PERSONVERN 2015

TILSTAND OG TRENDER

2014

APRIL

DATALAGRINGSDIREKTIVET KJENT UGYLDIG

EU-domstolen kjenner datalagringsdirektivet (DLD) ugyldig, og konkluderer med at direktivet innebærer alvorlige inngrep i privatlivet. Noen dager senere klargjorde samferdselsminister Ketil Solvik-Olsen at videre arbeid med Datalagringsdirektivet blir lagt på is.

MAI

«RETTEN TIL Å BLI GLEMT»

EU-domstolen pålegger Google å fjerne indekseringen av et søketreff om en spansk privatperson. Som følge av dommen kan enkeltpersoner henvende seg Google eller andre søkemotorer for å kreve at søketreff om dem slettes, gitt visse kriterier.

JULI

POLITIREGISTERLOVEN

1. juli trådte den nye politiregisterloven i kraft. Loven skal sørge for at informasjonssikkerheten og personvernet ivaretas bedre når politiet behandler personopplysninger. Loven stiller en rekke krav til politiets registre, og gir de registrerte rettigheter i form av blant annet innsyn.

AUGUST

PST ØNSKER Å BRUKE STORDATA

PST har fremmet lovforslag om å kunne samle og lagre såkalte stordata. Dette for å kunne identifisere trender og utfordringer, uten å rette fokus mot enkeltindivider. Politikere fra hele det politiske landskapet tok raskt avstand fra forslaget.

OKTOBER

SALG AV NORSKE TOPPDOMENER

Teknologirådet, Datatilsynet og Forbrukerrådet ber i et felles brev om at samferdselsministeren stopper salg av norsk toppdomene til utlandet. Bakgrunnen var en åpen høring om et forslag å bruke toppdomenene .sj og .bv som sikre personvernsoner på nett. Høringen viste bred enighet om at personvernutfordringene på nett er presserende, og at toppdomener kan by på personvernmuligheter som bør utredes videre.

NOVEMBER

KRYPTERING BEKYMRER ETTERRETNINGEN

Etter Snowden-avsløringene i 2013 har flere teknologiselskaper satt kryptering høyt på agendaen. Påtroppende direktør i den britiske etterretningstjeneste GCHQ Robert Hannigan utrykte bekymring for at økende kryptering fra de store teknologiselskapene gjør livet enklere for terrorister og kriminelle, og samtidig vanskeligere for etterretningstjenestene.

DESEMBER

OVERVÅKING AV MOBILNETTET I OSLO

Aftenposten avslører at det har forekommet overvåking av mobilnettet i Oslo sentrum ved hjelp av såkalte IMSI-fangere. Det er ikke kjent hvem som står bak overvåkingen. I et nytt lovforslag som er til høring foreslås det at politiet skal få utvidet myndighet til å bruke slikt utstyr også uten forutgående rettsbehandling.

KALENDER 2015: SE SISTE SIDE

PERSONVERN 2015
TILSTAND OG TRENDER

ISBN 978-82-92447-76-5 (trykket utgave)
ISBN 978-82-92447-77-2 (elektronisk utgave)

Utgitt: Oslo, januar 2015
Omslag og illustrasjoner: Lars Tothammer/Illustratørene
Trykk: ILAS

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

PERSONVERNDAGEN

Teknologirådet og Datatilsynet markerer i år for tredje gang den internasjonale personverndagen 28. januar med et felles arrangement og en rapport. Målet er å kartlegge viktige trender og å skape debatt om personvernspørsmål.

I fjor var Snowden-saken, med avsløringene av amerikanske NSAs storstilte innsamling av digital informasjon ett av hovedtemaene. I år ser vi nærmere på livet etter Snowden-avsløringene, og hvilken innflytelse saken har hatt på personvernets stilling i året som har gått.

Vi har også undersøkt folks holdninger til barns rett til privatliv. Hvor går grensene for hva foreldre kan gjøre for å følge med på hva barna driver med? Barns personvern utfordres også i skolen. I årene fremover vil klasserommene fylles med nye digitale verktøy som samler inn store mengder data om elevene. Vi ser på hvilke konsekvenser det kan få for elevene på kort og lang sikt at de vurderes ut i fra alle disse dataene.

Mens Snowden-saken dreide seg mest om opplysninger om hva vi foretar oss på nett, handler «tingenes internett» om de små, nesten usynlige dingsene som, uten at vi tenker over det, samler inn store mengder informasjon om hvordan vi lever livene våre i den fysiske verden. Det kan gi oss en enklere hverdag, et tryggere hjem og et mer velfungerende samfunn, men kan også utfordre personvernet.

I forbindelse med markeringen av personverndagen fikk vi i desember 2014 utført en spørreundersøkelse om personvern. TNS Gallup gjennomførte undersøkelsen via sitt nettpanel. Den ble besvart av 1091 innbyggere fra 15 år og oppover.

28. januar 2015

Tore Tennøe
direktør i Teknologirådet

Ove Skåra
fung. direktør i Datatilsynet

INNHOLD

ETTER SNOWDEN 5

FIKK SNOWDEN-SAKEN KONSEKVENSER? 6

VIKTIGE DOMMER FORSVARER PERSONVERNRETTIGHETER 8

PSTS ØNSKE OM STORDATA AVVISES RASKT 10

PERSONVERN SOM KONKURRANSEFAKTOR 11

MANNEN I GATA 14

BEDRE RUSTET FOR KOMMENDE DEBATTER 17

SKOLEN SOM ALDRI GLEMMER 18

SKOLEN DIGITALISERES 19

BIG DATA I SKOLEN 21

ELEVOPPLYSNINGER SOM BETALINGSMIDDEL 24

HVA KAN VI GJØRE? 27

HAR BARN RETT TIL PRIVATLIV? 29

BARNS KRAV TIL PRIVATLIV STØTER MOT ANDRE HENSYN 30

ER SNOKING OK? 32

DELING AV BILDER AV BARN 35

EN SPORET BARNDOM 37

TINGENES INTERNETT 40

HVA ER TINGENES INTERNETT? 41

HJEMMESEIER FOR SMARTE DINGSER 44

NÅR TING BLIR VANSKELIGE 47

ETTER SNOWDEN

Snowden-avsløringene om amerikanske sikkerhetsmyndigheters overvåking av Internett og telekommunikasjon vakte stor oppmerksomhet sommeren 2013. Saken satte personvern på dagsorden på en helt ny måte. I fjorårets personvernrapport skrev vi om Snowden-saken og hva som skjedde det første halve året etter at den ble kjent[1]. Hvor står vi i dag, halvannet år etter at avsløringene nådde media?

FIKK SNOWDEN-SAKEN KONSEKVENSER?

Hva førte Snowden-avsløringene til? Etter vår vurdering ligger det mye i kjølvannet av avsløringene. For å illustrere hvor vi står i dag, har vi valgt ut et knippe saker og utviklingstrekk som kan sies å være konsekvenser av avsløringene, eller det klima de skapte. Vi har sett særlig på hva Snowden-saken brakte med seg for Norges del, og for Europa for øvrig, som vi er knyttet til gjennom felles personvernregelverk.

NY DYNAMIKK I DEBATT OG PERSONVERNARBEID

En viktig konsekvens av Snowden-saken er en ny dynamikk i personverndebatten og i arbeidet med å ivareta personvernet. Snowden-saken har satt personvern, overvåking og individuelle friheter i den digitale tidsalder på dagsorden mer ettertrykkelig enn noen tidligere enkeltsak. Vi tror Snowdens avsløringer har gitt et nytt bakteppe for debatten om personvern og for de valg som tas på området. Avsløringene har gitt mange en erkjennelse av at demokratiske kjerneverdier står på spill når vi snakker om overvåking og personvern.

