/personvernundersokelsen/samlerapport-personvernundersokelsen.pdf)

[personvern/rapporter/personvernundersokelsen/samlerapport-personvernundersokelsen.pdf](https://www.datatilsynet.no/globalassets/global/om-personvern/rapporter/personvernundersokelsen/samlerapport-personvernundersokelsen.pdf)

⁶⁰ <https://ehelse.no/nyheter/ny-rapport-om-informasjonssikkerhet>

konkluderte med avvik etter henholdsvis ekomloven og sikkerhetsloven med forskrifter, og ga pålegg om endringer.⁶¹

Selv om hensynene de forskjellige myndighetene er satt til å ivareta er ulike, er de grunnleggende problemstillingene og løsningene i forbindelse med tjenesteutsetting mye av de samme. Myndigheter har tidligere i for stor grad blitt sittende på hver sin tue. Direktørene fra Datatilsynet, NSM, Direktoratet for E-helse, Helsetilsynet og Finanstilsynet har nå invitert departementer og en rekke etater til møte om utkontraktering av tjenester og infrastruktur. Målet er å formidle hva regelverket stiller som krav, dele erfaringer og informere hverandre om pågående arbeid om tjenesteutsetting.

VIL DU HA TILLIT, MÅ DU HA KONTROLL

Tallene fra vår undersøkelse viser at de fleste i beskjeden grad stoler på at offentlig og private aktører tar gode valg om tjenesteutsetting til utlandet.

Gode valg er også det sentrale poenget når man ser på myndighetenes reaksjon. Det er enighet blant myndigheter som Datatilsynet, NSM, Nkom eller E-helse-direktoratet om at tjenesteutsetting kan ha store fordeler, og kan også bedre sikkerheten i en del tilfeller. Men gode valg fordrer gode prosesser, kunnskap og kartlegging hos aktørene som vurderer tjenesteutsetting.

Sentralt i dette står vurderinger av risiko, det vil si vurdering av verdier, trusler og sårbarhet. Og det handler ikke minst om ledelse: Ledelsen må ha en klar forståelse av sitt ansvar for personvern og informasjonssikkerhet, og ansvaret for valg om hvilken risiko virksomheten kan akseptere. Ledelsen må vite hvilke verdier de forvalter i form av personopplysninger og hvordan personopplysningen i praksis blir brukt og sikret.

Når virksomheten benytter en ekstern part, må virksomhetens system for styring og kontroll også gjelde den eksterne, og man må ha kontroll med hva eksterne parter foretar seg. Bestillerkompetanse er også viktig for gode valg – hva som må gjøres og tas stilling til før og i en utlysning av tjenesteutsetting.

⁶¹ <https://www.nkom.no/aktuelt/nyheter/broadnet-hadde-flere-alvorlige-brudd-p%C3%A5-ekomloven>, <https://nsm.stat.no/aktuelt/status-pa-tilsynssak--direktoratet-for-samfunnssikkerhet-og-beredskap-dsb-og-motorola/>

For å kunne utvikle og tilby gode digitaliserte tjenester basert på personopplysninger er både offentlige og private aktører avhengig av tillit. For at vi skal bruke tjenestene og være villig til å dele våre opplysninger, må vi kunne være trygge på at de som forvalter informasjon om oss, har kontroll.

Vi må kunne stole på at risiko er grundig vurdert, valg av aktør og land inkludert. Vi må kunne stole på at økonomi og behov for fremdrift i store IKT-prosjekter ikke gjør sikkerhet til et underordnet tema. Vi må kunne stole på at ledelsen opplever personvern og informasjonssikkerhet som sitt ansvar, og ikke som noe IT-avdelingen alene kan stille med.

KAN VI STOLE PÅ DINGSENE?

Joggesko, leketøy, kjøleskap og blodtrykksmålere. Forbruker-elektronikk som samler opplysninger om oss for å hjelpe oss i hverdagen er i kraftig vekst. Det er praktisk, men er det sikkert?

