



PERSONVERN
TILSTAND OG TRENDER

2013

PERSONVERN 2013

TILSTAND OG TRENDER

ISBN 978-82-92447-56-7 (trykket utgave)
ISBN 978-82-92447-57-4 (elektronisk utgave)

Rapport 1/2013

Utgitt: Oslo, januar 2013

Omslag: Commando Group

Trykk: ILAS

Elektronisk publisert på: www.teknologiradet.no og www.datatilsynet.no



IDEEN BAK PERSONVERNDAGEN 2013

Det frigis daglig store mengder personlig informasjon, men hvor blir den av og hvem har tilgang? Det sies at vi nærmer oss et overvåkingssamfunn – eller at vi allerede er der. Er det slik, eller finnes det lyspunkter? Hvor er vi på vei?

I anledning den internasjonale personverndagen 28.januar 2013, har Teknologirådet og Datatilsynet forent krefter for å gi noen svar.

Ideen bak samarbeidsprosjektet er å gi et mest mulig konkret bilde av personvernsituasjonen for Ola og Kari Nordmann – det vil si hvor mye informasjon om oss som er tilgjengelig for andre. Vanlige oversikter over personvernsituasjonen er gjerne basert på lover og reguleringer, og hvor personverninngripende de vurderes til å være. Dette måler imidlertid ikke hvor eksponerte vi som enkeltindivider i realiteten er, for eksempel gjennom den meget raske utviklingen på sosiale medier, eller på arbeidsplassen.

Vi har også forsøkt å beskrive noen viktige trender. Teknologiutviklingen går fort og det er vanskelig å følge med på når, hvor og av hvem man registreres og analyseres. I samarbeid med TNS Gallup har vi dessuten utført en undersøkelse om folks holdninger til, og kunnskap om, personvernspørsmål.

Vi takker alle våre medarbeidere for godt utført arbeid. Konseptet for personverndagen har vært utviklet i samarbeid. Rapporten har to deler, der Datatilsynet har hatt hovedansvar for den første (Tilstand) og Teknologirådet for den andre (Trender).

Formålet med denne rapporten og arrangementet på Litteraturhuset den 28. januar er å bidra til bevissthet og diskusjon om personverntemaer som berører de fleste av oss.

Kjør debatt!

Vennlig hilsen

Tore Tennøe
Teknologirådet

Bjørn Erik Thon
Datatilsynet

INNHOOLD

PERSONVERN 2013 TILSTAND OG TRENDER 3

IDEEN BAK PERSONVERNDAGEN 2013 6

DET SOSIALE NETTET 9

HVA SKJER? 10

PERSONVERNUTFORDRINGEN 12

Vet facebook mer om oss enn staten? 12

Har vi kontroll på egen informasjon? 13

Innebygd personvern 14

EN HALE AV ELEKTRONISKE SPOR 16

HVA SKJER? 17

Registreringspunktene kommer tettere 17

Usikkerhet knyttet til lagring av data i bilen 18

Positiv utvikling - anonyme løsninger i kollektivtransportbransjen 18

Økning i omfanget av privat kameraovervåking 19

Beskjeden bruk av kameraovervåking i offentlig regi 20

Med sensor i lomma 21

PERSONVERNUTFORDRINGEN 22

Valgfrihet under press – utvikling i retning av obligatoriske løsninger 22

Attraktive opplysninger – bruk til nye formål 23

Mangel på informasjon og kontroll 23

ET SPORBART ARBEIDSLIV 24

HVA SKJER? 25

Mer kameraovervåking på arbeidsplassen 25

Fjernstyrt arbeidsdag 28

PERSONVERNUTFORDRINGEN 29

Dårlig kjennskap til lagringsrutiner for personopplysninger 29

Function creep: Bruk av opplysninger til nye formål 30

DRONER TAR AV	32
----------------------	-----------

HVA ER DRONER?	33
Fra krig til sivil bruk	33
Pilene peker oppover	33
Folket vil ha droner – så lenge de ikke er kommersielle	34
PERSONVERNUTFORDRINGEN	35

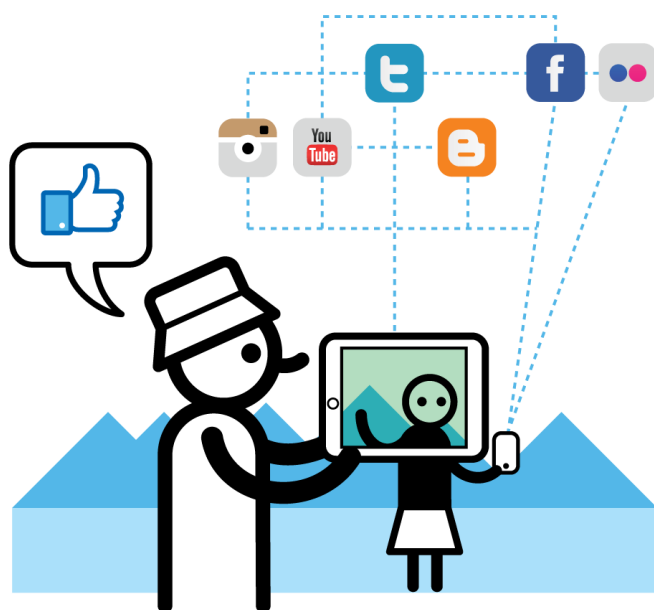
LEGEKONTOR PÅ INNERLOMMA	37
---------------------------------	-----------

HVA KAN VI GJØRE I DAG?	38
PERSONVERNUTFORDRINGEN	39

SMART POLITI	42
---------------------	-----------

Smart politi er på nett med seg selv.....	43
På nett med publikum	43
Er på nett med fremtiden.....	44
PERSONVERNUTFORDRINGEN	45
Formålsutglidning	45
Blir vi alle tystere?	46
På feil sted, til feil tid	46

DET SOSIALE NETTET

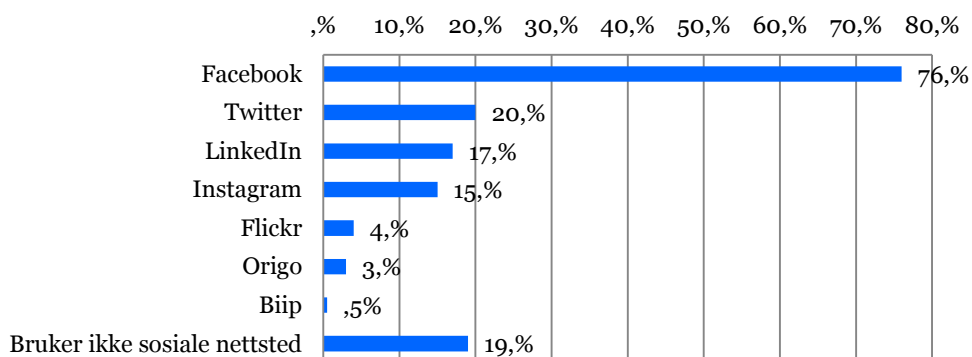


Aldri før har folk vært så opptatt av hvordan de forvalter sin personlige informasjon som i dag. Fra å være en rettighet som opptok bare de spesielt interesserte, eller kanskje de spesielt uheldige, har personvern blitt noe alle kjenner på kroppen og må forholde seg til. Det sosiale nettet åpner for fantastiske muligheter til å kommunisere, skape og dele, men utfordrer også hver enkeltes evne til å ha kontroll over egen informasjon.

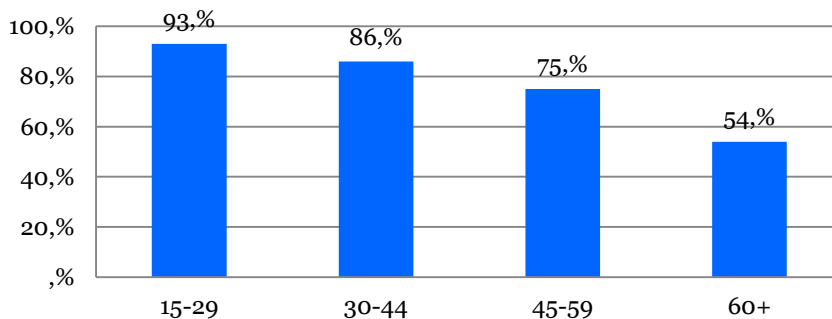
HVA SKJER?

Nordmenn er blant de ivrigste brukerne av nett og sosiale medier i europeisk sammenheng¹. Hele 80 prosent er medlem av et sosialt nettverk. Facebook er det desidert største sosiale nettverket i Norge – 79 prosent av kvinnene og 72 prosent av mennene er medlem. Twitter (20 prosent), LinkedIn (17 prosent) og Instagram (15 prosent) er også populære, men kan ikke sammenlignes med Facebook i størrelse. Hele 93 prosent av nordmenn i alderen 15-29 har en Facebook-konto. Men de er ikke de eneste: over halvparten av alle over 60 år er på Facebook.²

Andel nordmenn med brukerkonto på utvalgte sosiale nettsteder



Andel nordmenn med Facebook-konto fordelt på alder



¹ http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Information_society_statistics

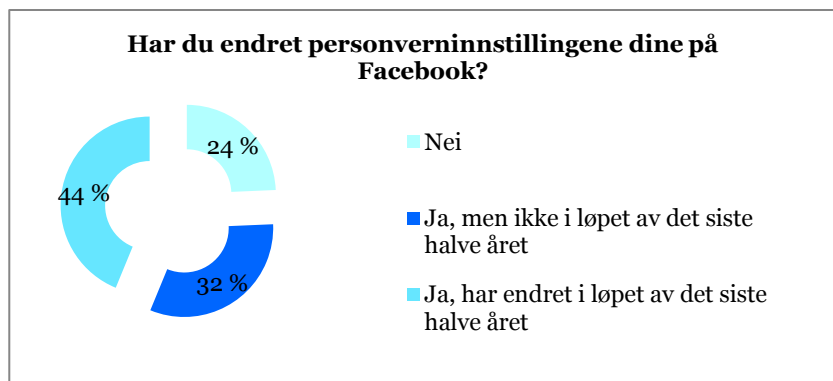
² TNS Gallup for Teknologirådet/Datatilsynet januar 2013

De siste ti årene har det skjedd en holdningsendring. Det er nå vanlig at folk i alle aldre deler feriebilder og bursdagshilsener med venner og ukjente på nettsamfunn, eller "sjekker inn" for å vise hvor de befinner seg akkurat nå. Seks av ti deler innhold som kommentarer, lenker, bilder og filmer på sosiale nettsamfunn ukentlig.³

Zuckerbergs lov: I 2007 spådde Facebookgründer Mark Zuckerberg at folk ville dele dobbelt så mye informasjon neste år som i år – og i årene framover. Mange trodde kanskje iveren etter å dele personlig informasjon ville avta etter de første hvetebrødsårene med Facebook, men seks år senere ser det ut som "Zuckerbergs lov" har bestått tidens tann. I 2012 ble det hver dag produsert 2.5 kvintillioner bytes data (det er 18 nuller) på internett. Hele 90 % av alt innhold på nett har blitt produsert de siste to årene.⁴

"Å logge seg av Facebook er blitt det samme som å melde seg ut av samfunnet." – Fortvilet, 17 år, Si;D i Aftenposten 10. januar 2013.

Å være tilstede på nett har blitt en nødvendighet – både praktisk og sosialt. Bevissthet rundt hva man deler har derfor blitt en grunnleggende kunnskap. Hele 44 prosent av norske Facebook-brukere oppgir at de har endret på personverninnstillingene i løpet av det siste halve året. Det er bra, men det er tankevekkende at en av fire aldri har rørt personverninnstillingene. Spesielt eldre brukere virker å ha en passiv holdning til personvernet – seks av ti har aldri endret personverninnstillingene⁵.