Vi mener den nye dynamikken bærer preg av at personvern betraktes som viktigere enn før. I dag eksisterer det et større mot og mer handlekraft blant mange aktører. Det betyr imidlertid ikke at personvernet som oftest vinner frem. Men det er i dag betydelig vanskeligere å skyve personvernhensyn til siden som irrelevante eller ubetydelige. Det er en stor endring.

Vi tror det er særlig er to aspekter ved Snowden-saken som har gjort at den har hatt så stor effekt. Det ene er at selv vanlige mennesker som ikke utgjør

[1] Kapittelet «Snowden-avsløringene» i *Personvern 2014 – Tilstand og trender*.

noen trussel verken for eget land eller USA kan føle seg direkte berørt. Det andre aspektet er at avsløringenes innhold endrer tradisjonelle tillitsforhold: Enkeltmenneskets tillit til kommunikasjon over Internett, til myndigheter og til tjenestetilbydere er blitt berørt. Det handler også om tilliten mellom tjenestetilbydere og deres myndigheter, og om tillit nasjoner imellom.

EU – NY PERSONVERNFORORDNING OG REFORHANDLING AV SAFE HARBOUR-AVTALEN

Etter Snowdens avsløringer kan vi se hvordan EU søker å øke vernet om europeiske borgeres personopplysninger. Dels har dette arbeidet brodd mot USA.

Snowden-saken satte fart i EUs arbeid med nytt personvernregelverk, som hadde en svak fremdrift før avsløringene kom. I oktober 2013 stemte medlemmene i EU-parlamentets komité for sivile rettigheter for å støtte et utkast til ny lovtekst. EUs justiskommisær, Viviane Reding, betegnet det som et gjennombrudd og tydeliggjorde at arbeidet hadde hast: «Heads of state and government should make clear that common European data protection rules are very much needed and are needed now»[2]. I mars 2014 kom EU-parlamentet til enighet om et forslag. En ferdig vedtatt lovtekst – en forordning – er ventet i løpet av 2015.

> Nytt personvernregelverk fra EU er viktig for Norge, og reglene vil gå inn i norsk lov. Dagens personverndirektiv (Direktiv 95/46/EF), som den nåværende personopplysningsloven bygger på, er fra 1995 og bærer preg av å være laget før vår tids omfattende bruk av Internett.

På mange felter synes regelverket å styrke personvernet. Hvilke aktører som må følge det europeiske regelverket, og hvor det skal gjelde – lovens geografiske virkeområde – er en interessante del i det nye regelverket. Etter dagens personverndirektiv må virksomheten være etablert innenfor landene omfattet av direktivet. Snowden-saken handler primært om ikke-europeisk bruk av personopplysninger. I ny forordningstekst, slik den står nå, utvides regelverket til å også omfatte en virksomhet dersom den retter sine tjenester mot eu-

[2] http://www.theguardian.com/world/2013/oct/22/breakthrough-data-privacy-rules-europe

ropeiske borgere, også om tjenestetilbyderen befinner seg utenfor Europa[3]. EU søker altså å gi sine borgere et europeisk personopplysningsvern, selv om tjenesten eksempelvis gis av en amerikansk aktør.

Safe Harbour-avtalen
I 2000 inngikk EU og USA har en særavtale, Safe Harbour-avtalen, som regulerer overføring av personopplysninger fra et EU-/EØS-land til USA. Virksomheter i USA som forplikter seg til avtalen kan motta personopplysninger fra Norge (eller et annet EU/ EØS-land) uten at personvernmyndigheten må godkjenne overføringen først.

Snowdens avsløringer førte til at det fra europeisk hold ble stilt spørsmål ved om Safe Harbour-avtalen[4] egentlig ga god nok sikkerhet for personopplysningene overført til USA. Avtalen er nå under reforhandling, noe som må ses som direkte konsekvens av Snowden-saken.

VIKTIGE DOMMER FORSVARER PERSONVERNRETTIGHETER

Etter Snowdens avsløringer har det falt to viktige dommer av betydning for europeiske borgeres personvern: EU-domstolens beslutning om Datalagringsdirektivet[5] og den såkalte Google-dommen[6]. Vi tror det er riktig å se de to dommene i lys av en ny dynamikk i personverndebatten. Denne dynamikken er i stor grad skapt av Snowden-saken. Den har gjort det lettere for EU-domstolen å sette ned foten av hensyn til personvernet.

Den 8. april 2014 kom EU-domstolens beslutning: Datalagringsdirektivet ble kjent ugyldig. Noe dager senere klargjorde samferdselsminister Ketil Solvik-Olsen at videre arbeid med Datalagringsdirektivet ble lagt på is[7]. Stortinget vedtok i 2011, med 89 mot 80 stemmer, å innføre Datalagringsdirektivet i norsk lov. Regelverkets ikrafttredelse har vært utsatt en rekke ganger. Den

[3] Se artikkel 3 i EU-parlamentets tekst (høyre kolonne) http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0212
[4] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:EN:PDF
[5] http://www.scribd.com/doc/216980523/Judgment-of-the-ECJ-in-Digital-Rights-Ireland-data-retention-challenge
[6] http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf
[7] http://www.dagbladet.no/2014/04/11/nyheter/samfunn/politikk/overvaking/dld/32780686/

norske varianten av direktivet kan nå sammenliknes med en bil som ble avskiltet før den i det hele tatt kom på veien.

Snowdens avsløringer handler i stor grad om opplysninger som Datalagringsdirektivet påla langtidslagring av, nemlig såkalte trafikkdata fra elektronisk kommunikasjon. Snowden-saken nevnes ikke eksplisitt i dommen. Vi mener likevel at det er naturlig å anta at avsløringene har vært en medvirkende faktor for utfallet av saken.

Tilsidesettelsen av Datalagringsdirektivet betyr ikke nødvendigvis en endelig slutt for regelverk om lagring av trafikkdata. Statsminister Erna Solberg har vært tydelig på at en grad av lagring av trafikkdata etter hennes vurdering er nødvendig. Hun er derfor åpen for å vurdere å lage nasjonale regler.

Google-dommen fra mai 2014 viser villighet og mot til å gripe inn mot en stor internasjonal aktør. Dommen har betydning for personvernverdien som ligger i «retten til å bli glemt». I korte trekk handler saken om en spansk privatpersons krav om at Google fjerner søketreff på hans navn knyttet til en gammel notis i en avis, hvor det fremgår at hans bolig ble tvangsauksjonert for å dekke gjeld til sosialtjenesten. EU-domstolen kom til at Google må fjerne indekseringen av mannens navn, slik at denne saken ikke dukker opp blant søketreffene når man søker på ham. Dommen betyr *ikke* at selve kilden til søketreffet må slettes, for eksempel at en nettavis må slette sin artikkel.

Som følge av Google-dommen kan enkeltpersoner henvende seg Google eller andre søkemotorer for å kreve at søketreff på deres navn slettes. I tillegg kan enkeltpersoner klage et eventuelt avslag hos søkemotoren inn for landets personvernmyndighet. Datatilsynet hadde ved årsskiftet mottatt 11 slike saker etter at dommen falt i mai 2014.

Sett fra et personvernsynspunkt er dommen både gledelig og viktig. Den har imidlertid vakt debatt, fordi den også berører et annet viktig hensyn, nemlig informasjonsfriheten.