De kalles ofte tingenes internett. Gjenstander som kobles til internett og snakker med hverandre. Dessverre ser vi alt for mange eksempler på at disse produktene ikke sikrer personopplysningene til brukerne på en god måte.

FOR DÅRLIG SIKKERHET I TINGENES INTERNETT

Høsten 2017 avdekket Forbrukerrådet alvorlige sikkerhetshull, upålitelige trygghetsfunksjoner og manglende forbrukervern i smartklokker for barn.⁶² Klokkene fungerer som en smarttelefon som kommuniserer med foreldrene via en mobilapp. Det ble funnet kritiske sikkerhetsbrister i tre av fire klokker som ble testet. To hadde sikkerhetshull som potensielt kan gi en fremmed kontroll over mobilappen og tilgang til barnets sanntidsposisjon og historiske lokasjonsdata. I tillegg var det mulig for en utenforstående å ta kontakt med barnet igjennom smartklokken.

⁶² <https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-october-2017.pdf>

Forbrukerrådet har også testet ti blodsukkerapparater.⁶³ Apparatene har god brukervennlighet, men svikter når det kommer til sikkerhet og personvern. Flere av mobilappene legger opp til usikret deling av helseopplysninger over internett. Ett av produktene inneholdt sporingskapsler fra kommersielle tredjeparter som potensielt kan brukes til å bygge opp profiler på forbrukere, som igjen kan brukes til målretting av reklame og andre tjenester. Flere av produktene informerte ikke om vilkårene på en tilfredsstillende måte.

Elektronikkprodusenten LG måtte oppdatere programvaren sin etter at sikkerhetseksperter oppdaget en feil som gjorde det mulig å ta kontroll over produkter som kjøleskap, ovner og oppvaskmaskiner.⁶⁴ Sikkerhetseksperter fant feilen i mobilappen og skytjenesten tilknyttet produktene. Uvedkommende kunne relativt enkelt logge seg på mobilappen for å styre innstillingene og hente ut opplysninger fra produktene, for eksempel gjennom kameraet på smartstøvsugen.

Dette er bare noen eksempler fra det siste året. En rapport fra Consumers International om markedet for smarte forbrukerprodukter konkluderer at i selvkapenes iver for å få produktene sine ut på markedet har de nedprioritert sikkerhet og forbrukerbeskyttelse.⁶⁵

BRYR FOLK SEG OM SIKKERHETEN I DINGSER?

Fordelene med smarte produkter er mange: De kan gi oss mer tilrettelagte tjenester, raskere responstid, et detaljert beslutningsgrunnlag, mulighet til å fjernstyre tingene våre og gi oss mer nøyaktig informasjon om oss selv og helsa vår. De er praktiske, men stoler vi på dem?

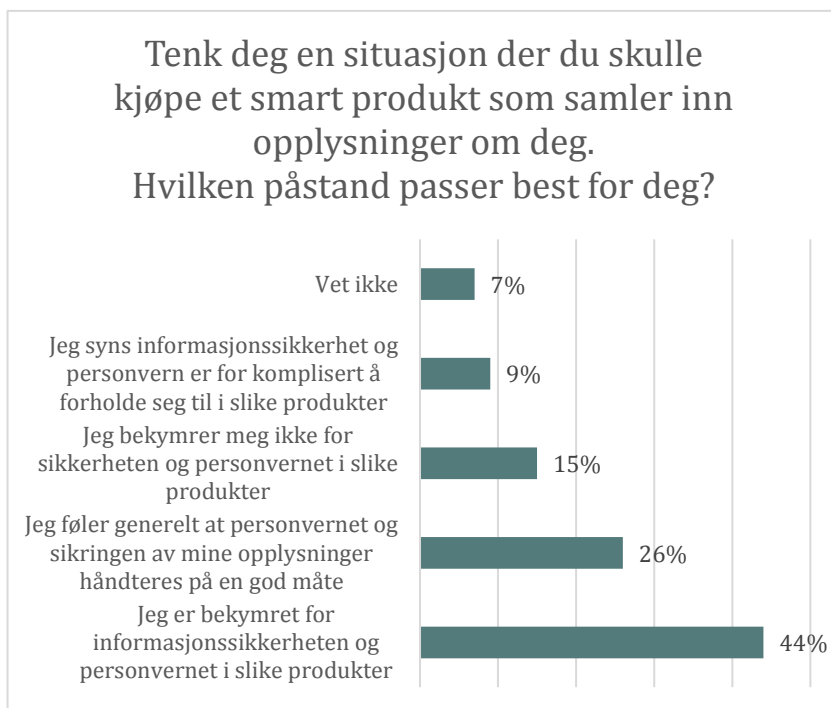
I vår undersøkelse ba vi respondentene velge mellom fire påstander som beskriver hvordan de opplever sikkerheten og personvernet i produkter koblet til internett i en kjøpsituasjon. Den påstanden flest valgte (44 prosent) var at de var bekymret for informasjonssikkerheten og personvernet i slike produkter. På andreplass kommer påstanden om at de føler at personvernet og sikringen av