³TNS Gallup for Teknologirådet/Datatilsynet januar 2013

⁴<http://www-01.ibm.com/software/data/bigdata/>

⁵TNS Gallup for Teknologirådet/Datatilsynet januar 2013

PERSONVERNUTFORDRINGEN

VET FACEBOOK MER OM OSS ENN STATEN?

Facebook er verdens største sosiale nettsamfunn, med rundt 800 millioner brukere. Facebook kan sies å være det største, og kanskje mest intrikate, lageret av personopplysninger⁶. Vi er nå kommet til et punkt der det ikke er usannsynlig at Facebook vet mer om en del av oss enn enkeltinstanser i staten.

Facebook er imidlertid bare en av mange nettjenester nordmenn benytter seg av. Flere store analyseselskaper spesialiserer seg på å kartlegge og sammenkoble opplysninger om alder, sivilstatus, utdanning, handlevaner, helseplager og feriedrømmer. Resultatet er detaljerte brukerprofiler som selges videre til aktører som er interessert i å nå ut til bestemte målgrupper. Summen av sporene vi legger igjen på nett kan gi et utfyllende bilde av den enkelte – og det kan være et bilde man ikke nødvendigvis kjenner seg igjen i. Ved analyse av store data kan én pluss én noen ganger bli mer enn to.

Du er hva du "liker"...

Forskere ved Universitetet i Cambridge mener at det er mulig å forutse visse personlighetstrekk på bakgrunn av hva vi "liker" på Facebook. Forskerne konkluderte med at etnisitet og kjønn kan sluttes av hva vi "liker", med henholdsvis 95 og 93 prosent treffsikkerhet. Det ble også funnet at man kunne skille mellom homofile og heterofile menn (88 prosent av tilfellene). Av faktorene som ble vurdert, var det vanskeligst å anslå hvorvidt Facebook-brukerens foreldre er skilte. Her fikk man likevel en treffrate på 60 prosent - en (mild) indikasjon på at barn av skilte foreldre i større grad «liker» utsagn som dreier seg om forhold og kjærlighet⁷.

Ny teknologi bidrar til innsamling og kobling av personlig informasjon i stor skala. Ansiktsgjenkjenningsteknologi er allerede i bruk på sosiale nettsamfunn og søketjenester i USA. Teknologien gjør det mulig å automatisere søk av personer basert på bilder. Etter kritikk fra flere europeiske tilsynsmyndigheter har Facebook lagt ansiktsgjenkjenning på is i Europa av personverngrunner. Brukernes posisjonsdata logges av apper slik som Facebook, Yr og Angry Birds av mer eller mindre hensiktsmessige grunner. Har du en Iphone med Google maps vet både Apple og Google hvor du befinner deg til en hver tid. Et stort

⁶ <http://www.regjeringen.no/nn/dep/fad/dokument/proposisjonar-og-meldingar/stortingsmeldingar/2012-2013/meld-st-11-20122013/8.html?id=709834>

⁷ <http://www.psychometrics.cam.ac.uk/page/255/mypersonality.htm>

problem er at det er vanskelig for brukeren å ha oversikt over hvem som overvåker hvor du befinner deg.

Facebooks nye søkemotor Graph Search har som mål å gjøre all personlig informasjon søkbar, og blir fremstilt som en helt ny måte å tenke både søk og sosialt nettverk på. Ideen er å gjøre søk personlig og sosialt. Istedenfor generiske googlesøk kan du søke på restauranter vennene dine liker eller hvilke damer som er single i ditt nabolag. Sosiale søk gjør bilder og annen personlig informasjon mer tilgjengelig for andre.⁸

Flurry is Big Data: App-analyseselskapet Flurry har gjort Big Data til Big Business ved å tilby informasjon om app-brukere til annonsører. Selskapet har 80 000 kunder, finnes inne i 230 000 apper og når 700 000 mobiler og nettbrett i måneden.⁹ App-brukerne er ofte uvitende om at lommelykt-appen eller Angry Birds-spillet samler inn personlig informasjon om alt fra hvor mobilen befinner seg til navnene på adresselisten og mobilbilder.

HAR VI KONTROLL PÅ EGEN INFORMASJON?

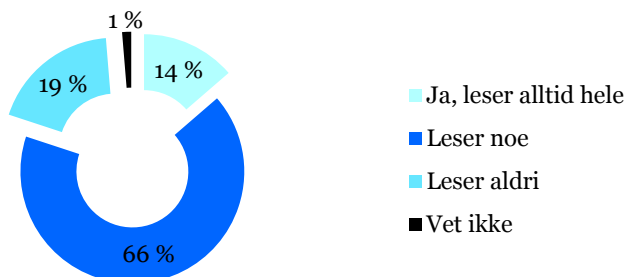
Tradisjonelt har offentlige registre og foretak som behandler persondata vært ansett som de største truslene for personvernet. I dag står nettbrukeren selv høyt opp på lista over personverntrusler når det kommer til deling av sensitiv personinformasjon. Det har blitt sosialt akseptert å dele detaljert personlig informasjon på nett og det er nettopp deling av personlig informasjon forretningsmodellen til de sosiale nettjenestene bygger på.

Når du oppretter en profil på et sosialt nettsamfunn eller laster ned en sosial app, må du ofte akseptere vilkår eller avtaler. Teksten i avtalene er ofte lange og kompliserte og de kan være vanskelige for brukeren å forholde seg til. Kun 14 prosent oppgir at de leser hele avtalen når de laster ned en app eller registrer seg hos et nettsamfunn. De eldste brukerne er flinkest til å sette seg inn i avtalen de går inn i – tre av ti sier de leser hele.

⁸ <http://www.wired.com/business/2013/01/the-inside-story-of-graph-search-facebooks-weapon-to-challenge-google/all/>

⁹ <http://www.flurry.com/big-data.html> og http://www.nytimes.com/2012/10/29/technology/mobile-apps-have-a-ravenous-ability-to-collect-personal-data.html?_r=0

Pleier du å lese avtalevilkårene når du oppretter en profil hos et nettsamfunn eller laster ned en app?



I praksis har brukeren liten eller ingen kontroll over hvordan tilbyderne benytter personopplysninger som brukeren gir fra seg. En ting er hva som står i vilkårene (som for øvrig ofte endres underveis), en annen ting er hva som skjer i praksis. Hva skjer hvis tjenesten blir solgt til en annen aktør, eller hvis det oppstår et sikkerhetsbrudd (personopplysninger lekker ut eller noen bryter seg inn i systemet)?

Du er din egen redaktør. Rådgivningstjenesten Slettmeg.no kan, så langt mulig, hjelpe til med å få fjernet uønsket personinformasjon på nettet. Tjenesten er populær og hadde i 2012 rundt 1,5 millioner sidevisninger på nett og 6977 henvendelser. En fjerdedel av henvendelsene gjelder Facebook. Mange av henvendelsene gjelder informasjon lagt ut av brukeren selv. Det er de yngste brukerne i alderen 16-25 år som henvender seg oftest til Slettmeg.no.

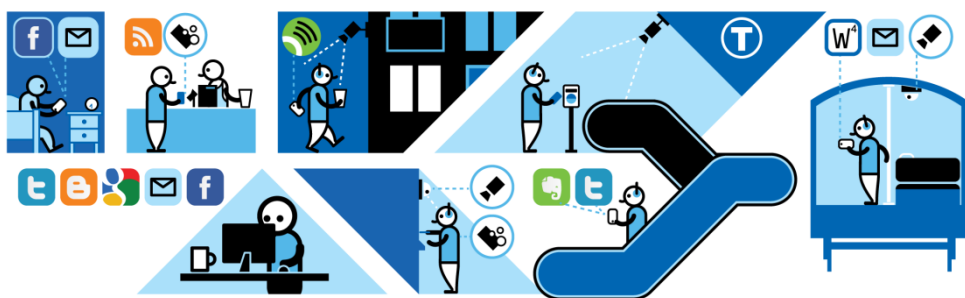
INNEBYGD PERSONVERN

Personvern skal være en del av alle ledd i utviklingen og bruken av informasjonsteknologi – det er tanken bak begrepet innebygd personvern. Det er ikke bare det tekniske systemet som skal ta ivareta personvernet, det er også en måte å tenke på og bør være en bevisst del av verdigrunnlaget til de sosiale nettjenestene. Personlig informasjon er valutaen til selskapene bak nettsamfunn, og det er ikke tilfeldig at ”dele åpent på nett” ofte er standard personverninnstilling – et eksempel på manglende innebygd personvern.

Snapchat er den raskest voksende bildeappen etter Instagram, og er et paradoksalt eksempel på innebygd personvern. Tjenesten tilbyr brukere å sende bildemeldinger til hverandre. Det som skiller Snapchat fra andre bildemeldingstjenester er at bildet slettes ett til ti sekunder etter at mottakeren har åpnet bildet.

Selve formålet med appen er å gi brukeren bedre kontroll over egne bilder. Men konsekvensen er at brukerne, som i hovedsak er ungdom, sender mer utfordrende innhold. Hadde det ikke vært for at de selv kan bestemme hvor mange sekunder mottakeren kan se bildet, ville de i mange tilfeller ikke ha sendt bildet i det hele tatt. Det er registrert flere tilfeller av digital mobbing i forbindelse med bruk av Snapchat. Snapchat-eksemplet minner oss på at godt personverndesign er viktig, men at det viktigste personvernfilteret sitter inne i hodet.

EN HALE AV ELEKTRONISKE SPOR



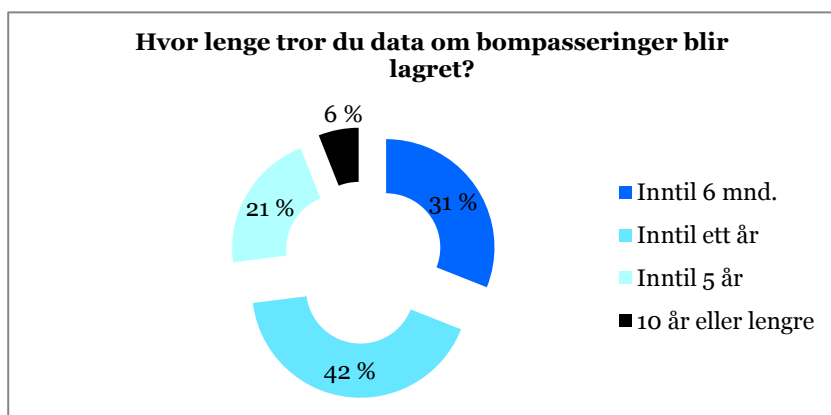
Hvilke elektroniske spor legger vi igjen på en vanlig dag på farten, fra hjem til jobb og henting i barnehage? Når vi kjører bil, reiser kollektivt eller går gate- langs – hele tiden med telefonen i lomma – legger vi igjen en hale av elektro- niske spor. Det er vanskelig å holde oversikt over alle systemene som registre- rer vårt bevegelsesmønster.

HVA SKJER?

REGISTRERINGSPUNKTENE KOMMER TETTERE

Det er i dag 165 bomstasjoner i Norge. Det er en økning på 33 prosent på ti år. Det er planlagt 37 nye bomstasjoner i løpet av de neste fem årene. Åtte av disse kommer i 2013.¹⁰ Mellom Oslo og Hamar står bomstasjonene så tett at det er mulig å avlese nøyaktig kjøremønster til den enkelte bilist.