Gjennom dommen viser EU-domstolen både vilje og mot til å underlegge en stor amerikansk internettaktør europeisk personvernjurisdiksjon. Til grunn for dommen ligger et viktig, men slett ikke selvinnlysende premiss: Googles

søketjeneste er omfattet av det europeiske personverndirektivet (fordi Google Spain har kontor i Europa). «… domstolen [har] i realiteten foregrepet – og dermed samtidig forhåndsgodkjent – Kommisjonens forslag om at EUs nye personvernforordning skal gjelde også for ikke-europeiske selskaper så lenge disse tilbyr varer eller tjenester i EU. Rettspolitisk er standpunktet velkomment, men det må være lov å karakterisere EU-domstolens tolkning av det territorielle anvendelsesområdet for dagens personverndirektiv som temmelig frisk[8]», skrev Halvard Haukeland Fredriksen, førsteamanuensis ved Det juridiske fakultetet ved Universitetet i Bergen, i artikkelen *EU mot Google – Retten til å bli glemt mot retten til å vite*.

Etter vårt syn er Google-dommen et eksempel på en vurdering som bærer preg av tiden etter Snowden. Det er større mot og vilje til å treffe beslutninger som prioriterer personvernet, også når andre viktige hensyn taler for motsatt konklusjon. Det samme gjelder dommen om Datalagringsdirektivet. Direktivet kom i kjølvannet av terroranslagene i London og Madrid. Anti-terrorhensyn har etter 11. september 2001 hatt preg av «trumfkort» over andre hensyn. Dommen viser villighet til å sette foten ned for et regelverkstiltak selv om det er begrunnet med behovet for å bekjempe terror.

PSTS ØNSKE OM STORDATA AVVISES RASKT

Vi ser tegn til at det fokuset på personvern og overvåking som Snowden-saken har brakt med seg, har senket terskelen for å si nei til personverninngripende tiltak. Vi tror også at avsløringene av hva som er mulig og hvilke gigantiske innsamlingsprogrammer som kan bygges opp har vært bevisstgjørende. Politikere er trolig mer bevisst på hvor de mener grensen bør trekkes. I august 2014 skjedde noe som illustrerer dette:

Sjef for PST, Benedicte Bjørnland, skulle holde foredrag på Nordisk juristmøte. Her skulle hun legge frem sitt syn på sikkerhet i de nordisk samfunnene, og snakke om behovet for nye midler i kampen mot terror. Bjørnland foreslo å lagre informasjon om nettbruk og at PST burde kunne ta i bruk såkalt stordataanalyse. Bjørnland var åpen på at dette ville medføre innsamling av informasjon om personer som ikke ellers var av interesse for PST. Ønsket om å ta i bruk stordata nådde pressen før selve foredraget ble holdt[9]. Fra politisk hold

[8] http://voxpublica.no/2014/06/google-og-eu-retten-til-a-bli-glemt-mot-retten-til-a-fa-vite/
[9] http://klassekampen.no/article/20140822/ARTICLE/140829982

var responsen både rask og kritisk. «… etter at PSTs ønske ble kjent, har norske toppolitikere stått i kø for å ta avstand fra slike virkemidler», meldte NRK[10]. En så rask og relativt unison negativ respons ville neppe ha kommet uten Snowden-saken som bakteppe.

PERSONVERN SOM KONKURRANSEFAKTOR

Amerikanske myndigheter forsvarte overvåkingen med at den ikke rammet amerikanske borgere da Snowden-saken sprakk. Facebooks Mark Zuckerberg kommenterte: «The government response was, 'Oh don't worry, we're not spying on any Americans.' Oh, wonderful: that's really helpful to companies trying to serve people around the world, and that's really going to inspire confidence in American Internet companies[11]»

Snowden-sakens evne til å svekke tillitsforhold ble særlig tydelig på markedet. Det gjelder både kundenes tillit til de amerikanske internettselskapene og de samme selskapenes tillit til egne myndigheter. Avsløringene skapte et anstrengt forhold mellom store, amerikanske IT-selskaper og amerikanske myndigheter. Allerede noen måneder etter de første avsløringene, fremstod det som sannsynlig at amerikanske selskaper ville kunne tape store penger som følge av tillitstap hos kundene. Et eksempel fra våre trakter er skytjenesteleverandøren Jottacloud, som vakte oppmerksomhet for sin kundevekst som en konsekvens av Snowden-saken[12]. Selskapet satt veksten i sammenheng med at de kort etter avsløringene la frem en garanti om at de ikke ville utlevere opplysninger til myndigheter eller andre uten en rettslig kjennelse. Garantien ble hyppig referert til på amerikanske IT-nettsider og Twitter.

I en rapport fra august 2013 estimerte The Information Technology and Innovation Foundation at skytjeneste-industrien i USA kunne tape mellom 22 og 35 milliarder dollar frem til 2016, som følge av avsløringene om NSAs overvåking[13]. Rapporten fokuserer særlig på konkurranseforholdet mellom USA og Europa.

---

[10] http://www.nrk.no/norge/sv_-_-gar-kaldt-nedover-ryggen-1.11892589
[11] http://www.theguardian.com/technology/2013/sep/11/yahoo-ceo-mayer-jail-nsa-surveillance
[12] http://e24.no/digital/snowden-saken-ga-kundeboom-for-norsk-nettsky/21106285
[13] *How Much Will PRISM Cost the U.S. Cloud Computing Industry?* http://www2.itif.org/2013-cloud-computing-costs.pdf

Europa har ambisjoner om vekst for europeiske digitale tjenester. Allerede i 2012 la EU-kommisjonen frem en strategi for skytjenester som drivkraft for europeisk næringsliv og forvaltning.[14] For EUs arbeid med nytt personvernregelverk, har det vært en målsetting å legge til rette for europeisk digital tjenesteyting og å bygge tillit hos borgerne til europeisk behandling av personopplysninger. Europeiske aktører har sammenliknet med amerikanske tradisjonelt vært forstått som «tynget» av strengere personvernlovgivning. Som følge av avsløringene kan strenge personvernkrav og europeisk jurisdiksjon vise seg å ha markedsfordeler, og fremstå som det trygge alternativet.

Vi vet ennå ikke om Snowden-saken vil gi en varig dreining i markedet. På kort sikt fremstår det i hvert fall som om avsløringene gir europeiske aktører en gylden mulighet til å skaffe seg konkurransefortrinn. Vi ser tegn til en utvikling der godt personvern fremstår som en stadig viktigere konkurransefaktor for bedrifter, og det kan se ut som denne utviklingen har fått drahjelp av Snowden-saken.

IT-SELSKAPENE – KRYPTERING OG MER ÅPENHET

Kort etter avsløringene startet flere amerikanske IT-giganter å ta mer kryptering i bruk. Dette kan forstås som et mottrekk, og som et tiltak for å gjenvinne tillit. Avsløringene vakte også sinne og frustrasjon hos teknologiselskapene. «Googlers say "F*** you" to NSA, company encrypts internal network», lød en artikkeloverskrift på nettstedet Ars Technica fra november 2013[15]: Google krypterte datatrafikken mellom sine datasentre for å stanse den omfattende overvåkingen i sitt interne nett fra NSA og den britiske etterretningstjenesten GCHQ.

I november 2014 meldte tidsskriftet The Economist om flere viktige utviklingstrekk når det gjelder bruken av kryptering[16]. Kryptering blir enklere å ta i bruk for den vanlige bruker. Stadig flere aktører tar gode krypteringsløsninger i bruk i sine tjenester, og kryptering tenderer mot å bli standardinnstillingen på digitale enheter. Flere løsninger baserer seg også på at brukeren skal sitte med nøkkelen. På den måten avskjærer tjenesteleverandøren seg fra å kunne

[14] http://europa.eu/rapid/press-release_IP-12-1025_da.htm
[15] http://arstechnica.com/information-technology/2013/11/googlers-say-f-you-to-nsa-company-encrypts-internal-network/ Overskriften viser til bloggposter fra to sikkerhetsingeniører hos Google, Brandon Downey og Mike Hearn
[16] The Economist, 29. november 2014. *Cryptography for dummies* (side 67 og 68)

etterkomme myndigheters krav om utlevering. En rettslig kjennelse hjelper ikke.