⁶³ <https://www.forbrukerradet.no/siste-nytt/brukervennlige-blodsukkerapparater-men-appersvikter>

⁶⁴ <http://www.zdnet.com/article/security-flaw-in-lg-iot-software-left-home-appliances-vulnerable/>

⁶⁵ <http://www.consumersinternational.org/media/154746/iot2017review-2nded.pdf>

sine opplysninger er godt ivaretatt (26 prosent). 15 prosent svarer at de ikke bekymrer seg for sikkerheten og personvernet i slike produkter.



Tallene forteller oss at nesten halvparten av norske forbrukere bekymrer seg for informasjonssikkerheten og personvernet til tingens internett. Det er ikke gode nyheter for produsenter og tilbydere av slike produkter. Samtidig melder en god del (til sammen 41 prosent hvis du slår sammen de som ikke bekymrer seg og de som føler at opplysningene deres blir håndtert på en god måte) at de ikke føler en slik bekymring. Det viser at bildet ikke er helsvart, men at en stor andel av forbrukere ikke har tillit til at opplysningene deres håndteres på en god måte i tingenes internett.

Mange forbrukere er bekymret for opplysningene sine i produkter koblet til internett. Men bruker de likevel produktene?

Ja, folk kjøper og bruker smarte produkter som samler inn personopplysninger. Men salgsøkningen av denne typen produkter er ikke like stor som forventet de siste to årene. Cisco har nedjustert sin prognose for antall smarte produkter i omløp i 2020 fra 50 til 30 milliarder.⁶⁶ Accenture sier at i tillegg til pris og brukervennlighet er sikkerhet en av hovedbarrierene for vekst. Sikkerhet og personvern er ikke lengre bare et irritasjonsmoment, men en av hovedårsakene til at forbrukere ikke tar i bruk produkter eller tjenester.⁶⁷

I en undersøkelse Accenture har gjennomført svarer nesten halvparten av de 28 000 respondentene at sikkerhet og personvern er en barriere for at de skal ta i bruk smarte produkter. 18 prosent sier de har sluttet å bruke et produkt eller tjeneste på grunn av bekymring for informasjonssikkerheten, og 24 prosent har utsatt et kjøp av samme grunn. Mange forbrukere gjør imidlertid en avveining og tar i bruk produkter på tross av at de er bekymret for sikkerheten og personvernet sitt.

Det interessante spørsmålet er hvor grensen går for at folk velger å ikke ta i bruk et produkt eller å ikke dele informasjonen sin med slike produkter. Og hva er konsekvensen hvis vi kommer til et skifte der tilliten blir så lav at majoriteten vegrer seg for å dele opplysninger?

Hvor grensen går er ikke godt å si, men tallene fra Accenture sin undersøkelse viser at en god del forbrukere allerede har nådd grensen. Hvis vi går i retning av en situasjon der store deler av befolkningen ikke har tillit til digitale tjenester og produkter, har vi et problem. For forbrukere kan det bety færre gode og trygge tjenester å velge mellom fordi mange leverandører er uaktuelle på grunn av manglende sikkerhet og personvern. For virksomheter kan manglende tillit og tilbakeholdne forbrukere by på utfordringer for salg og videreutvikling av produkter – fordi mange virksomheter er avhengige av data for å utvikle tjenestene sine.