I Norge brukes Autopass-brikken som automatisk registrerer bompasseringer. Det finnes i dag ikke et fullverdig anonymt alternativ til Autopass. Passeringsdata lagres i bomstasjonene i ti år i henhold til bokføringsloven. Folk flest er ikke kjent med at lagringstiden for disse opplysningene er så lang. Kun 6,2 prosent tror opplysningene lagres i ti år. Hele 42 prosent antar at opplysningene lagres i inntil ett år.¹¹



Antallet fotobokser har økt med 50 prosent siden 2000, og ligger i dag på 345 bokser. I tillegg finnes det 48 fotobokser på 23 ulike strekninger som utfører automatisk måling av gjennomsnittsfarten mellom to fotobokser.¹² Løsningen ble innført i 2009 og i motsetning til de vanlige fotoboksene som kun tar bilde av bilister som kjører for fort, registrerer dette systemet alle biler som passe-

¹⁰<http://www.vegvesen.no/Fag/Fokusomrader/Trafikksikkerhet/Automatisk+trafikk kontroll+ATK/R egionvise+oversikter> og korrespondanse med Statens Vegvesen, Vegdirektoratet, januar 2013.

¹¹ TNS Gallup for Teknologirådet og Datatilsynet januar 2013.

¹²<http://www.vegvesen.no/Fag/Fokusomrader/Trafikksikkerhet/Automatisk+trafikk kontroll+ATK/R egionvise+oversikter> og korrespondanse med Statens Vegvesen, Vegdirektoratet, januar 2013.

rer. Systemet er laget slik at ingen har mulighet til å se bildene av kjøretøy som har kjørt i lovlig hastighet.

USIKKERHET KNYTTET TIL LAGRING AV DATA I BILEN

Nye biler er rullende datamaskiner. En rekke bilmerker er utstyrt med det som populært omtales som "svarte bokser" eller adferdsgeneratorer (EDR). Disse boksene kan registrere opplysninger om kjøremønsteret ditt; blant annet hvor fort du kjører, hvor fort bilen akselererer, nedbremsingskraft, rattutslag, bruk av bilbelte, bruk av blinklys og bensinforbruk.

Formålet med lagring av dataene er blant annet å benytte dem til å diagnostisere eventuelle feil med bilen. Det er imidlertid flere uavklarte spørsmål knyttet til lagring, tilgang og bruk av disse opplysningene. Hvilke bilfabrikanter lagrer slike data? Hvilke data lagres og hvor lenge lagres de? Hvem har tilgang til dataene? Foruten bilforhandleren og verkstedet, har forsikringsselskaper tilgang til disse opplysningene? Hva med politiet i forbindelse med oppklaring av ulykker? Og hvem eier egentlig dataene som lagres i bilen, er det bilfabrikanten eller bileier? Hva skjer med de registrerte dataene ved for eksempel eierskifte?

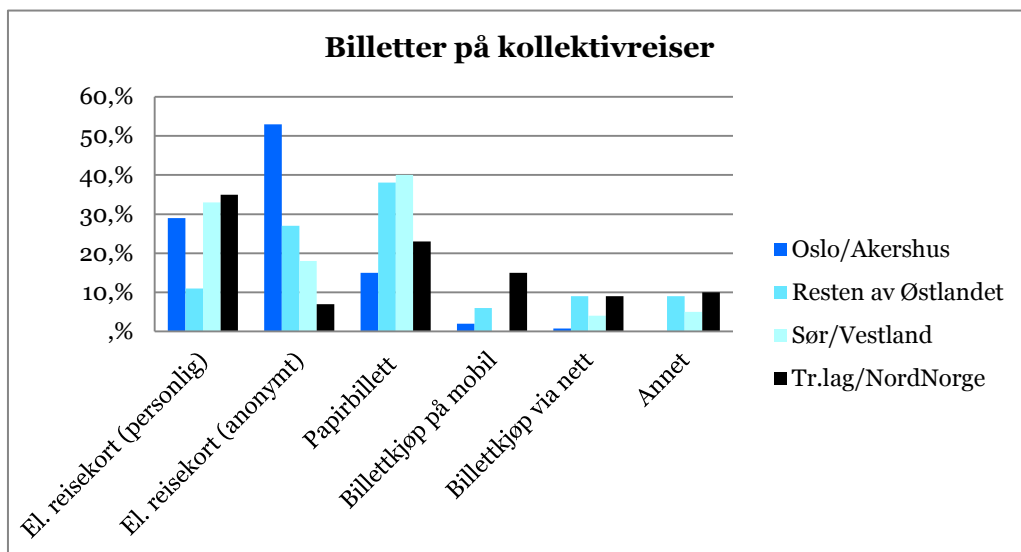
Tall fra vår undersøkelse viser at til sammen 70 prosent mener at det ikke lagres, eller at de ikke tror det lagres data om deres kjøremønster i bilen.

POSITIV UTVIKLING - ANONYME LØSNINGER I KOLLEKTIVTRANSPORTBRANSJEN

Papirbilletter er nå i ferd med å forsvinne. Ordningen med elektroniske reisekort teller 500 000 brukere over hele landet – og er i sterk økning. Enkelte steder har man også begynt å betale billetten med mobiltelefonen. Fra lanseringen i november 2011 har administrasjonsselskapet for kollektivtrafikk i Sør-Trøndelag solgt over to millioner billetter via app og SMS¹³. Ruter i Oslo avviker papirbilletten fra 1. mai i år og oppgir at mobilappen deres er lastet ned 300 000 ganger.

72 prosent av de spurte i undersøkelsen benytter som regel en elektronisk billettype når de reiser kollektivt. Det er imidlertid store geografiske forskjeller når det gjelder hvilken billettype som oppgis å være hyppigst i bruk.

¹³ Tall per 20. januar 2013 oppgitt fra markedssjef i AtB



I tillegg til opplysninger om kunden registrerer det personlige elektroniske reisekortet reiseopplysninger slik som startstasjon, varighet på reisen, retning og eventuelle merknader i forbindelse med billettkontroll. Analyse av folks reisemønster gjør det mulig for kollektivtransportsselskapene å foreta avregning mellom selskaper, planlegge og effektivisere driften av virksomheten ytterligere.

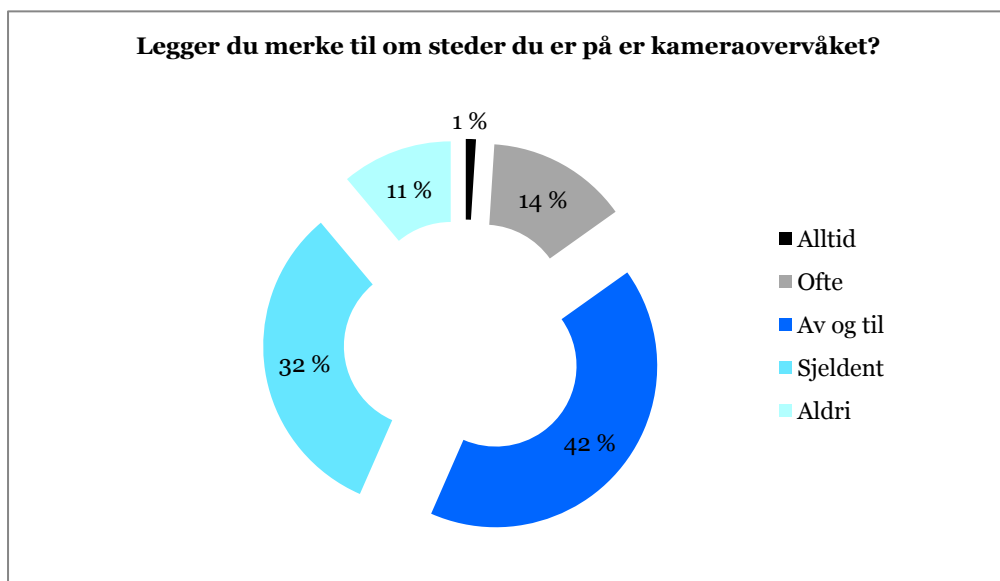
Kollektivtransportsselskapene og Datatilsynet har utarbeidet en bransjenorm for elektronisk billettering. Dette ble gjort etter at det ved tilsyn ble oppdaget at e-billetter førte til omfattende registreringer av reisedata på enkeltpersoner, samt at slike data ble lagret unødvendig lenge. Normen forplikter hele bransjen til å tilby e-billetter som gir godt personvern for de som reiser. Det betyr at alle trafikanter skal kunne reise kollektivt uten å oppgi hvem eller hvor de er, og samtidig få de samme fordelene og servicen som trafikanter som har personlige avtaler med et transportselskap.

ØKNING I OMFANGET AV PRIVAT KAMERAOVERVÅKING

De siste årene har det vært en jevn utvikling i omfanget av kameraovervåking. Det har vært en økning på 33 prosent i antall meldinger om kameraovervåking til Datatilsynets meldingsdatabase de siste fire årene. Med erfaring fra områdedekontroller er det imidlertid kun én av fem som melder inn kameraovervå-

king til tilsynet. Tar vi hensyn til dette, har vi estimert at antallet aktører som har kameraovervåking er over 20 000 pr januar 2013.

Økningen i bruken av overvåkningskameraer skyldes blant annet at teknologien har blitt rimeligere og mer brukervennlig. Teknologien er ikke lenger kun forbeholdt profesjonelle aktører. Folk har begynt å sette opp kameraer til formål som ikke har noe med sikkerhet og trygghet å gjøre.



I undersøkelsen oppgir kun 15 prosent av de spurte at kameraovervåking er noe de alltid eller ofte legger merke til. 44 prosent legger sjelden eller aldri legger merke til dette.¹⁴

BESKJEDEN BRUK AV KAMERAOVERVÅKING I OFFENTLIG REGI

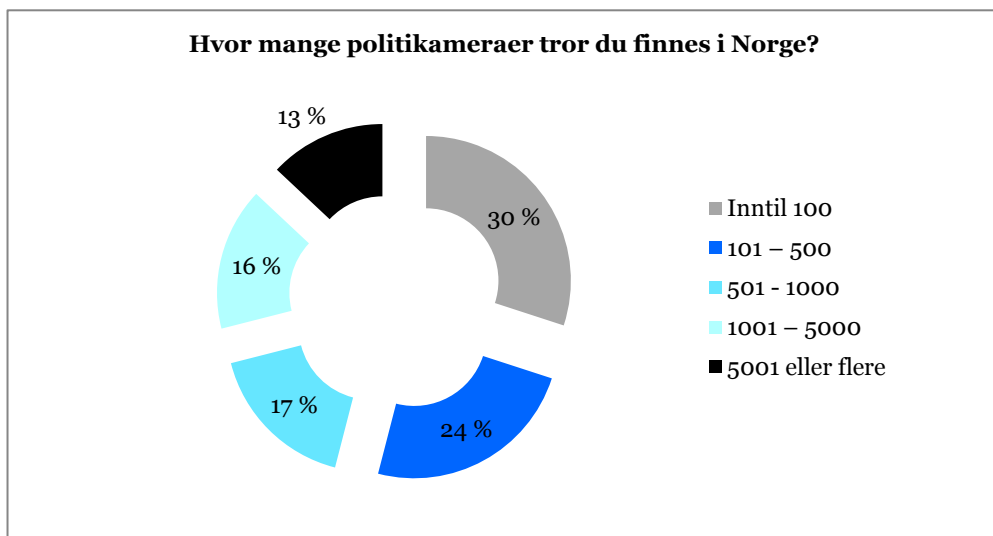
Politiet har i svært beskjeden grad tatt dette virkemiddelet i bruk. Kun tolv kameraer er utplassert av politiet i norske byer og tettsteder: seks i Oslo, tre i Hamar og tre i Stavanger. I Storbritannia, kjent som verdens kanskje mest kameraovervåkede land, har politiet til sammenligning plassert ut over 12 000 kameraer bare i London¹⁵. I Norge har myndighetene gått motsatt vei – kame-

¹⁴ TNS Gallup for Teknologirådet og Datatilsynet januar 2013.

¹⁵ <http://content.met.police.uk/Article/Met-Command-and-Control/1400005435512/1400005435512>

raer blir tatt ned. Blant annet valgte politiet i Trondheim å ta ned overvåkingskameraet utplassert i byens sentrale handlegate etter at testperioden var over.