Kryptering er ikke noen nytt. Teknologien har vært der, og den har også vært i bruk. Eksempelvis har både Microsoft og Apple også tidligere muliggjort full kryptering av harddisken fra sine operativsystemer, og nettjenester innen bank og finans, helserelaterte tjenester og netthandel har brukt kryptering lenge. Snowden-saken resulterte imidlertid i en ny hast for å få krypteringsløsninger på plass. Det gjelder både mer kryptering av lagret informasjon og mer kryptert datatrafikk. Eksempelvis startet Twitter å kryptere private beskjeder direkte mellom brukerne, og Facebook-eide WhatsApp, en app for lynmeldinger, har tatt i bruk et åpen kilde-basert system kalt TextSecure for apper på Android-enheter.

Det er et viktig utviklingstrekk at det krypteres mer nå enn tidligere. Kryptering gir imidlertid ikke full sikkerhet mot overvåking dersom man står overfor svært kompetente aktører. Kryptering gjør likevel masseovervåking svært vanskelig. «This is all about making dragnet surveillance impossible», uttalte Christopher Soghoian, IT-sikkerhetsekspert ved American Civil Liberties Union[17].

Selskapenes krypteringsreaksjon har nå til og med begynt å skape irritasjon og fortvilelse hos politimyndigheter i flere land. I september 2014 gikk direktør for FBI, James B. Comey, hardt ut mot Apple og Google for deres nye krypteringstiltak på mobile enheter[18]. Etter terroranslagene i Paris i januar 2015 uttalte Storbritannias statsminister, David Cameron, at han vil stoppe kommunikasjonsmidler hvis kryptering gjør det umulig for sikkerhetsmyndigheter å lese innholdet, slik som WhatsApp og Snapchat[19].

Kan den avslørte masseovervåkingen ha ødelagt for den mer rettede overvåkingen og etterforskningen? Det er først og fremst misnøye og sinne over NSAs masseovervåking som har drevet frem krypteringsreaksjonen. I en artikkel i Washington Post om negative reaksjoner på Apples og Googles kryptering av smarttelefoner, beskrives det at konsekvensene av krypteringen erfares sterkest blant politietterforskere. Disse har gjerne en rettslig kjennelse på

[17] http://www.washingtonpost.com/business/technology/google-encrypts-data-amid-backlash-against-nsa-spying/2013/09/06/9acc3c20-1722-11e3-a2ec-b47e45e6f8ef_story.html
[18] http://www.washingtonpost.com/business/technology/2014/09/25/68c4e08e-4344-11e4-9a15-137aa0153527_story.html
[19] http://www.dailymail.co.uk/news/article-2907466/Cameron-vows-boost-online-surveillance-PM-says-fanatics-not-able-talk-without-security-agencies-listening-in.html

ransaking av innholdet på en smarttelefon, men får ikke tilgang på grunn av kryptering.

IT-aktørene har også brukt større åpenhet om utlevering av personopplysninger til myndighetene, gjennom såkalte gjennomsiktighetsrapporter (transparency reports), som et virkemiddel for å bedre tilliten hos kundene. Også før Snowden-saken publiserte noen av selskapene denne type rapporter, men avsløringene førte med seg en ny utbredelse. «Thanks, Snowden! Now All The Major Tech Companies Reveal How Often They Give Data To Government» var overskriften på nettartikkel fra november 2013[20].

Etter avsløringene har amerikanske teknologiselskaper presset på egne myndigheter for å få tillatelse til å offentliggjøre mer detaljert informasjon om myndighetenes etterspørsel etter kundedata. Et stykke på vei er dette imøtekommet. I januar 2014 ble det annonsert at selskapene snart kunne offentliggjøre aggregerte tall over utleveringskrav med utgangspunkt i rettskjennelser fra Foreign Intelligence Surveillance Court (FISA-domstolen) og såkalte National Security Letters (en administrativ stevning fra FBI), og antallet kundekontoer disse gjaldt[21].

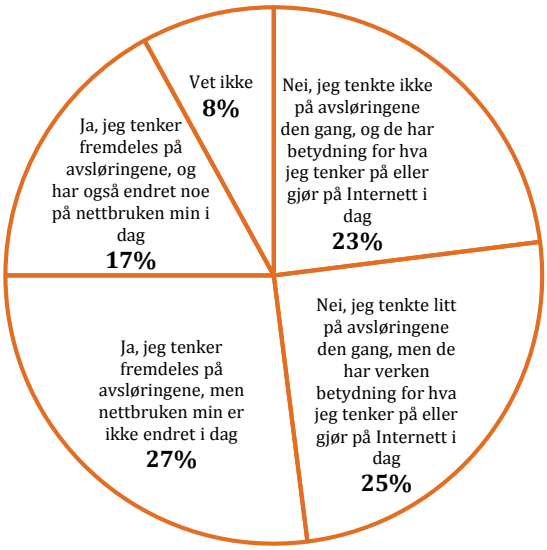
MANNEN I GATA

Saker om personvern og overvåking vekker sjelden oppmerksomhet blant alle. Fjorårets personvernundersøkelse viste imidlertid at nesten alle (94 prosent) nordmenn over 15 år hadde hørt om Snowden-saken. En snau halvparten av de spurte mente overvåkingen var «uakseptabel», og en drøy fjerdedel beskrev den om «bekymringsverdig, men nødvendig»[22]. Samme undersøkelse viste også at folk er mer opptatt av personvern enn før[23], noe vi antar at Snowden-saken har vært en sterkt medvirkende faktor til. Men etter at det har gått ytterligere ett år, har mannen i gata nå glemt Snowden-saken?

[20] http://www.forbes.com/sites/kashmirhill/2013/11/14/silicon-valley-data-handover-infographic/
[21] http://www.justice.gov/opa/pr/joint-statement-attorney-general-eric-holder-and-director-national-intelligence-james-clapper og http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/28/heres-why-tech-companies-nsa-transparency-reports-are-mostly-a-pr-stunt/
[22] Kapittelet «Snowden-avsløringene» i *Personvern 2014 – Tilstand og trender*. Intervjuene ble innsamlet i november 2013.
[23] Kapittelet «Bryr folk seg om personvern?» i *Personvern 2014 – Tilstand og trender*.

I vår nye undersøkelse fra desember 2014[24] fikk respondentene følgende spørsmål: «Det er nå gått halvannet år siden Snowdens avsløringer av amerikanske sikkerhetsmyndigheters overvåking av Internett, og deres tilgang til personopplysninger hos IT-selskaper som Apple, Microsoft, Facebook og Google. Har Snowden-avsløringene hatt noe å si for tenkningen din om nettovervåking, og for hva du gjør på Internett i dag?» Resultatene viser at Snowden-saken fortsatt er i folks bevissthet.

Har Snowden-avsløringene hatt noe å si for tenkningen din om nettovervåking, og for hva du gjør på Internett i dag?



At en snau halvpart, 44 prosent, fremdeles tenker på avsløringene, er sterkere enn vi forventet. 27 prosent svarer «Ja, jeg tenker fremdeles på avsløringene, men nettbruken min er ikke endret i dag». I tillegg svarer 17 prosent svarer «Ja, jeg tenker fremdeles på avsløringene, og har også endret noe på nettbruken min i dag».

[24] Undersøkelsen er kort beskrevet i forordet i rapporten.

Vi må anta at det å endre sine nettvaner har en temmelig høy terskel i Norge. Folk føler seg trygge, og de stoler på egne myndigheter. Mange vil trolig også være usikre på hva de kan gjøre for å sikre seg bedre. At 17 prosent, halvannet år etter avsløringene, sier at deres nettbruk er noe endret i dag, må ikke forstås som lite. Vi skal være forsiktige med å legge for mye i svarene, men at en betydelig andel opplever at de har gjort noen endringer i sin nettbruk, er talende. At Snowden-avsløringene førte til at en del gjorde endringer i sin nettbruk, er ikke et særnorsk fenomen. Andelen er enda høyere i andre land.