⁶⁶ 'Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated', IEEE Spectrum, 18/08/2016

⁶⁷ https://www.accenture.com/_acnmedia/PDF-3/Accenture-Igniting-Growth-in-Consumer-Technology.pdf#zoom=50

HVA MÅ TIL FOR AT VI KAN STOLE PÅ TINGENES INTERNETT?

Det er vanskelig for en forbruker å vite hvordan opplysningene deres blir brukt. I en undersøkelse gjennomført av personverntilsyn verden over var konklusjonen at 59 prosent av de 300 testede smartproduktene ikke forklarte hvordan personopplysningene til brukerne ble behandlet.⁶⁸

Hva må til for at forbrukerne får tilbake kontrollen over egne opplysninger? Vi spurte hva folk mente måtte til for at de kan stole på produktene de kjøper.



71 prosent mener at et godkjentstempel fra et sertifiseringsorgan ville være «svært nyttig» eller «litt nyttig» for å kunne stole på at opplysningene deres håndteres på en god måte. Litt over halvparten svarte at en personvernerklæring er nyttig. Og litt under halvparten mener en merkeordning i regi av bransjen selv er nyttig.

FORBRUKEREN KAN IKKE STÅ ALENE

Forbrukerne ønsker veiledning, helst gjennom en uavhengig merkeordning. Men det er også viktig at myndighetene jobber aktivt for å styrke forbrukernes rettigheter. Datatilsynet og andre myndigheter som forvalter et regelverk må

⁶⁸ <https://www.privacyenforcement.net/sites/default/files/Annual%20Report%202016.pdf>

føre tilsyn med produsenter av smarte produkter og slå hardere ned dersom disse ikke følger reglene.

Det er viktig at utviklere og tilbydere nå tar sitt ansvar og setter fokus på å ivareta brukernes personvern. Dette er en forutsetning for å vinne tilbake og opprettholde kundenes tillit og villighet til å dele data – noe videre vekst og utvikling er avhengig av. Også politikere må ha et samlet fokus på personvern, sikkerhet og næringsutvikling. Personvern er ikke bare et lovkrav og et samfunnsansvar, men også et potensielt konkurransefortrinn.

KINAS DIGITALE KJEMPER

Kina har på få år vokst frem som en digital kjempe. Tilgang til enorme datamengder og fravær av personvernregulering, har gjort Kina til et laboratorium for eksperimentell databruk. Kinesiske teknologiselskaper ekspanderer nå vestover og samler inn personopplysninger fra kunder over hele verden. Snart vil betalingstjenester levert av kinesiske selskap bli tilgjengelig i Norge. Har nordmenn tillit til disse tjenestene?

ALT I ETT

Google, Amazon, Facebook og Apple (populært kalt GAFA) er fortsatt verdens største teknologiselskaper, men en ny generasjon utfordrere vokser frem i øst. I dag er tre av de ti største internettelskapene i verden kinesiske: Tencent, Alibaba og Baidu (populært kalt BAT i Kina). I tillegg til å være markedsledende på hvert sitt område, forandrer disse selskapene markedene, og skaper nye. De siste årene har BAT figurert på MIT Technology Reviews årlige liste over de smarteste selskapene i verden.⁶⁹ Tiden da kinesiske selskap ble betraktet kun som copycats, er definitivt over.

BAT har ingen respekt for grenser, det være seg sektorer, land eller teknologi. Selskapene har sine respektive røtter innen søketeknologi, ehandel og sosiale

⁶⁹ <https://www.technologyreview.com/lists/companies/2017/>

nettsamfunn, men alle har de siste årene beveget seg inn på nye områder. Alibaba og Tencent har etter hvert tjenester som berører omtrent alle aspekter av livet til en kinesisk forbruker.