Tall fra undersøkelsen viser at folk generelt tror at politiet benytter kameraovervåking i langt større utstrekning enn hva som er tilfelle. Nesten 30 prosent av de spurte tror politiet har satt opp over 1000 kameraer. Til sammen 70 prosent tror det må være over 100 kameraer.¹⁶



MED SENSOR I LOMMA

Når du bruker telefonen blir opplysninger om hvor du befinner deg lagret. 67 prosent av oss går aldri hjemmefra uten å ha telefon med¹⁷. I norske tettsteder står mastene som henter inn lokasjonsdata så tett at de kan registrere svært nøyaktige opplysninger om hvor du befinner deg. Noen teleleverandører lagrer denne typen opplysninger i tre måneder av faktureringsgrunner.

I tillegg er det, hvis du har en smarttelefon og er bruker av apper, også andre aktører som henter ut personopplysninger fra telefonen din. Dette kan være opplysninger om for eksempel ditt vennennettverk, dine vaner, preferanser og

¹⁶ TNS Gallup for Teknologirådet og Datatilsynet januar 2013.

¹⁷ http://services.google.com/fh/files/blogs/our_mobile_planet_norway_no.pdf

interesser og om du skal til legen denne uken hvis du har notert det i kalenderen. Mobilprodusenter, operativsystemleverandører, app-eiere, sosiale nett-samfunn og ulike analyse- og markedsføringsselskap er blant mottakerne av slike opplysninger¹⁸. En undersøkelse utført av Datatilsynet, viste at ingen av de 20 norske mobilapplikasjonene som ble undersøkt informerte brukeren på en tilfredsstillende måte om hvilke personopplysninger som ble hentet inn.

Vet hvor du er. En av Datatilsynets ansatte ba om å få utlevert alle lagrede trafikkdata hos Telenor. Vedkommende er smarttelefonbruker med et moderat telefonforbruk. Konvolutten som vedkommende fikk tilsendt inneholdt 42 sider med data lagret over en periode på tre måneder. I gjennomsnitt ble det lagret opplysninger fra telefonen 30 ganger i døgnet, av disse utgjorde lokasjonsdata omtrent en tredjedel. De andre opplysningene var knyttet til datatrafikk i forbindelse med bruk av apper og Internett.

PERSONVERNUTFORDRINGEN

VALGFRIHET UNDER PRESS

– UTVIKLING I RETNING AV OBLIGATORISKE LØSNINGER

Suget etter data er enormt. Data gir kunnskap som kan bidra til økt effektivitet og lønnsomhet. Hensynet til sikkerhet og miljø fungerer også som sterke drivere for innføring av nye systemer. Vi ser en utvikling der obligatoriske løsninger blir standard, særlig i samferdselssektoren.

eCall vil for eksempel bli pålagt installert i alle biler i Norge og EU fra og med 2015. eCall er en alarmtjeneste for bilulykker i Europa. Tjenesten skal virke slik at en kommunikasjonsenhet i bilen automatisk ringer nødnummeret og oppgir bilens posisjon i tilfelle ulykke. Det er fortsatt diskusjon om systemet skal være kontinuerlig aktivert, eller om det skal være mulig å skru av via en "av og på"-knapp.

Autopass kan bli obligatorisk for tungtransportkjøretøy. Pålegg om bruk av Autopass-brikke i privatbiler vil trolig også komme da dette vil forenkle innkreving av bompenger. Det foreligger ønsker om å bruke opplysningene til for eksempel trafikkplanlegging for å redusere bilforurensingen.

¹⁸ Datatilsynets rapport om mobile applikasjoner "Hva vet appen om deg?"

Fra et personvernståsted bør loydlige bilister ha adgang til å bruke veinettet uten å bli registrert. Frivillighet er derfor viktig – at hver og en skal ha mulighet til selv å bestemme om man som bilist, fotgjenger eller kollektivreisende skal overvåkes. I dag er dette ikke alltid tilfelle.

ATTRAKTIVE OPPLYSNINGER – BRUK TIL NYE FORMÅL

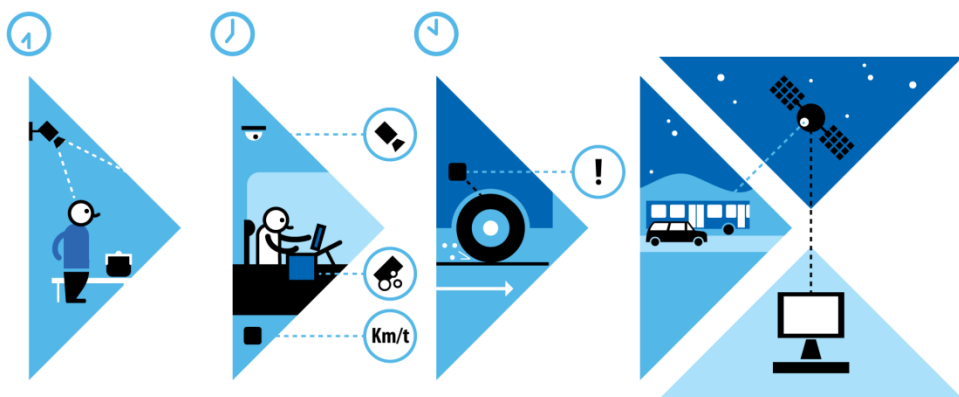
Opplysninger om vårt bevegelsesmønster forteller mye om oss. Opplysningene er attraktive for mange ulike aktører. På den ene siden kan det være virksomheter som ønsker å selge oss en tjeneste eller å forbedre sitt produkt. På den andre siden kan det være myndighetene som ønsker tilgang til slike data for å kontrollere at vi ikke bryter loven eller misbruker felles samfunnsgoder. Det kan gi grunn til bekymring at mer omfattende lagring av elektroniske spor bidrar til at bevisbyrden ovenfor myndighetene på sett og vis snur. Siden sporene allerede ligger der, blir det den registrerte som må sannsynliggjøre sin uskyld.

Datatilsynet ser stadig vekk eksempler på at personopplysninger innsamlet for ett formål senere vil bli forsøkt benyttet til andre formål. eCall-systemet vil for eksempel bli kostbart. Det er ikke utenkelig at kostnadene vil bli forsøkt dekket ved å gi andre aktører tilgang til posisjonsdata og andre opplysninger fra systemet, for eksempel kommersielle virksomheter eller forsikringsselskaper. Man kan også se for seg tjenester som reklame, vei- og værmeldinger etc. Gjøres Autopass-brikken obligatorisk er det flere aktører som vil ha stor interesse av å benytte denne. Det kan være alt fra parkeringshus, bensinstasjoner, drive-in hurtigmatbutikker med videre. Myndighetene kan også ha interesse av å benytte opplysninger som ligger lagret for andre formål enn det som opprinnelig var tiltenkt. Skattemyndighetene ønsker for eksempel tilgang til passeringsdata i bomringene for kontrollformål.

MANGEL PÅ INFORMASJON OG KONTROLL

Et generelt problem er at det informeres for dårlig om hvilke personopplysninger som samles inn og hva de brukes til. Undersøkelsen vår viser for eksempel at folk flest ikke har kjennskap til, eller kunnskap om, *hvilke* opplysninger som lagres og *hvor lenge* de lagres. Mangel på informasjon og oversikt gjør det vanskelig for den enkelte å praktisere sine grunnleggende personvernrettigheter.

ET SPORBART ARBEIDSLIV

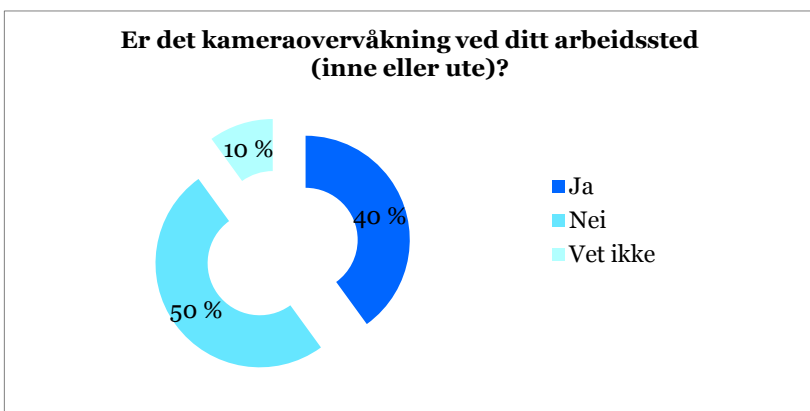


Det har vært en betydelig økning i registrering av personopplysninger i arbeidslivet de siste årene. Utbredelsen av teknologi som muliggjør overvåking og kontroll av ansatte har økt kraftig. Datatilsynet mottar mange spørsmål relatert til arbeidsliv fra publikum. I 2012 utgjorde arbeidslivsspørsmål 15 prosent av den totale mengden med epost-henvendelser til tilsynet. Henvendelsene er hovedsakelig konsentrert om temaene GPS, kameraovervåking, ulike kontrolltiltak, innsyn i e-post, personalmapper og lydopptak.

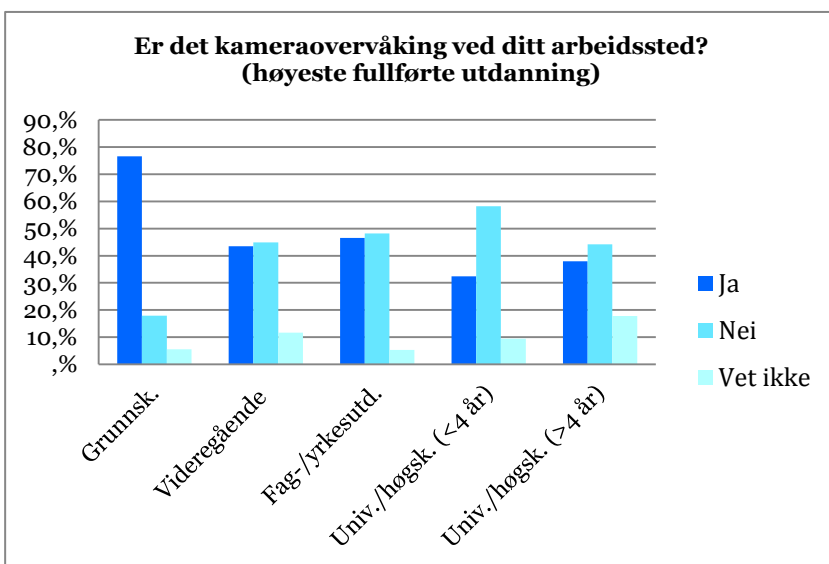
HVA SKJER?

MER KAMERAOVERVÅKING PÅ ARBEIDSPLASSEN

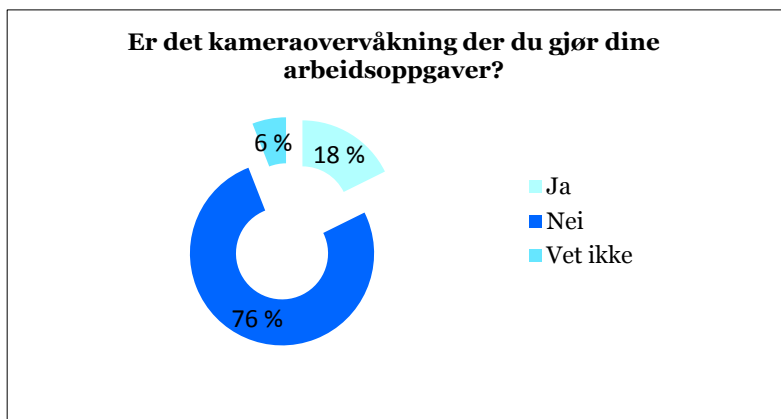
Kameraer har blitt billigere og mindre, og dermed mer tilgjengelige for bruk i arbeidslivet. 40 prosent av de spurte i undersøkelsen oppgir at det er kameraovervåking i eller utenfor arbeidsstedet deres.