Høsten 2014 gjennomførte det globale markedsanalysebyrået Ipsos en stor spørreundersøkelse med 23 376 respondenter, fordelt på 24 land[25]. Undersøkelsen handler om internettsikkerhet og tillit, og hadde et par spørsmål om Snowden-saken. 73 prosent av de europeiske respondentene husket å ha hørt om Edward Snowden. Gjennomsnittet i den globale undersøkelsen var 60 prosent. Tyskland kommer sterkest ut med hele 94 prosent, fulgt av Sverige med 86 prosent. Det er ikke uventet at et flertall husker Snowden. Det som gjør større inntrykk, er svarene på oppfølgingsspørsmålet:

De som husket Snowden fikk spørsmål om de hadde tatt forholdsregler for å beskytte sitt personvern og sin sikkerhet på Internett som følge av hva Snowden avslørte. 39 prosent bekreftet at de hadde gjort dette. Gjennomsnittet for de europeiske landene var på 29 prosent, altså mindre enn det globale snittet. Tallet for Tyskland var på 39 prosent, Polen 32 prosent, Italia 25 prosent og Frankrike 23 prosent. Sverige – som det er naturlig for oss å sammenlikne oss med – hadde en andel på 20 prosent som oppgav at de hadde tatt forholdsregler for å beskytte seg. Det svenske snittet er altså svært likt andelen i vår egen undersøkelse som sier at deres nettbruk er noe endret i dag[26].

Sikkerhetseksperten og kryptolog Bruce Schneier har kommentert funnene på sin blogg[27]. Her tilbakeviser han en fremstilling om at undersøkelsen viser at Snowden-saken fikk liten betydning. Han har regnet ut at over 700 millioner mennesker i så fall har endret nettvaner som følge av Snowden-saken. «Name another news story that has caused over ten percent of the world's population to change their behavior in the past year?», skriver han.

---

[25] https://www.cigionline.org/internet-survey

[26] 86 prosent av svenskene husket Snowden. 20 prosent av disse oppgav at de hadde tatt steg for å bedre sin sikkerhet på nett. Det tilsvarer 17 prosent av svenskene i undersøkelsen, altså samme andel nordmenn som svarte at de fremdeles tenker på avsløringene, og har endret noe på sin nettbruk.

[27] https://www.schneier.com/blog/archives/2014/12/over_700_millio.html?utm_source=twitterfeed&utm_medium=twitter

BEDRE RUSTET FOR KOMMENDE DEBATTER

«Den som ikke ser at de vestlige demokratiene står sterkere etter Edward Snowdens avsløringer enn før, gjør seg selv blind» [28]

Mats Karlsson, direktør ved Sveriges utenrikspolitiske institutt

Snowden-saken innebærer et vannskille – vi kan dele tiden i før og etter. På personvernfeltet har avsløringene brakt med seg en ny dynamikk preget av større press og utålmodighet, og hos mange aktører har de utløst mot og handlekraft. Ny giv i EUs arbeid med nytt personvernregelverk og teknologiselskapenes implementering av krypteringsløsninger er eksempler på konkrete konsekvenser av Snowden-saken. Også vi som er vanlige brukere av internettbaserte tjenester og annen elektronisk kommunikasjon har blitt påvirket. Mange av oss tenker fremdeles på avsløringene – bevisstheten er skjerpet.

Helt i slutten av 2014 kom nyheten om at ukjente aktører mobilovervåket Stortinget, ambassader og næringsvirksomheter ved hjelp av såkalte IMSI-catchere. Som en slags skjebnens ironi skjedde dette parallelt med at Justisdepartementet sendte ut et høringsforslag om politiets bruk av samme utstyr.

Året 2015 startet med terroranslagene i Paris. Hendelsene ble etterfulgt av den britiske statsministerens uttalelse om at han vil forby kommunikasjonsmidler som er kryptert slik at sikkerhetsmyndighetene ikke kan få tak i innholdet. Den tyske forbundskansleren ønsker fortgang i EUs arbeid med et revidert datalagringsdirektiv[29]. I tiden som kommer kan vi vente oss viktige debatter om overvåking og personvern, både nasjonalt og internasjonalt.

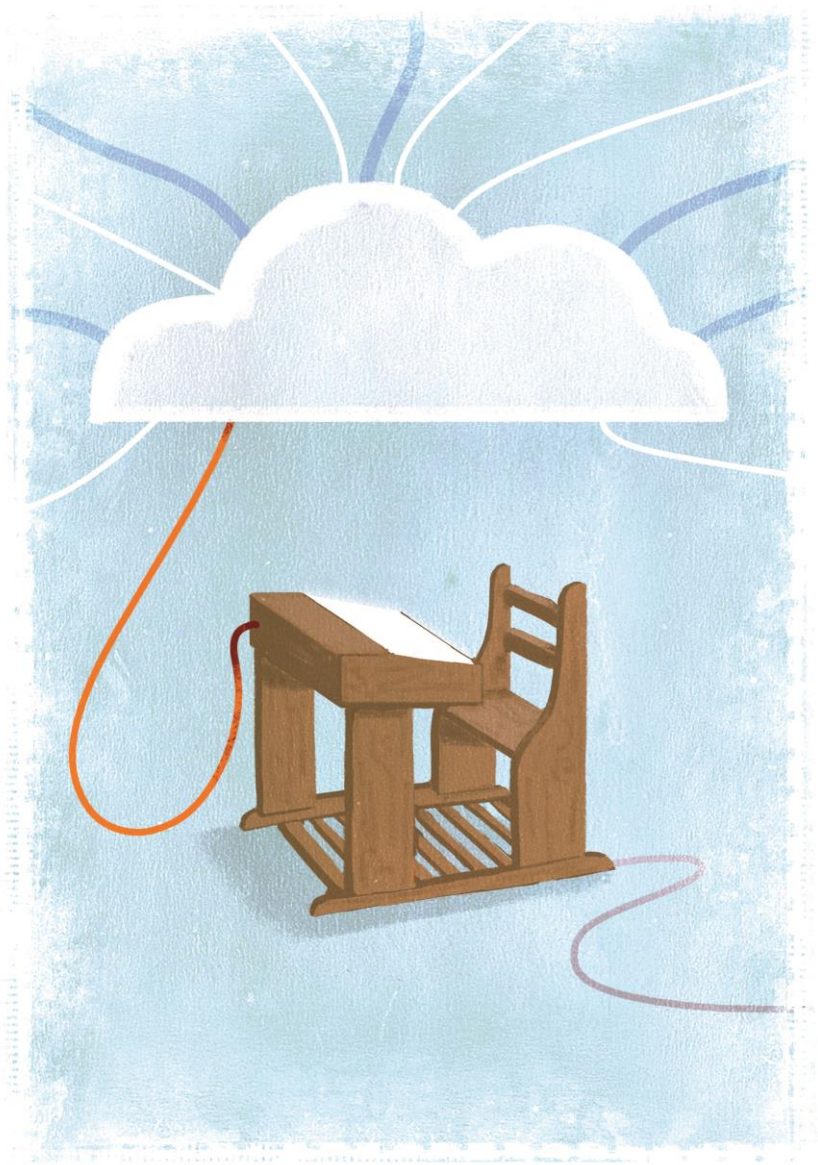
Et kontinuerlig fokus på personvern er helt vesentlig for å unngå for store inngrep i den enkeltes rett til privatliv. Snowden-saken har på ingen måte endret alt, men den har gjort nødvendigheten av personvern enda tydeligere. Dette er viktig, med tanke både på de politiske debattene vi vil få og den teknologiske og samfunnsmessige utviklingen vi vil se fremover.