Tencent eier Kinas største sosiale nettsamfunn WeChat, som har omlag én milliard brukere verden over. Selskapets suksess kommer av at de er gode til å tiltrekke seg nye brukere og holde på dem. Dette gjør de ved å kontinuerlig utvide mobilappen sin til å inkludere nye typer tjenester, slik som messaging, online-spill, shopping, musikk, videoer og vennebetaling.

På samme måte som Tencent, bygger Alibaba opp en verdensomspennende plattform av ulike forbrukertjenester. I tillegg til å være verdens største ehandels-selskap er de Ebay, Vipps, Facebook, forsikringsselskap og mye annet i ett. I likhet med Amazon tilbyr de også skylagringstjenester. Alibaba Cloud er deres raskest voksende tjeneste⁷⁰. Alibaba eier også Alipay, verdens største mobilbetalingstjeneste med over 520 millioner brukere (til sammenligning har Apple Pay om lag 12 millioner brukere).⁷¹

Baidu er Kinas Google. Selskapet eier den dominerende søkemotoren i Kina og er verdensledende på utvikling av kunstig intelligens. Selskapet jobber blant annet med å utvikle førerløse biler. Da kinesiske myndigheter nylig opprettet en nasjonalt laboratorium for kunstig intelligens, ble Baidu valgt til å lede prosjektet.

PÅ VEI VESTOVER

BAT beveger seg nå vestover. Betalingstjenesten Alipay ble for eksempel gjort tilgjengelig i norske butikker i 2017. Den kan foreløpig kun benyttes av kinesere på besøk i Norge, men det er trolig kun et spørsmål om tid før også norske forbrukere kan ta i bruk Alipay, både hjemme i Norge og på ferie i utlandet.

Skal Kina nå målsettingen om å bli verdens ledende stormakt på kunstig intelligens, må kinesiske selskap ekspandere til nye markeder på jakt etter enda mer data.⁷² Tilgang til store mengder forbrukerdata er avgjørende for å kunne hevde

⁷⁰ E24, «Verdens største betalingsløsning lanseres i Norge – men ikke for nordmenn», 08.09.2017, <http://e24.no/naeringsliv/teknologi/verdens-stoerste-betalingsloesning-lanseres-i-norge-men-ikke-for-nordmenn/24133447>

⁷¹ <https://intl.alipay.com/>

⁷² <https://www.ft.com/content/856753d6-8d31-11e7-a352-e46f43c5825d>

seg i konkurransen om å bygge de mest innovative og brukervennlige tjenestene. I den sammenheng er det også interessant for kinesiske selskap å samle inn data fra norske brukere.

Alibaba og Tencent beveger seg vestover:

- I november 2017 kjøpte Tencent 25 prosent av Snap, morselskapet til Snapchat. Gjennom kjøpet av Snap har Tencent fått en alliert som gir tilgang til 166 millioner vestlige brukere og en plattform for selskapets enorme økosystem av innhold og tjenester, inkludert en betalingstjeneste.
- I 2016 kjøpte Tencent det finske spill-selskapet Supercell. Oppkjøpet styrket deres posisjon som verdensledende på onlinespill.
- Alibaba Cloud har beveget seg ut av Kina og etablert datasentre i blant annet USA og Europa.
- Både Tencent og Alibaba har investert i Didi Chuxing, Kinas konkurrent til Uber. Didi Chuxing har eierandeler i ridesharing-selskap i Europa.

ET MARKED UTEN PERSONVERNREGULERING

Det er mange årsaker til at Kina er blitt verdensledende på digital innovasjon. Fraværet av personvernregulering er en av dem. Kinesere med suksess i Silicon Valley vender nå nesen hjemover til attraktive jobber i kinesiske teknologiskapere. De lokkes av gode lønnsbetingelser, men også av de enorme datamengdene selskapene har tilgang til, og muligheten til å benytte disse dataene uten særlige restriksjoner.