Svarene i undersøkelsen indikerer imidlertid at det er store forskjeller avhengig av respondentenes utdanningsnivå. Hele 77 prosent av de med grunnskole som høyeste fullførte utdanning svarer at arbeidsstedet er kameraovervåket. Tilsvarende tall for dem med høyere utdanning er henholdsvis 32 og 38 prosent.



I undersøkelsen spurte vi videre om selve stedet der folk *utførte sine arbeidsoppgaver* ble kameraovervåket. 18 prosent, nesten to av ti, svarer bekreftende på dette¹⁹. I en spørreundersøkelse i regi av Forskningsstiftelsen FAFO fra 2010, svarte 70 prosent av de spurte at de var negative til kameraovervåking av ansatte i arbeidssituasjonen²⁰.

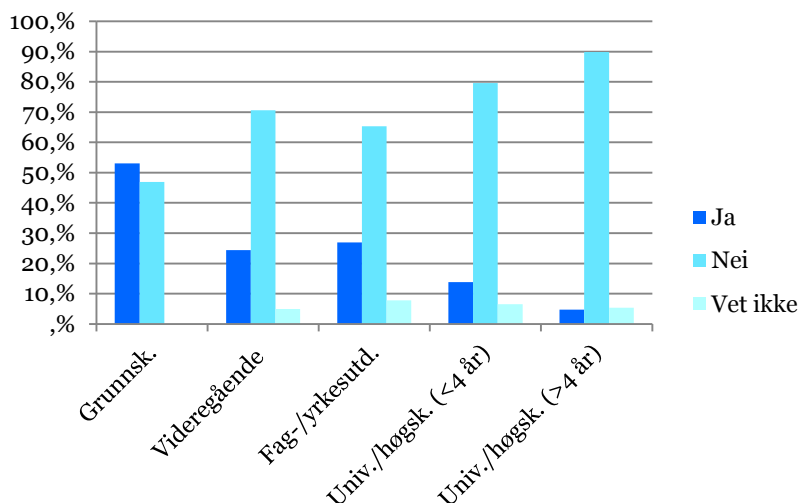


I likhet med det første spørsmålet om kameraovervåking, er det store forskjeller mellom dem med lav og høy utdanning. Over halvparten, 53 prosent, av de med grunnskole som høyeste utdanning oppgir at de er kameraovervåket der de utfører sine arbeidsoppgaver. Dette kan inkludere arbeidsplasser som butikker, kafeer og bensinstasjoner. Dette er arbeidsplasser som tradisjonelt ansetter mange ufaglærte og ungdommer. Tillitsnivået mellom ansatte og ledelse kan være lavere her enn ved arbeidsplasser som primært ansetter folk med høy utdanning. En del av de mer kameraovervåkede arbeidsplassene er nok også mer risikofylte, for eksempel for ran og tyveri. Kun fem prosent av de med syvårig høyere utdanning svarer at stedet der de utfører sine arbeidsoppgaver er kameraovervåket.

¹⁹ Til sammenligning svarte ni prosent at de var kameraovervåket der de arbeidet i en undersøkelse i regi av FAFO fra 2010. (*Kontroll og overvåking i arbeidslivet*, Mona Bråten, FAFO 2010)

²⁰ *Kontroll og overvåking i arbeidslivet*, Mona Bråten, FAFO 2010

Er det kameraovervåking der du utfører dine arbeidsoppgaver? (høyeste fullførte utdanning)



Datatilsynet behandler flere tilfeller av ulovlig kameraovervåking hvert år.

I januar 2013 ble det avslørt at ansatte ved Norsk Kyllings kontor på Lillehammer hadde blitt ulovlig kameraovervåket over lengre tid. Da pauserommet til Norsk Kylling skulle pusses opp, fant de et skjult kamera bak en list. Bildene ble sendt til to av sjefenes telefoner. Forholdet er, av den nåværende ledelsen, meldt til politiet.

I 2010 avslørte Datatilsynet skjult kameraovervåking av de ansatte hos United Bakeries på Majorstua i Oslo. Kameraene var gjemt i to røykvarslere. Bedriften fikk et overtredelsesgebyr på 40 000 kroner.

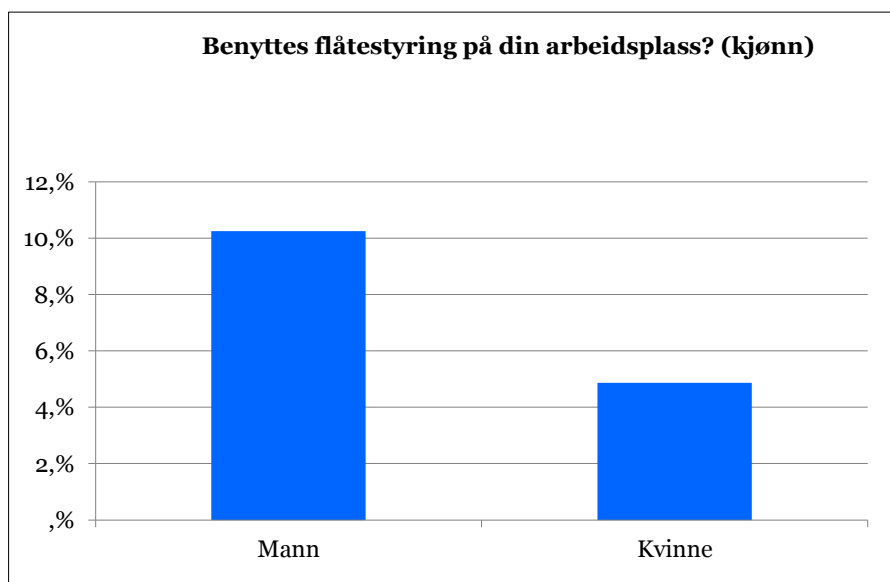
En pub i Hønefoss fikk i 2011 et overtredelsesgebyr på 30 000 kroner for å ha overvåket toalettgjestene ved å skjule kamera i røykvarsleren.

Ved Horten Næringspark Hotell i Horten gjorde man lyd og bildeopptak av gjester og ansatte. Saken ble avdekket i 2011, men overvåkingen skal ha pågått i flere år. Saken var så alvorlig at Datatilsynet meldte saken til politiet.

FJERNSTYRT ARBEIDSDAG

Bruk av flåtestyring har endret arbeidshverdagen i mange yrkesgrupper. Med flåtestyring menes en elektronisk innretning som muliggjør at arbeidsgiveren kan spore bevegelsene til virksomhetens kjøretøy. Arbeidstakere som før utførte sine arbeidsoppgaver relativt fritt ”ute i felten” kan nå bli fulgt i detalj av arbeidsgiver. Av de spurte i undersøkelsen svarer åtte prosent at det benyttes et system for flåtestyring på arbeidsplassen.

Undersøkelsen viser at menn er i et klart flertall blant de som har flåtestyring på arbeidsplassen. En av ti menn i undersøkelsen svarer at flåtestyring benyttes på deres arbeidssted. Flåtestyring er som oftest knyttet til kjøretøy og maskiner.



Datatilsynet har vært med bussjåfør "Vidar" på jobben for å få et inntrykk av hvordan arbeidsdagen hans loggføres. Vidar jobber for et rutebusselskap i en stor norsk kommune og yrket har forandret seg mye siden han startet for 15 år siden. Fra å ha en relativt autonom arbeidsdag har presset på å holde ruten blitt større, og omfanget av registreringer er langt mer omfattende.

Seks ulike elektroniske system registrerer detaljerte opplysninger om Vidars arbeidsutførelse i løpet arbeidsdagen. Kamera i garderoben fanger opp når han kommer og går for dagen. Vidar registrerer seg for dagens rute med oppmøtebrikken. I selve bussen overvåkes Vidar av sanntidssystemet, fartsskriveren, kjøretøycomputeren, billettsystemet og overvåkingskameraet. Kameraet i bussen slås automatisk på ved oppstart av bussen. Fartsskriveren registrerer hvor lenge Vidar kjører og hvor lenge han har pauser. I tillegg har fartsskriveren GPS-funksjonalitet som logger opplysninger om bussens lokasjon gjennom dagen. Kjøretøycomputeren registrerer alle operasjoner Vidar utfører med bussen: hvor fort bussen kjører, posisjon og bevegelse, kraften i oppbremsning og akselerasjon, åpning og lukking av dører, blinklys, dieselforbruk og tomgangskjøring med mer. Billettsystemet registrerer antall solgte billetter og tidspunkt for salg. Når han begynner på ruta logger Vidar på "sanntidssystemet". Dette er et GPS-basert system som beregner bussens ankomsttid til en stasjon. Systemet benyttes også som et flåtestyringssystem av busselskapet; busser som ikke går etter ruta kan kalles opp.

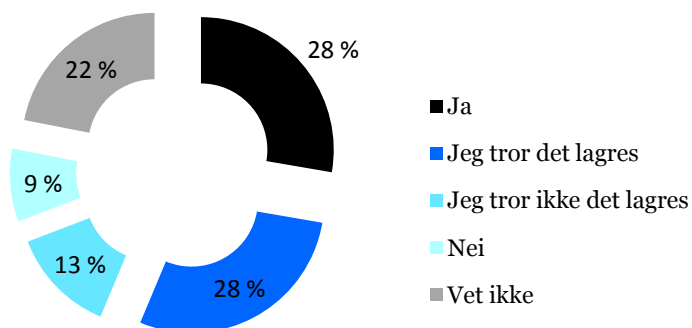
PERSONVERNUTFORDRINGEN

DÅRLIG KJENNSKAP TIL LAGRINGSRUTINER FOR PERSONOPPLYSNINGER

Det er en utfordring at det er vanskelig for arbeidstakerne å holde oversikt over hvilke personopplysninger som behandles om dem. Det er ofte flere ulike systemer som registrerer opplysninger. Det er heller ikke alltid opplagt hva som registreres, eller om det registreres noe i det hele tatt. Et eksempel på dette er når man drar adgangskortet eller surfer på Internett. Arbeidstakeren kan ikke selv se de elektroniske sporene og det kan da være vanskelig å få oversikt over hvilke opplysninger som registreres til hvilke formål, og hvem som har tilgang til opplysningene.

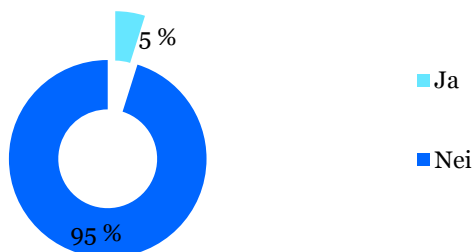
I undersøkelsen spurte vi om folk visste hvorvidt data ved bruk av nøkkelkortet på jobben ble lagret eller ikke. Et mindretall svarer klart ja eller nei på spørsmålet. Flertallet er usikre på om dette gjøres eller ikke.

Lagres data fra nøkkeltet/brikken din?



På spørsmål om de vet hvor lenge opplysningene fra nøkkeltet lagres, svarer hele 95 prosent at de ikke vet dette. Tallene illustrerer at arbeidstakere ofte har liten oversikt over hvilke data som lagres om dem, og hvor lenge de lagres.

Vet du hvor lenge opplysningene fra nøkkeltet lagres?



FUNCTION CREEP: BRUK AV OPPLYSNINGER TIL NYE FORMÅL

Datatilsynet har i et stort antall saker avdekket systematiske brudd på regelverkets krav om sletting, og at personopplysninger gjenbrukes til nye formål.

Lagring av data har blitt billigere, noe som fører til at det ofte er dyrere og mer ressurskrevende for virksomheten å etablere tilfredsstillende sletterrutiner, enn å lagre opplysningene videre.