---

[28] Snowden ble nominert til Nobels fredspris. Sitatet er en kommentarer til Snowdens kandidatur. http://www.nrk.no/nobel/ekspertenes-rad-til-nobelkomiteen-1.11960020

[29] http://www.digi.no/932423/merkel-vil-ha-fortgang-paa-nytt-dld

SKOLEN SOM ALDRI GLEMMER



Tidligere foregikk kommunikasjonen mellom skole og hjem mest via lapper i sekken. Skolearbeidet ble sirlig lagret i kladdebøker. Etter endt skolegang satt vi igjen med et berg av kladdebøker, som vi enten kastet eller stuet ned i pappesker på loft og i kjellerboder. Fremover vil elevenes gjøremål, prestasjoner og skolearbeid ikke lengre ligge lagret på loftet, men i nettskyen. Hvor lenge vil opplysningene ligge lagret der? Finnes det en «utgått-dato» på elevopplysninger? Og hvem vil ha tilgang på opplysningene og hva vil de brukes til?

Vi vil trekke frem tre utviklingstrekk i dagens skole som vil få betydning for elevenes personvern fremover: den gjennomgående digitaliseringen av skolen, nærværet av sterke kommersielle interesser og ønsket om å utnytte data om elevenes gjøremål og prestasjoner til analyse og profileringsformål: Big Data er på vei inn i skolen.

SKOLEN DIGITALISERES

HVA SKJER?

Skolen er i ferd med å digitaliseres. Nye digitale verktøy tas i økende grad i bruk for praktiske og pedagogiske formål. Bruk av slike verktøy og tjenester bidrar til å gjøre undervisningen bedre og mer aktuell. De gjør det lettere for skolen å skreddersy undervisningsopplegg til den enkelte. Men mer bruk av digitale tjenester i skolen fører også til at det samles inn og lagres *flere* personopplysninger om elevene enn tidligere.

Skolene benytter mange ulike systemer som alle samler inn opplysninger om elevene. De fleste skoler bruker digitale læringsplattformer (LMS – Learning Managment System). Fronter og ItsLearning er de mest brukte. Plattformene åpner for kontinuerlig logging av elevenes aktivitet, for eksempel når på døgnet eleven leverer oppgaver, hvor lang tid eleven bruker på oppgaveløsning, logg av kommunikasjon med lærer og andre elever, samt hvilke fag eleven har jobbet aktivt med i leksearbeidet. I tillegg til læringsplattformene bruker skolene ulike skoleadministrative systemer som lagrer andre opplysninger om

elevene, blant annet fravær og karakterer. Enkelte skoler benytter i tillegg også digitale verktøy til å kartlegge og registrere uønsket atferd[30]. For å kommunisere med hjemmet bruker skolene læringsplattformene, men mange skoler bruker i tillegg også andre kommunikasjonskanaler som e-post, SMS, Facebook og Twitter.

Bruken av nettbaserte læringsressurser blir også stadig mer utbredt og er i ferd med å erstatte den tradisjonelle læreboka[31]. Til forskjell fra lærebøkene, samler de nye verktøyene inn personopplysninger om elevene, som for eksempel hva de heter, kjønn, alder og prestasjoner. Et eksempel på en nettbasert læringsressurs er det norskutviklede matteprogrammet Kikora. Dette programmet logger elevenes tastetrykk ned til hvert ledd i regnestykket og tilbyr læreren et «dashboard» med detaljert oversikt over *hva* hver enkelt elev har gjort, *når* og *hvordan* det gikk.

PERSONVERNUTFORDRINGER

Personvern dreier seg blant annet om selvbestemmelse. For barn og unge i skolen, vil personvern handle om at foreldre og barn skal vite om og ha kontroll over hvordan opplysningene om barna blir brukt. Når skolen tar i bruk mange forskjellige digitale verktøy legges det igjen opplysninger om elevene på mange ulike steder. Dette skaper utfordringer knyttet til å gi elever og foreldre god informasjon om hvilke opplysninger som egentlig samles inn. Det skaper også utfordringer knyttet til hvem som har ansvar for behandlingen av opplysningene.

Uklare ansvarsforhold

For mange av de digitale verktøy som brukes i skolen vil det være tilbyderen av verktøyet som er mottager av elevopplysningene verktøyet samler inn. Skoleeier har plikt til å ha oversikt over hvilke personopplysninger som samles inn om elevene. Hvis tilbyderen av det digitale verktøyet lagrer opplysninger om elevene, skal det alltid etableres en såkalt databehandleravtale mellom skolen og tilbyderen. Skoleeiere skal vite hvilke opplysninger som lagres, hvorfor, hvem som skal ha tilgang til dem og hvor lenge de skal lagres.

---

[30] Et eksempel på et slikt system er SWIS (The School-Wide Information System). Det er et databasert informasjonssystem som lagrer rapporter om negative hendelser i skolemiljøet. http://www.swis.no/

[31] «Rapport fra kartleggingen av digitale læringsressurser», Senter for IKT i utdanningen, 2013, læringsressurserhttps://iktsenteret.no/sites/iktsenteret.no/files/attachments/kartlegging_av_digitale_laeringsressurser_lowrez_0.pdf

Det kan imidlertid være utfordrende for skoleeier å få oversikt over hvilke verktøy som brukes i skolen og å sikre at databehandleravtaler er på plass. Ofte blir verktøyene tatt i bruk av skoleledelsen ved hver enkelt skole, eller av ansatte ved skolen, uten at skoleeier informeres. Da er det en fare for at de digitale løsningene tas i bruk uten at nødvendige risikovurderinger er gjort i forkant. Dette gjelder blant annet risikovurderinger knyttet til sikkerhet. Det er også en fare for at skoleledelsen ikke har satt seg inn i hvilke opplysninger verktøyene samler inn og lagrer slik at elever og foreldre heller ikke får informasjon om hvilke opplysninger som lagres om elevene.

Informasjon til foresatt og elever om hvorfor og hvordan opplysningene om elevene blir behandlet, er en grunnleggende personvernrettighet. Uten informasjon har foresatte og elever ingen mulighet til å si ifra hvis de mener skolen ivaretar personvernet på en dårlig måte. Uten informasjon har de heller ikke mulighet til å be om innsyn, retting eller sletting – som er rettigheter personopplysningsloven gir den enkelte.

BIG DATA I SKOLEN

HVA SKJER?

Digitaliseringen av skolen legger grunnlaget for å drive læringsanalyse basert dataene som legges igjen i de ulike verktøyene. Troen på Big Data, og hvordan analyse av enorme datamengder kan gi store gevinster, preger i dag nær sagt alle sektorer - også skolesektoren. Tradisjonelt har vi tenkt på "elevdata" som karakterutskriften, individuelle oppgaver, testresultater, disiplinære forhold, demografiske data. Men de administrative og pedagogiske systemene som brukes i skolen i dag kan spore så mye mer. For å lære mest mulig om hver enkelt elev er det ønskelig å sammenstille mest mulig data om den enkelte. Fremover kan det derfor bli interessant å kombinere elevenes testresultater og data om deres foreldres utdanningsnivå med opplysninger om hvilke sider elevene leser i de digitale lærebøkene, hva de markerer i disse bøkene, deres søkehistorikk på nett, hvor mye tid de har brukt på Facebook i skoletiden og hvilke videoer de har sett på Khan Academy.