Kina er i ferd med å bli et laboratorium for eksperimentell databruk, særlig innen ansikts- og stemmegjenkjenning, og i bruk av forbrukerdata til profileringsformål. Kinesiske selskap ruller ut nye digitale forretningsmodeller i et tempo og en skala verden ikke har vært vitne til før. Mange av disse forretningsmodellene vil aldri se dagens lys i Norge på grunn av personvern hensyn. Ant Financial, morselskapet til Alipay, har for eksempel utviklet kredittvurderingssystemet Sesame Credit. Sesame Credit gir kundene en score basert blant annet på hvor mye penger de bruker via Alipay og hvordan de oppfører seg i sosiale medier. Jo høyere score kunden har, jo flere muligheter åpner seg. Hvis kunden

har mer enn 600 poeng, kan hun leie biler uten depositum og har hun mer enn 650 poeng kan hun sjekke ut av hoteller raskere.⁷³

Kinesiske myndigheter utnytter også mulighetene som ligger i dataanalyse og har de siste årene satt i gang flere omfattende overvåkingsprogrammer, ofte ledet av et av de store teknologiselskapene. BAT-selskapene er statlig lisensiert og vi må regne med at myndighetene har tilgang til personopplysningene disse selskapene samler inn uten de samme rettsgarantier som i Norge.

Kina har blant annet installert det mest omfattende kameraovervåkingssystemet i verden, med 170 millioner kameraer sprett rundt i landet. De neste tre årene vil de installere 400 millioner kameraer til. Videoovervåkingssystemet er knyttet til kunstig intelligens, blant annet et system for ansiktsgjenkjenning. I tillegg til å kjenne igjen ansikter, kan kameraene fastslå kjønn, alder og etnisitet. I byen Guiyang sitter myndighetene på bilder av alle byens 3,5 millioner innbyggere og kan koble disse til deres ID-kort. BBC-journalist John Sudworth fikk tillatelse til å teste systemet i Guiyang og hvor effektivt det var til å gjenkjenne folk ute på gata. Basert på et bilde av seg selv som han sendte til politiet i forkant, tok det kun syv minutter fra Sudworth gikk ut på gata i Guiyang, til ansiktsgjenkjenningssystemet hadde lokalisert ham og myndighetene «på-grep» ham.⁷⁴

Kinesiske myndigheter er også i ferd med å bygge opp et nasjonalt profilerings-system av alle landets innbyggere, basert på de digitale sporene de legger igjen. Formålet med systemet er ifølge myndighetene å øke den sosiale og økonomiske stabiliteten ved å oppmuntre til tillitvekkende oppførsel.⁷⁵ Systemet heter Social Credit System (SCS) og skal gjøre vurderinger ved å kombinere personopplysninger fra kommersielle kilder som banker, e-handel og sosiale medier med opplysninger fra offentlige registre. SCS utvikles og opereres blant annet med hjelp fra Baidu.⁷⁶

Statsminister Erna Solberg var nylig på besøk i Kina. Der møtte hun Jack Ma, grunnleggeren av Alibaba. Tema for møtet var blant annet norske myndigheters bekymring knyttet til selskapets ivaretagelse av informasjonssikkerheten og

⁷³ Wired, «Big data meets Big Brother as China moves to rate its citizens», 21.10.2017, <http://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion>

⁷⁴ BBC, «In Your Face: China's all-seeing state», 2017, <http://www.bbc.com/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state>

⁷⁵ <http://www.chinalawtranslate.com/seeing-chinese-social-credit-through-a-glass-darkly/?lang=en>

⁷⁶ Wired, «Big data meets Big Brother as China moves to rate its citizens», 2017, <http://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion>