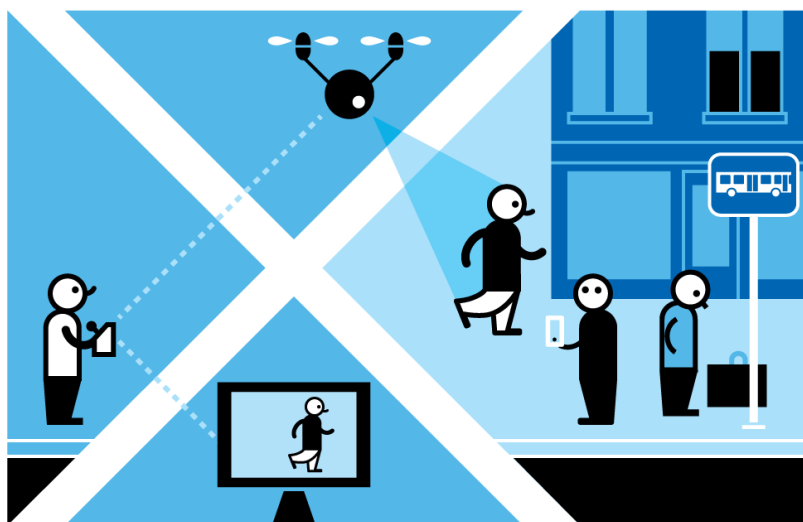
Ifølge personopplysningsloven skal personopplysninger ikke lagres lenger enn nødvendig for å gjennomføre formålet med behandlingen. Ofte argumenteres det med at man ønsker å oppbevare opplysningene fordi de kan komme til nytte senere, uten at man nødvendigvis har klart for seg hva man senere skal benytte opplysningene til. I tillegg til at manglende sletting som regel vil være et brudd på personopplysningsloven, øker det også faren for at opplysningene senere kan brukes til andre formål som er uforenlig med det opprinnelige.

For lange pauser. Det offentlig eide selskapet Avfallsservice i Nord-Troms ga i 2010 en av sine medarbeidere sparken. Årsaken var at han ifølge arbeidsgiveren hadde tatt for lange pauser, og så skrevet overtid. Avfallsservice hadde et GPS-system som de brukte for å sjekke om dunker var tømt eller ei. Det samme systemet brukte de til å sjekke opp mot timelistene til vedkommende.

Arbeidstakeren nektet for å ha tatt for lange pauser, og gikk til rettssak med støtte fra fagforeningen. De mente at dette var ulovlig overvåking, og at de ansatte ikke var tilstrekkelig informert om at arbeidsgiveren ville bruke denne metoden. De mente også at retten ikke skulle kunne bruke informasjonen fra GPS-overvåkingen som bevis i arbeidsrettssaken.

I sin kjennelse konkluderte Hålogaland lagmannsrett med at GPS-datatene kunne fremføres som bevis selv om de var innhentet i strid med personopplysningsloven.

DRONER TAR AV



Du kan ha den i lomma, den veier 16 gram, er utstyrt med tre kameraer, har autopilot med fullt GPS-system, samt en aksjonsradius på opptil 1000 meter. Dronen «Black Hornet» er utviklet av det norske selskapet Prox Dynamics. Den har foreløpig kun vært brukt av militæret, men en sivil versjon er nå snart klar.

Dronene er på vei inn i vår hverdag. Prisene daler, dronene blir bedre, mindre og flyr lengre. Må personvernet ofres for de store mulighetene dronene gir?

HVA ER DRONER?

Felles for dronene er at de er ubemannede. De kan utstyres med mange typer sensorer: Kameraer som kan se detaljer på langt hold, nattsyn, sensorer som kan lytte, lukte, måle, og kjenne igjen ansikter og andre fysiske kjennetegn. Rekkevidden blir stadig bedre, og dronene kan være svært små, slik at de blir vanskelige å oppdage fra bakken.

FRA KRIG TIL SIVIL BRUK

Droner assosieres ofte med krigføring og militære operasjoner. Nå inntar drone-teknologien imidlertid også det sivile luftrommet, med helt nye bruksområder. Uten våpen, men med kameraer og sensorer. Dronene er allerede tatt i bruk på en rekke områder i Norge, for eksempel i forskning og klimaovervåkning. Samtidig ser både politi, redningstjeneste, og media på dem med stor interesse. Flere politidistrikter har allerede eksperimentert med droner. Scenariene varierer fra overvåking av mistenkte i nattemørket, til leting etter savnede.

PILENE PEKER OPPOVER

Det foregår nå et intensjonalt markedskappløp om å utvikle dronenes kommersielle potensial i sivil bruk. Amerikanske luftfartsmyndigheter anslår at rundt 30 000 sivile droner vil være i luften i løpet av det neste tiåret.²¹ For Europa anslår EU-kommisjonen at det vil være mellom 30 og 40 000 operative droner i Europa på samme tid. Det globale markedet anslås å være på 90 milliarder dollar i samme periode. I USA skal nye regler som åpner for kommersiell bruk av droner være på plass i 2015²². EU ønsker å gjøre det samme året etter²³.

Den kraftige veksten i antall droner har også sammenheng med kraftig reduserte kostnader, som kommer av utviklingen innen sensorer og kontroller, datalink-løsninger og databehandling. Amatører med en smarttelefon kan nå enkelt eie og drive en drone med kamera. En Parrot AR.Drone Quadcopter, kan kjøpes av hvem som helst og koster ca. 2 000 kroner.

²¹ <http://www.washingtontimes.com/news/2012/feb/7/coming-to-a-sky-near-you/>

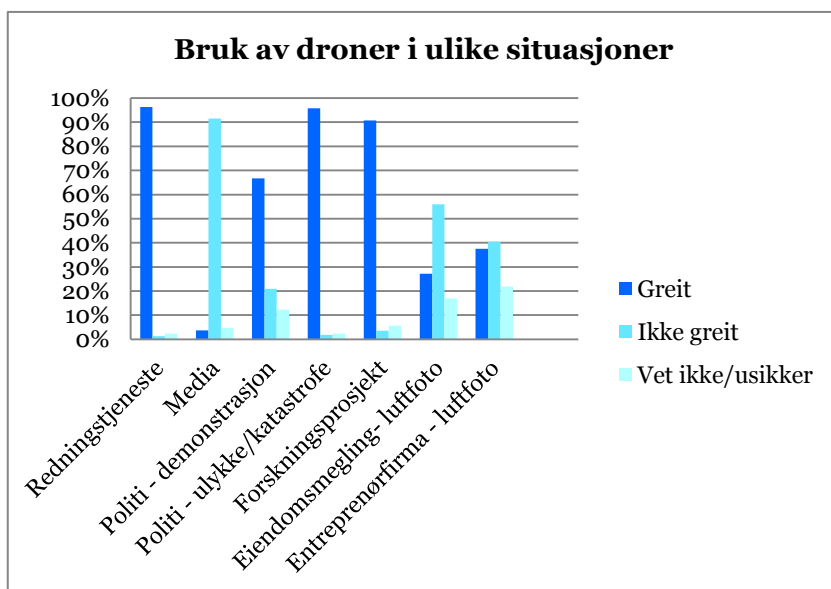
²² <http://go.bloomberg.com/political-capital/2012-11-26/faa-going-slow-on-drones-as-privacy-concerns-studied/>

²³ http://www.luftfartstilsynet.no/regelverk/Europeisk_regelverk/article6972.ece

I eiendomsbransjen er dronene allerede i bruk. Aeorovision AS og zMedia Systems er to ledende aktører som tilbyr luftfoto tatt av droner. Bedriftene forteller om stor etterspørsel fra eiendoms- og entreprenørbransjen. Aeorovision AS tilbyr i dag fotografering og video av arrangementer fra luften. Det norske selskapet Zovenfra hadde i løpet av 2012 i overkant av 1 200 oppdrag. I tillegg til luftfoto av private- og næringsbygg tilbyr de bildedokumentasjon av utbyggingsprosjekter over tid. Bildene brukes til utvikling av 3D-modeller og som kontrollverktøy for prosjektledere. Zovenifra planlegger også å lansere HD video i løpet av våren 2013.²⁴

FOLKET VIL HA DRONER – SÅ LENGE DE IKKE ER KOMMERSIELLE

Vi har spurt et representativt utvalg nordmenn om hva de mener om bruk av droner i ulike situasjoner. Akkurat nå, før det er tatt i bruk av offentlige aktører i større grad, ser vi en klart positiv holdning til bruk av droner i politi og redning. Over 90 prosent synes slik bruk er greit, men synker noe for politiet når det gjelder bruk av droner til å overvåke folkemengder ved demonstrasjoner. Undersøkelsen gir negative tall for bruk av droner i bransjer som eiendomsmegling og media. Dette er i dag de bransjene som faktisk tar i bruk droner i stor grad. Hvorfor er folk mot bruk av droner i disse bransjene? En tanke kan være frykten for at slik bruk ikke rettferdiggjør trusselen mot personvernet.



²⁴ <http://www.aerovision.no/>, www.zovenfra.no

PERSONVERNUTFORDRINGEN

Droner er en ny teknologiplattform som gjør at terskelen for overvåkning fra lufta blir dramatisk senket, samtidig som det utvikles stadig kraftigere kameratelelinser, bedre nattsyn og mer sofistikert videoanalyse. Dronenes enorme mobilitet, mengden av sensorer de kan utstyres med, samt økningen i sivil bruk, representerer en potensiell utfordring for personvernet.

I USA er denne debatten allerede varm. Våren 2012 ble en ambisiøs plan for å tillate sivil bruk av droner ført hurtig gjennom den amerikanske kongressen og sporenstreks signert av president Obama. I tillegg til å pålegge luftfartstilsynet (FAA) å ha de generelle reguleringene på plass innen 2015, ble det bestemt en liberal praksis for forskning og ikke minst at luftrommet skulle åpnes for politidroner innen 60 dager etter vedtaket. I etterkant har imidlertid mange borgerrettsorganisasjoner reagert, og personvernet blitt et viktig tema. I en rapport fra den amerikanske riksrevisjonen (GAO) etterlyses rammer for overvåkning, datainnsamling og -behandling fra myndighetenes side²⁵.

Også i Norge er bruk av droner primært regulert av luftfartsmyndighetene. Det er ikke lov å filme eller fotograferer fra luften uten tillatelse fra Nasjonal Sikkerhetsmyndighet (NSM). Men NSMs formål er hovedsakelig å skjerme områder og bygg som ikke skal fotograferes av hensyn til nasjonal sikkerhet, og dermed ikke av hensyn til personvernet.