Læringsanalyse er omtalt som en av de viktigste teknologiske trendene i norsk utdanning. Senter for IKT i utdanningen spår at læringsanalyse vil bli tatt i bruk i norsk skole i et fire- til femårs perspektiv[32]. Fronter, itsLearning og Kikora legger allerede i dag til rette for slik analyse i sine systemer. To andre systemer som gir grunnlag for læringsanalyse er VOKAL og PULS. VOKAL brukes av 80 prosent av grunnskolen. Dette verktøyet samler, sorterer og viser lærerne hvordan enkeltelever og klassen har gjort det på ulike kartlegginger og tester. PULS ser ikke på enkeltelever, men gir en samlet oversikt over utviklingen i en klasse, skole eller et skoleområde gjennom hele skoleløpet[33].

Metodene som brukes i læringsanalyse er de samme som Google og Amazon bruker når de analyserer forbrukertrender og forbrukeratferd. Hensikten er også den samme – å bruke data for å tilpasse produkter og tjenester til den enkelte bruker. Sammenstilling av opplysninger lagret i ulike digitale læringsressurser muliggjør analyser som tidligere ikke har vært mulig. Kunnskapen som hentes ut brukes til å utvikle modeller for å forutsi hvordan elevgrupper lykkes med studiene, hvordan de lærer og hvilke behov de har. Formålet er å gi elevene individuelt tilpasset undervisning og å identifisere elever som står i fare for å falle utenfor slik at relevante tiltak kan settes inn på et tidlig tidspunkt. Da vil man også kunne optimalisere nytteverdien av digitale læremidler.

«School of one» er et eksempel på et læringsanalyseverktøy som er innført i offentlige skoler i New York City. I dette verktøytet benyttes læringsalgoritmer til å analysere elevenes læringsstil og matematikkferdigheter. Algoritmen produserer en personlig «læringsliste» i matematikk for hver elev, som følger den progresjonen som er beregnet å være optimal for hver enkelt.

[32] «Teknologiske framtidsutsikter for norsk skole i 2013 – 2018 – en regional analyse fra NMC Horizon Project», et samarbeid mellom New Media Consortium og Senter for IKT i utdanningen, 2013. http://iktsenteret.no/sites/iktsenteret.no/files/attachments/horizon_2013-technology-outlook-for-norwegian-schools-en.pdf

[33] http://www.conexus.no/blog/2014/10/16/conexus-deler-erfaringene-med-laeringsanalyse/

PERSONVERNUTFORDRINGER

«Students profile should not become etched like a tattoo into their digital skins. » [34]

Digitale tatoveringer

Læringsanalyse kan gi den enkelte bedre og mer tilrettelagt undervisning, men storstilt innsamling, lagring og analyse av elevopplysninger kan også medføre personvernutfordringer. Det kan være utfordrende for den enkelte elev, og elevenes foresatte, å følge med på hvordan personopplysninger deres behandles og hvilke formål de benyttes til. Formålsbestemthet er et viktig prinsipp i personvernet. Det betyr at før noen samler inn personopplysninger skal de ha avklart formålet med innsamlingen, det vil si hva de skal brukes til. Når dette er avklart skal ikke opplysningene brukes til andre formål. Dette skal garantere forutsigbarhet knyttet til hva personopplysningene man gir i fra seg blir brukt til.

Det er særlig bruk av såkalt prediktiv analyse som kan medføre personvernutfordringer. Kunnskapsdepartementet har nylig ferdigstilt en utredning som har som målsetting å innføre læringsanalyse, herunder prediktiv analyse, i høyere utdanning[35]. Prediktiv analyse har som mål å forutsi hver enkelt elevs prestasjoner. For å få til dette må man kombinere mest mulig data om eleven. Det er vanskelig å se for seg hvilke rammer som skal gjelde for denne typen læringsanalyse, og hva som er yttergrensene for hvilke opplysninger skolen vil vurdere som nyttige i en slik sammenheng. Det vil for eksempel kunne argumenteres med at en god prediktiv analyse krever at skolen kan registrere, lagre og bruke opplysninger om det meste av det eleven foretar seg i løpet av skolegangen i tillegg til elevenes sosiale profil og forhistorie. En slik bred datafangst utfordrer prinsippene om at minst mulig, og kun relevante data skal lagres om den enkelte. I tillegg vil det være utfordrende for elevene å forstå eller forutse hva alle opplysningene som samles inn om dem samlet sett vil vise. Hvilket bilde sitter skolen igjen med om dem basert på alle dataene som er samlet inn?

Hvilke konsekvenser kan det ha for barn hvis de må dra med seg en hale av digitale spor fra barnehagen og oppover i skolesystemet, spor som hele tiden vil legge premisser for hvordan de behandles? Forfatter Eli Pariser har uttalt

---

[34] Slade, Sharon and Prinsloo, Paul: "Learning analytics: ethical issues and dilemmas". American Behavioral Scientist, 57(10) pp. 1509–1528., 2013

[35] NOU 2014: 5. «MOOC til Norge - Nye digitale læringsformer i høyere utdanning»

at en fare ved Big Data er at vi blir gjort til fanger av våre tidligere valg[36]. Vil vi utstyre våre barn med digitale tatoveringer som vil få avgjørende innflytelse på deres videre livsløp? En gang urokråke, alltid urokråke?

Retten til å bli glemt er et viktig personvernprinsipp. Dette prinsippet innebærer at det skal være mulig for enkeltindividet å starte på nytt med blanke ark og at man ikke skal vurderes og dømmes på bakgrunn av hva man har gjort tidligere. Dette er særlig viktig for barn. Barn forandrer seg, modnes og utvikles hele tiden. Bruk av dataanalyse i skolen må ta hensyn til dette.

Det er også viktig å være klar over at elevers suksess eller feilgrep er et komplekst og flerdimensjonalt fenomen og alt kan ikke forklares ved å studere data alene. Det er svært uheldig hvis vi får en utvikling der elever utelukkende vurderes ut fra hva dataene om dem sier de vil komme til å gjøre, og ikke på bakgrunn av hva de faktisk gjør.

ELEVOPPLYSNINGER SOM BETALINGSMIDDEL

HVA SKJER?

Personopplysninger har lenge vært en attraktiv handelsvare og et fundament for utvikling av nye tjenester. De siste par årene har utdanningssektoren vokst frem som et nytt og attraktivt marked for datainnhøsting både blant etablerte IT-kjemper som Google og Apple, og blant nye nisjeselskaper. I USA er mange bekymret for at den økende digitaliseringen av skolen vil gjøre klasserommet om til et «showrom» for konkurrerende aktører i den fremvoksende «læringsindustrien»[37].

Skoleeierne mangler ofte kunnskap og kapasitet til å sette krav til produkter og tjenester som de kjøper. Det blir derfor i stor grad leverandørene som setter standarden for personvernet og sikkerheten i løsningene. I tillegg har skolene stramme budsjetter å forholde seg til, og de mange gratis læringsressursene

[36] Victor Mayer-Schonberger, Victor: "Delete: The Virtue of Forgetting in the Digital Age", 2009, Princeton University Press
[37] Polonetsky, Jules and Omer Tene: «The Ethics of Student Privacy: Building trust for Ed Tech», International Review for Information Ethics, vol. 21 (07/2014), http://www.i-r-i-e.net/inhalt/021/IRIE-021-Polonetsky-Tene.pdf

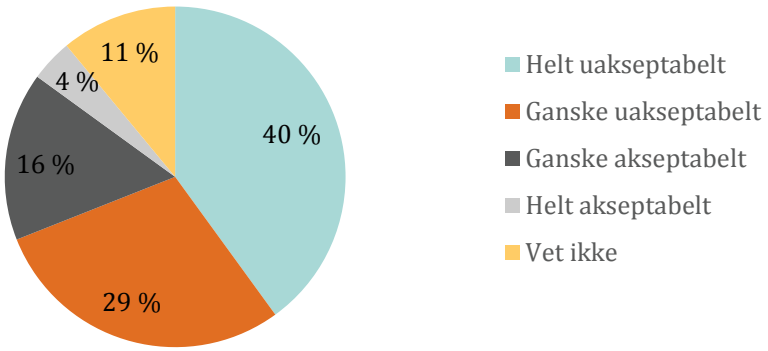
som finnes på markedet representerer derfor et attraktivt alternativ til kostbare betalingstjenester. «Gratis» applikasjoner har imidlertid en pris. Valutaen det betales i er elevenes personopplysninger. Identitet, kjønn, alder, interesser, tilstedeværelse, prestasjoner, kontakter, kalender etc. er opplysninger som er verdt milliarder i en industri i kraftig vekst. Selskaper er ivrige etter å samle inn og aggregere elevdata som de kan bruke til å forbedre sine egne analyseverktøy eller selge videre til kommersielle aktører som vil nå skoleelever med sine produkter.