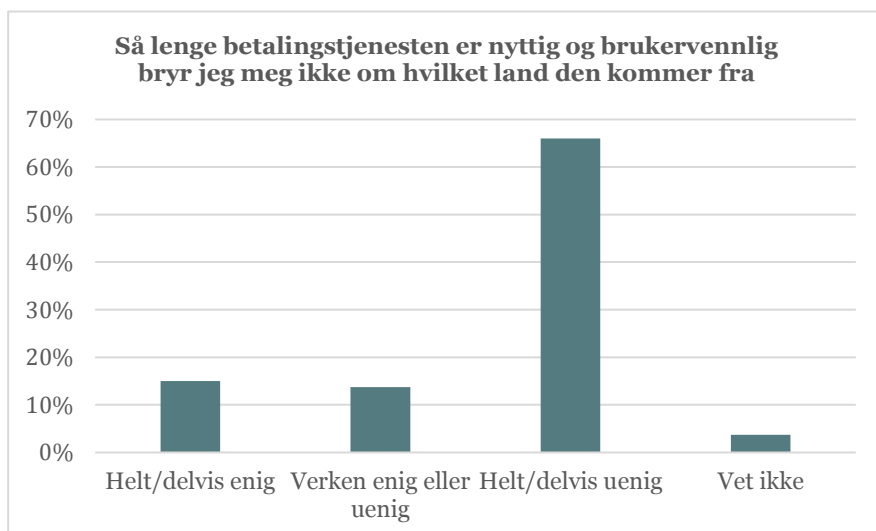
personvernet til sine kunder, kunder som også er norske.⁷⁷ Jack Ma vedgikk overfor statsministeren at det var utfordringer knyttet til personvern og informasjonssikkerhet. Samtidig uttalte han, ifølge NRK, at privatlivets tid er forbi, og at hvis noen vil vite noe om noen i dag, så får de vite det.

LAV TILLIT TIL UTENLANDSKE BETALINGSTJENESTER

Vi lever i en global verden når det gjelder bruk av digitale tjenester. Vi handler bøker, sko og klær fra nettbutikker over hele verden og kommuniserer med venner og familie via utenlandske tjenester. Snart vil vi også betale for varer og tjenester med utenlandske tjenester. Betalingstjenester fra Apple og Facebook er allerede tilgjengelig i våre naboland. Også AliPay vil trolig snart kunne tas i bruk av norske forbrukere.

I årets personvernundersøkelse ønsket vi å undersøke om nordmenns tillit til digitale betalingstjenester avhenger av hvem som leverer dem og hvor i verden de kommer fra.

HVOR TJENESTEN KOMMER FRA HAR BETYDNING



⁷⁷ <https://www.nrk.no/urix/kinesisk-nettgigant-vil-vite-mer-om-deg-1.13468466>

Den store majoriteten, 66 prosent av de spurte, er uenig i påstanden «så lenge betalingstjenesten er nyttig og brukervennlig bryr jeg meg ikke om hvilket land den kommer fra». De aller fleste bryr seg altså om hvilket opprinnelsesland tjenesten har. Kun to prosent bryr seg ikke om hvilket land betalingstjenesten kommer fra så lenge den er nyttig og brukervennlig.

I en tidligere spørreundersøkelse gjennomført av Datatilsynet, kom det frem at folk opplever opplysninger om sin privatøkonomi som følsomme.⁷⁸ Å ha tillit til tjenestene som samler inn slike data blir da ekstra viktig. Det kan være at folk i større grad er opptatt av hvilket land tjenesten kommer fra når det er snakk om betalingstjenester enn når det gjelder ehandelstjenester eller sosiale nettsamfunn.



LITEN TILLIT TIL KINESISKE BETALINGSTJENSTER

Tallene viser at tilliten til norske betalingstjenester er svært stor, hele 77 prosent av de spurte har tillit til at norske banker leverer betalingstjenester som ivaretar deres personvern. Dette tallet støttes av en tidligere undersøkelse gjennomført

⁷⁸ Datatilsynet, Personvernundersøkelsen 2013/2014,

<https://www.datatilsynet.no/globalassets/global/om-personvern/planer-strategier/personvernundersokelsen/samlerapport-personvernundersokelsen.pdf>

av Datatilsynet, som viste at åtte av ti har tillit til at norske banker ivaretar deres personopplysninger på en god måte.⁷⁹ Ettersom tilliten til norske banker er høy, skulle man kanskje tro at tilliten til europeiske banker også var relativt høy. Slik er det ikke. Under halvparten, bare 31 prosent av de spurte, har tillit til at betalingstjenester levert av finansielle institusjoner i andre europeiske land ivaretar deres personvern.