Kameraovervåking av personer som kan gjenkjennes er et inngrep i personvernet, og er i Norge regulert gjennom personopplysningsloven. I 2012 ble imidlertid lovteksten om kameraovervåking oppdatert. Blant annet ble ordet "fastmontert" introdusert i definisjonen av hva som defineres som kameraovervåking: "Med kameraovervåking menes vedvarende eller regelmessig gjentatt personovervåking ved hjelp av fjernbetjent eller automatisk virkende overvåkningskamera eller annet lignende utstyr som er fastmontert.» Dette innebærer at håndholdte kameraer ikke defineres som kameraovervåking i personopplysningsloven.²⁶

^{25a} <http://markey.house.gov/press-release/markey-barton-ask-faa-details-drones-who%E2%80%99s-using-them-public-airspace-how%E2%80%99s-privacy>

^b <http://go.bloomberg.com/political-capital/2012-11-26/faa-going-slow-on-drones-as-privacy-concerns-studied/> og <http://www.gao.gov/products/GAO-12-889T>

²⁶ <http://www.lovdatab.no/ltavd1/hefter/ hele-1-2012-05.pdf>

Viktige spørsmål fremover vil være:

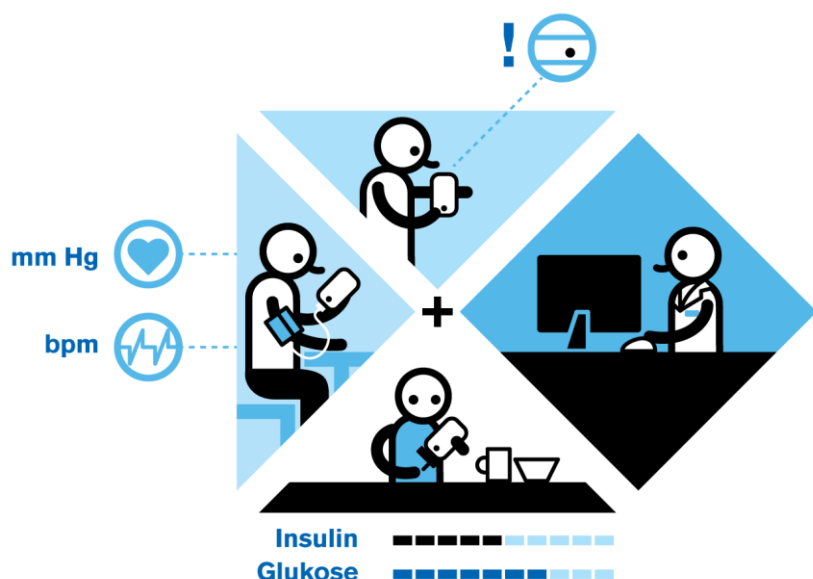
- I hvilke situasjoner skal droner kunne brukes? Når trenger politiet rettslig kjennelse?
- Hva er privat? Er for eksempel luftrommet over en hage privat?
- Er det innbrudd å fjernstyre en drone inne på andres eiendom?
- Kan politiet bruke droner for å innhente bilder av identifiserbare personer?
- Hva gjør man med overskuddsinformasjon – for eksempel dersom dronen filmer en mistenkelig hendelse på vei til et åsted?
- Hva og hvor lenge kan man lagre opptak fra dronen, og med hvem kan det deles?

Når det gjelder privat bruk, finnes det visse bestemmelser både i åndsverkloven (som regulerer midlertidig publisering, men ikke selve opptaket)²⁷, og i straffeloven som går på krenkelsen av privatlivets fred²⁸. Det spørs imidlertid om teknologien blir så tilgjengelig, rimelig og teknologisk fasinende, at mange nok vil la seg friste til å benytte kameraene til ulovlig overvåking, spionasje og «kikking».

²⁷ <http://www.lovdatab.no/all/tl-19610512-002-043.html>

²⁸ <http://www.regjeringen.no/nb/dep/jd/dok/regpubl/otprp/2008-2009/otprp-nr-22-2008-2009-/5/11.html?id=540403>

LEGEKONTOR PÅ INNERLOMMA



Du oppdager en mistenkelig føflekk. Du tar bilde av den med mobilkameraet²⁹ og sender det til automatisk analyse som vurderer om den faktisk er farlig. Heldigvis fikk du grønt lys i retur, som betyr at alt ser ut til å være i orden. Det var ikke gult eller rødt, da måtte du ha oppsøkt lege. Scenariet er ikke science fiction, men noe du allerede kan gjøre i dag. Stadig mer av legekontoret er nå mulig å få på mobilen.

²⁹ <https://skinvision.com>

HVA KAN VI GJØRE I DAG?

En kan i dag enkelt og rimelig kjøpe godkjent tilleggsutstyr til mobiltelefonen som kan gjøre medisinske målinger. For kronikere er dette gode nyheter som kan gjøre hverdagen enklere. Diabetikere kan kjøpe godkjente blodsuktermålere³⁰ som kontrollerer insulinbehovet. Folk med høyt blodtrykk kan kjøpe en blodtrykksmåler³¹.

Nylig godkjente amerikanske helsemyndigheter et deksel til smarttelefonen som måler hjerterytmen hver gang man tar i telefonen³². Folk med hjerteproblemer kan dermed enkelt observere egen tilstand.

Ved avvikende målinger kan måleresultatene sendes til legen for oppfølging. Man kan også se for seg at legen kontinuerlig overvåker målingene og kaller deg inn hvis nødvendig. Måleresultatene kan også sendes til pasientnettverk, sosiale nettverk eller medisinske eksperter ved private klinikker. Allerede har mange amerikanske selskaper etablert seg i dette markedet.

En ny trend er at disse ekspertene er maskiner, som IBMs superdatamaskin Watson, som kan diagnostisere resultatene og sette dem i sammenheng med andre resultater og siste nytt på forskningsfronten.

Slik snur digitaliseringen kombinert med mobiltelefon og ekstrautstyr helse-tjenestene på hodet. I USA og Europa jobbes det med å utvikle et rammeverk for både applikasjoner og sensorer³³. Food and Drug Administration (FDA) i USA har allerede godkjent en håndfull applikasjoner som oppfyller krav som stilles til "vanlig" medisinsk utstyr³⁴. Også EU-kommisjonen ser på helseapplikasjoner som et godt verktøy til selvhjelp for borgernes helse. De har nettopp publisert en europeisk oversikt over anbefalte helseapplikasjoner³⁵.

Eldrebolegen medfører at antallet nordmenn med kroniske sykdommer vil øke i årene som kommer. Med en befolkning helt i verdenstoppen på bruk av smarttelefoner, vil mobil helseteknologi kunne styrke forebygging, måling,

³⁰ <http://www.bgstar.com/web/ibgstar/app/app>

³¹ <http://www.withings.com/en/bloodpressuremonitor>

³² <http://www.drjohnm.org/2012/12/alivecor-iphone-ecg-transforms-heart-rhythm-monitoring/>

³³ <http://medicaldeviceslegal.com>

³⁴

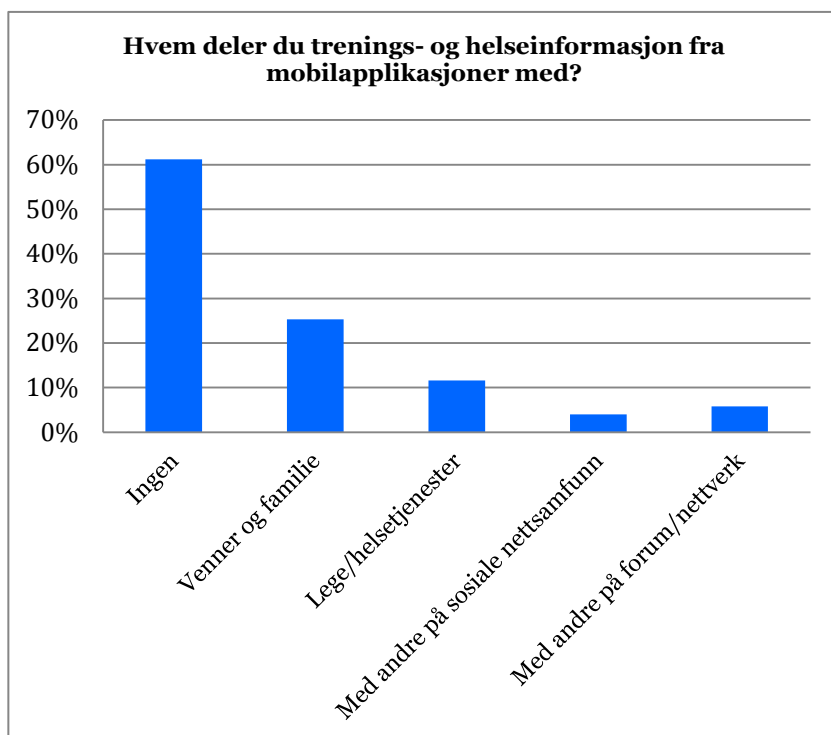
<http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/DeviceApprovalsandClearances/510kClearances/ucm330634.htm>

³⁵ <http://alturl.com/qd58y>

diagnostisering, behandling og kommunikasjon med helsesektoren. Det vil kunne spare tid, ressurser og liv.

PERSONVERNUTFORDRINGEN

Helseopplysninger er noe av den mest personsensitive vi har. Slike opplysninger er interessante for mange ulike kommersielle aktører, forsikringsselskaper og snokere. I Norge har vi lang tradisjon for at det offentlige samler helseopplysningene våre. I tillegg har det i stor grad vært helsetjenesten som har innhentet informasjonen og kontrollert og rasjonert med bruk av kostbar teknologi. Alt dette utfordres av den mobile helseteknologien.



Vår undersøkelse viser at få deler sin helse- og treningsinformasjon i dag. 11 % av de som bruker helserelaterte applikasjoner deler informasjonen med helsepersonell. Imidlertid sier 40 prosent at de kan tenke seg å gjøre det. Dette kan vise hvilken retning dette går i.

Landskapet som tegner seg er integrerte tjenester hvor helseopplysningene skapes og deles av brukeren selv.

Dersom opplysningene bare lagres på mobilen, som for eksempel ved bruk av en skritt- eller kaloriteller, er personvernutfordringene små. Men for å få mer avansert diagnostisk informasjon, om for eksempel føflekk-kreft, vil det være nødvendig å dele med andre aktører som kan analysere den. Dette kan være den norske offentlige helsetjenesten, men det kan også være kommersielle aktører i inn- og utland som tilbyr avanserte analyser.

Helsetjenesten i Norge er i dag ikke klar for å ta i mot data fra mobil helseteknologi. Samtidig tar stadig flere i bruk den nye teknologien. Regjeringen har nylig varslet at folks egne helseopplysninger skal kunne lastes opp på helsenorge.no³⁶. På sikt skal det bli mulig å dele opplysningene med helsepersonell og andre kontakter som pårørende, frivillige hjelpere og pasientnettverk, når dette er relevant.

Så langt, så bra. Men dette forutsetter i utgangspunktet at helseopplysningene som sendes inn fra pasientene helse-apper er vurdert som «relevante og nødvendige» (dvs. journalverdige) av helsepersonell. Store mengder overskuddsinformasjon, som automatisk kan havne i journalen rett fra mobilen uten å bli vurdert av en lege, vil kunne utgjøre en fare for brukerens personvern. Vil personvernprinsipper som samtykke, begrunnet formål, relevans og korrekthet fortsatt gjelde?

Dersom disse helseopplysningene ikke tas inn i journalen, vil det offentlige i praksis sitte med et nytt helseregister det ikke er hjemmel for. Det offentlige må finne sin rolle i det nye landskapet.

Mobil helseteknologi er disruptiv, den forstyrrer måten vi organiserer informasjonsflyt på og skaper nye markeder i høyt tempo. Dette gjør det vanskelig for det offentlige å henge med. Antageligvis vil derfor mange velge å bruke kommersielle aktører til å lagre og analysere helsedata de neste årene. Dette vil by på mange åpne spørsmål:

- Det er uklare ansvarsforhold i app-markedet. Hvilke opplysninger blir behandlet? Hvem behandler dem, og hva blir de brukt til?

³⁶ Stortingsmelding 9/2012-2013 "En innbygger – én journal"

- Kan mine opplysninger bli videresolgt eller brukt til forskning? Faren at opplysningene blir brukt til helt andre formål som f. eks markedsanalyser er stor.
- Hva har jeg egentlig samtykket til og hvilket lands lover gjelder?

Det finnes over 40.000 helserelaterte applikasjoner for smarttelefoner og nettbrett. 10% av alle smarttelefoneiere har lastet ned en helseapplikasjon³⁷.

Anslagsvis 30 prosent av smarttelefonbrukere vil bruke helseapper innen 2015³⁸
Helseapper omsettes for rundt 718 millioner dollar internasjonalt og er forventet doblet i løpet av et år.