Sett i lys av fjorårets personvernundersøkelse, der kun syv prosent av de spurte svarte at de var interessert i å ta i bruk en betalingstjeneste levert av Google eller Facebook, synes vi det er overraskende at så mange som 25 prosent har tillit til at betalingstjenester levert av amerikanske teknologiselskap som Apple og Facebook ivaretar deres personvern.⁸⁰ Tilliten til betalingstjenester fra finansielle virksomheter i EU er altså omtrent lik den folk har til de amerikanske teknologiselskapene. Svært få, bare ni prosent av de spurte, har imidlertid tillit til at en betalingstjeneste levert av et kinesisk teknologiselskap ivaretar deres personvern.

KINESISKE SELSKAP KAN IKKE IGNORERE GDPR

Når den nye personvernforordningen trer i kraft i mai vil europeiske regler gjelde for alle selskaper som tilbyr tjenester og produkter til europeere, selv om selskapet ikke er lokalisert i Europa. Regelverket vil gjelde for betalingstjenester som Alipay, hvis de etter hvert åpnes for europeiske brukere.

Personvernforordningen setter andre krav til behandling av personopplysninger enn det som er tilfelle i Kina. En konsekvens av forordningen er at kinesiske selskaper som opererer i EU må forholde seg til blant annet kravene om formålsbegrensning og relevans. Dette er krav som blant annet setter restriksjoner på viderebruken av innsamlede opplysninger.

Å håndheve regulering i en global økonomi er imidlertid utfordrende. Personvernmyndighetene i Europa har gjennom flere år vært kritiske til de amerikanske teknologiselskapenes behandling av personopplysninger, blant annet relatert til bestemmelsene knyttet til formålsbegrensning. Å håndheve regelverket overfor de kinesiske teknologigigantene vil trolig også by på store utford-

⁷⁹ Idif.

⁸⁰ Datatilsynet og Teknologirådet, *Personvern 2017. Persontilpassing og kunstig intelligens*, 2017

ringer. I hvilken utstrekning kinesiske myndigheter vil ha tilgang til personopplysninger om norske borgere og hva de vil bruke de til, er for eksempel ikke lett å vite.

SMARTKLOKKE FJERNES FRA MARKEDET

I januar trekker GPSforbarn sin smartklokke fra markedet. GPSforbarn er en av flere aktører som ble pålagt å stanse all behandling av personopplysninger om sine kunder, da de ikke hadde sørget for god nok informasjonssikkerhet

EUS PERSONVERNFORORDNING BLIR NORSK LOV

En ny personopplysningslov, som gjennomfører EUs personvernforordning i norsk rett, trer i kraft i Norge og erstatter dagens personopplysningslov med forskrift. Det nye regelverket gir virksomheter nye plikter og enkeltpersoner nye rettigheter.

NY HØRING OM DIGITALT GRENSEFORSVAR

Forsvarsdepartementet fortsetter med å utrede digitalt grenseforsvar etter høringen på Lysne II-utvalgets rapport. Forsvarsminister Frank Bakke-Jensen har varslet at et høringsnotat med lovforslag vil komme i løpet av 2018. Hvilken form for digitalt grenseforsvar regjeringen til slutt vil foreslå, er for tidlig å si.

FRIERE FLYT AV BETALINGSDATA

I 3. januar innføres et nytt EU-direktiv som skal regulere betalingsformidling i EU og EØS. Direktivet innebærer at bankene mister monopol over kundenes transaksjonsopplysninger. Med samtykke fra kunden kan nye aktører få direkte innsyn i kontoer og transaksjoner og bygge nye tjenester med utgangspunkt i disse opplysningene.

MÅLRETTET KONTROLL VED GRENSA

Tolletaten inngår avtale med IT-selskapet Palantir som ved hjelp av kunstig intelligens skal målrette grensekontrollen bedre. Informasjon om bilskilt og sjåførens historikk, kombinert med data fra for eksempel valuta- og aksjonærregister kan gjøre kontrollarbeidet mer effektivt.