Antall brukere av helse-apper doblet seg fra 2011 til 2012 – fra 124 millioner til 247 millioner.³⁹

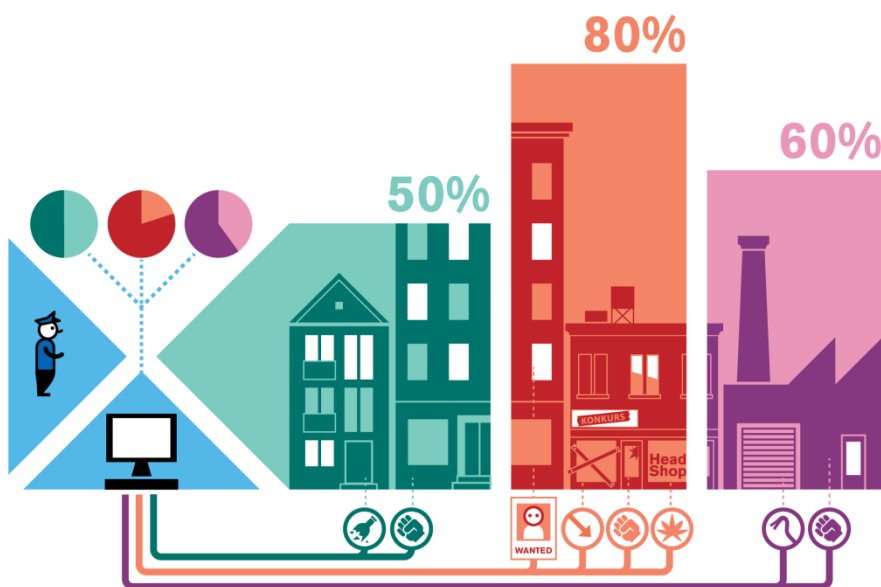
Ifølge vår undersøkelse har 33% av den norske befolkning brukt minst én helse- eller treningsapp. Skrittmåler er mest populært blant kvinner, treningsapper er mest populært blant menn.

³⁷ <http://www.helsenorgebeta.net/2013/01/ehelse-mobilhelse-og-helseapper/>

³⁸ <http://www.mobilehealthlive.org/go/download/?file=telenorreport.pdf>

³⁹ <http://www.bizjournals.com/dayton/news/2012/04/24/health-care-apps-soar-in-popularity.html?page=all>

SMART POLITI



En god politibetjent trenger bra ører, skarpe øyne og et kvikt hode. Teknologien gir nå muligheten til å forsterke alle disse egenskapene – fra «lytteposter» på internett, via digitale HD-kameraer og bilskiltlesere til avanserte analyser av store datamengder.

22. juli-kommisjonen var knusende i sin dom over politiets bruk av teknologi⁴⁰: PST hadde for eksempel begrensede muligheter til å søke i egne data, viktig informasjon som gjerningsmannens bilnummer nådde ikke ut i tide, riksalarmer kom for sent og patruljene kunne ikke motta tekst, bilder eller kartopplysninger. Listen er lang, men kort fortalt må norsk politi, i følge kommisjonen, begynne å utnytte «potensialet i informasjons- og kommunikasjonsteknologien». Politiet må bli smartere. Men hvor smart vil vi at politiet skal bli?

SMART POLITI ER PÅ NETT MED SEG SELV

Tilgang til relevant informasjon tett opp til hendelsen er viktig for å etablere et korrekt situasjonsbilde. Jo bedre sammenstilt og formidlet denne informasjonen er, jo bedre blir politiets situasjonsforståelse.

I kjølvannet av 11. september tok New York nye grep for å gi politimannen i gata raskest mulig tilgang til all relevant informasjon om en hendelse. NYPDs "Real Time Crime Center"⁴¹ (RTCC) samler, behandler og videreformidler informasjon mellom politifolkene på operasjonssentralen og de som er i felten.

Med tilgang til registre om involverte personer og steder, som nødtelefonlogg, tidligere arrestasjoner, parkeringsbøter, bygningstegninger, veinett, osv. kan RTCC gi fortløpende informasjon til patruljene og supplere med nye ledetråder i etterforskningen. Systemet kobler altså sammen ulike datakilder: data fra et åsted, politiinterne data, samt offentlige datakilder. Med RTCC kan politiet være trygg på at de til enhver tid vet akkurat det de trenger å vite. Resultatet er i følge New York-politiet høyere oppklaringsrate og bedre resursbruk.

PÅ NETT MED PUBLIKUM

22. juli tvitret ungdommene på Utøya om hendelsene på øya. Med riktig bruk av denne informasjonen kunne politiet brukt det til raskt å etablere et klarere bilde av situasjonen på øya. Nødtelefoner og varsling til politiet har i utgangspunktet vært designet for talemeldinger, men med utbredelsen av smarttele-

⁴⁰ <http://www.22julikommisjonen.no/Rapport>

⁴¹

http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=9&ved=0CFEQFjAI&url=http%3A%2F%2Fwww.nyc.gov%2Fhtml%2Ffuncp%2Fgprb%2Fdownloads%2Fpdf%2FFNYC_Safety%2F520and%2F520Security_RTCC.pdf&ei=gosBUejJDMOs4AST9oCABg&usq=AFQjCNGvRYjATRbQHSEQdYeYy2wFxoe2pw&bvm=bv.41524429,d.bGE

foner kan dette endres til å gi langt rikere informasjon. I flere land planlegges det nå å utvide 112-loggen med informasjon fra publikum med bilder, lyd og geografisk plassering. Det er allerede utviklet mobilapper⁴² der brukeren lager en enkel rapport med bilder, plassering, tekst og muntlige beskrivelser av en hendelse, og sender rapporten til politiet.

I Norge, som er blant de landene i verden med høyest utbredelse av smarttelefoner, ville innspill fra publikum enkelt kunne supplere politiets situasjonsbilde.

ER PÅ NETT MED FREMTIDEN

Algoritmer som ser etter mønstre og trender i datasett, kan nå trenes opp på stadig større datamengder. Når du kjøper en bok hos Amazon, får du en personalisert handleopplevelse med tips og tilbud basert på kjøpshistorikken til andre kunder med tilsvarende kjøpsmønster.

Lignende verktøy kan politiet benytte for å avdekke tidligere ukjente sammenhenger i kriminalitetsdata og andre tilgjengelige datakilder. Trender og mønstre kan brukes til å sannsynliggjøre en fremtidig utvikling. Dette kan hjelpe politiet i å forutsi hendelser, fordele ressurser og kanskje til og med komme noen hendelser i forkjøpet.

Sentrum politistasjon i Oslo har gjort gode erfaringer med dette i bekjempelsen av lommetyverier. Ved å analysere mønstre som danner seg når historiske kriminalitetsdata blir lagt over på kart sammen med andre data, kunne politistasjonen raskt se nye sammenhenger mellom tid og sted for registrerte lommetyverianmeldelser og aktivitet ved bestemte utesteder. Gjennom relativt enkle grep kunne så politiet, i samarbeid med utestedene, iverksette tiltak som gjorde det vanskeligere for lommetyver å operere i området. Denne metodikken ga resultat i form av en kraftig reduksjon i anmeldte lommetyverier i Oslo sentrum.

Politiet i Los Angeles har gått enda lenger. Med økende kriminalitet og økonomiske krisetider har de funnet nye måter å ta i bruk analytiske verktøy på i bekjempelsen av kriminalitet. De tok utgangspunkt i matematiske modeller utviklet for å forutsi jordskjelv og etterskjelv, og foret inn lokale kriminalitetsdata og annen relevant informasjon, med gode resultater⁴³. LAPD kan nå

⁴² <http://www.vorpalfox.com/ispotacrime>

⁴³ <http://www.predpol.com>

forutsi hvor og når det er sannsynlig at en gitt kriminell handling finner sted – og det innenfor områder ned til 150 m. Ved hjelp av mobile digitale kart, kan politipatruljene bruke denne informasjonen til å ligge i forkant av kriminelle hendelser. At politiet er på stedet allerede før forbrytelsen har skjedd, har naturlig nok ført til en kraftig reduksjon i kriminaliteten.

PERSONVERNUTFORDRINGEN

Det er bred enighet om at norsk politi må bli flinkere til å bruke data. Dette kan forebygge, forutse alvorlig hendelser, og gjøre politiet bedre i stand til å håndtere kriser. Samtidig preges samfunnet av stadig større datamengder. Digitaliseringen av samfunnet kommer til uttrykk bl.a. gjennom flere og flere sensorer og mobile enheter som vekselvirker over nettverk. Samtidig forgår mer og mer menneskelig aktivitet over nettet, det være seg handel, kommunikasjon, debatter og utveksling av informasjon og ideer. Dette vellet av data og informasjon åpner for nye muligheter, men har samtidig noen betenkelige sider.

FORMÅLSUTGLIDNING

Et smart politi vil være sultent på data. Politiet vil ønske seg rask tilgang til all relevant informasjon så nært opp til hendelsen som mulig. I Norge har politiet tilgang til mange typer opplysninger i sine ulike registre, og mye vil være av personsensitiv natur. Politiets arbeidsområde spenner vidt og omfavner både forvaltningsoppgaver og arbeid relatert til etterforskning. Dette kan være en utfordring.

Erfaringer fra andre land viser at data som opprinnelig var samlet inn i forvaltningsøyemed, ofte kan være nyttig i en etterforskningssak når den for eksempel sammenstilles med informasjon fra et annet register og på denne måten brukes til å avdekke sammenhenger og mønstre. For eksempel kan en vite noe om bevegelsesmønsteret til en bileier ved å sammenstille et bilregister, hvor formålet med innsamlingen er kontroll av registrering og årsavgift, med plasseringsdata fra automatiske bilskiltavlesere.

Slik kan deling og "gjenbruk" av data gi et mer slagkraftig politi, men dette innebærer at opplysninger blir brukt til andre formål og i andre sammenhenger enn opprinnelig tiltenkt. Og hvis en først tillater en slik formålsutglidning,

hvordan da sikre at kun de riktige personene får tilgang til informasjonen og forvalter den på en måte som ivaretar personvernet?

BLIR VI ALLE TYSTERE?

Gitt den stadig økende utbredelsen av smarttelefoner i befolkningen, kan politiet i prinsippet raskt innhente mer detaljert informasjon enn noen gang overalt hvor folk befinner seg. Men hvordan spiller disse mulighetene inn på forholdet mellom politi og samfunn? Når skal politiet få lov til å innhente slik informasjon fra publikum? Ønsker vi at naboen skal kunne berike en anmeldelse med lyd og bilde? Og hvordan håndterer vi eventuell overskuddsinformasjon: skal politiet kunne bruke informasjon om personer som tilfeldigvis befinner seg i bakgrunnen i en videorapport fra f.eks. en bilulykke i en annen straffesak?

PÅ FEIL STED, TIL FEIL TID

Et forutseende politi, eller *predictive policing*, gir allusjoner til science fiction filmer som "Minority Report". Blir politiet allvitende?

I utgangspunktet er det lite personsensitivt å overvåke steder. Dette har bidratt til at LAPD har møtt relativt lite kritikk fra borgerrettighetsforkjempere. Det forutseende politiet kombinerer kriminalitetshistorikk med andre data fra omgivelsene for å forutsi hvor og når hendelser som krever en politirespons vil kunne finne sted. Politiet vurderer så hvordan de bør handle og forvalte ressursene på bakgrunn av denne innsikten.

Men selv om algoritmene i utgangspunktet er personnøytrale, vil slike metoder kunne rette søkelys på områder og steder som har høy sannsynlighet for eksempel kriminelle handlinger. Kan slike sannsynlighetsprognoser være tilstrekkelig til å gi politiet "skjellig grunn til mistanke" og anledning til å ransake personer som ellers ikke ville blitt stoppet, eller banke på en dør som ellers ikke ville blitt banket på, kun fordi vedkommende befinner seg på et bestemt sted ved et bestemt tidspunkt? Vil vanlige folk som tilfeldigvis befinner seg i et slikt område føle seg kriminalisert?