PERSONVERNUTFORDRINGER

For noen elever og deres foresatte vil det være akseptabelt å betale med sine personopplysninger, for andre ikke. Det problematiske med bruk av personopplysninger som betalingsmiddel i skolesektoren er at det ikke er eleven selv som tar avgjørelsen. Det er skoleeieren som aksepterer betaling med personopplysninger på vegne av elevene.

Når elevopplysninger samles inn av tredjeparter via digitale verktøy kan det også bli uklart hvem som eier opplysningene. Er det selskapet som samler inn opplysningene, skolen eller eleven?

I en spørreundersøkelse gjennomført av Teknologirådet og Datatilsynet i desember 2014, svarte 40 % av de spurte at det var *helt uakseptabelt* og 29 % at det var *ganske uakseptabelt* at skolene benytter gratis læringsverktøy mot at selskapene kan benytte opplysningene samlet inn om elevene til egne formål.



Den samme sterke motstanden mot at kommersielle selskaper benytter elevdata til egne og nye kommersielle formål ser vi i USA, der bruken av slike verktøy har kommet lengre enn i Norge[38]. I 2014 valgte InBloom, et av de største selskapene innen dataanalyse i skolesektoren i USA, å legge ned virksomheten etter sterk kritikk fra foreldre og foreldresammenslutninger. Til tross for at det ikke ble påvist at selskapet hadde misbrukt informasjonen de samlet inn om elevene, reagerte foreldre på at enorme mengder med elevdata ble samlet inn og analysert av et kommersielt selskap, uten at elevene hadde mulighet til å reservere seg mot det[39].

[38] The New York Times: «With Tech Taking Over in Schools, Worries Rise», 14. september 2014, http://www.nytimes.com/2014/09/15/technology/with-tech-taking-over-in-schools-worries-rise.html?_r=0
[39] Bloomberg Businessweek: «Privacy Fears Over Student Data Tracking Led to InBloom's Shutdown», 1. Mai 2014, http://www.businessweek.com/articles/2014-05-01/inbloom-shuts-down-amid-privacy-fears-over-student-data-tracking

HVA KAN VI GJØRE?

SKOLEEIERE MÅ BLI BEDRE BESTILLERE

Skoleeiere må bli bedre bestillere av digitale tjenester. Skolene må stille større krav til utviklerne av nye verktøy, og i mindre grad kjøpe hyllevare eller bruke nettbaserte tjenester som ikke er tilpasset deres behov. Det pågår for tiden et arbeid med å utvikle en norm for bruk av digitale tjenester i utdanningssektoren. Denne normen vil danne et godt grunnlag for å gjøre skoleeierne til mer bevisste bestillere.

En forutsetning for å bli bedre bestillere er at skoleeierne forstår hvilke personvernutfordringer bruken av nye digitale verktøy medfører. Mange misforstår for eksempel hva personopplysninger omfatter. De vet ikke at det favner svært mye videre enn fødselsnummer, navn og adresse. Personopplysninger er alle opplysninger som kan knyttes til enkeltpersoner, som for eksempel: bilder, kommunikasjon mellom elever/lærere/hjem, informasjon om allergier, logg fra elevers bruk av skolens nettverk, apper og liknende.

Kontroll over elevopplysningene som samles inn

Skoleeiere må ha kontroll over elevopplysningene som samles inn av ulike digitale verktøy. Hvis skolen benytter digitale verktøy der elevopplysningene tilflyter tredjeparter, må skoleeier sørge for å etablere avtaler som sikrer at de vet hvilke opplysninger som samles inn, hvordan de behandles og hvem som har tilgang til dem. Hvis de ikke vet dette, er det vanskelig å gi elever og foreldre den informasjonen de har krav på for å kunne ivareta sitt eget personvern.

Mer åpenhet og tydelig formål

Bruk av datadrevet undervisning og læringsanalyse vil føre til at skolene etter hvert vil sitte på store datamengder om elevene, som sammenstilt og analysert kan gi et nærgående bilde av den enkelte. For at skolene skal ivareta tillitsforholdet de har med elevene, må skolene være bevisste, tydelige og åpne om hvilke data verktøyene samler inn og hvordan de brukes. I denne sammenheng er det spesielt viktig at skolene tydelig kommuniserer til foreldre og elever hvilket *formål* bruken av læringsanalyse har. Er formålet å tilpasse undervisningen til hver enkelt elev (pedagogiske formål), er det å kontrollere at elevene gjør det de skal (rapporteringsformål) eller er det å effektivisere

virksomheten (økonomisk formål)[40]? Mangel på åpenhet om bruken av data-analyse, kan føre til mistillit mellom skole og elev/hjem.

Når skolen er åpen om formålet kan elevene å ha et aktivt og kritisk forhold til bruken av verktøyet, og det skaper forutsigbarhet rundt bruken. Elevene skal være trygge på at bruken av dataanalyse i skolen ikke får karakter av å være enveis overvåking (*panoptisk overvåking*). Elever og foreldre må sikres innsyn i de opplysningene om dem som ligger lagret og som danner grunnlag for profilbyggingen. Dette er viktig for at de skal kunne kontrollere at både opplysningene i seg selv, og beslutningene som fattes på grunnlag av disse opplysningene, er korrekte.

Utløpsdato på elevopplysninger

Dataanalyse må ta hensyn til at elevenes identitet er i konstant endring. Data som samles inn gjennom læringsanalyseverktøy bør av derfor ha en utløpsdato, og elever må ha mulighet til å be om at data slettes etter bestemte kriterier.

[40] Slade, Sharon and Prinsloo, Paul: "Learning analytics: ethical issues and dilemmas". American Behavioral Scientist, 57(10) pp. 1509–1528., 2013

HAR BARN RETT TIL PRIVATLIV?

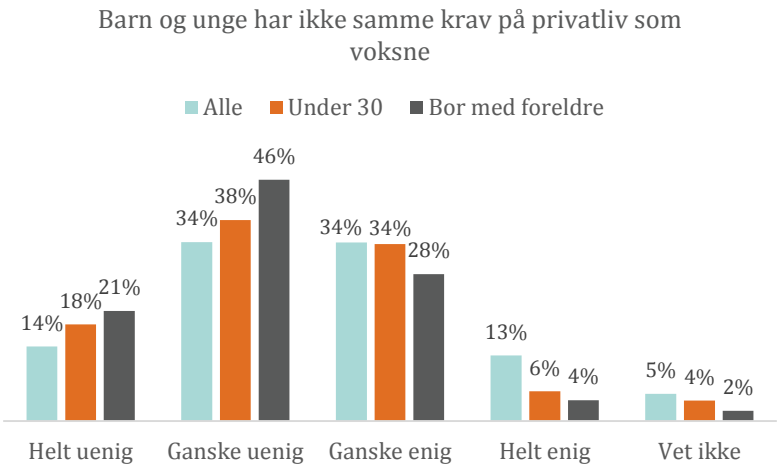
Har barn rett til privatliv? Er det ok at foreldre snoker i sine barns profiler på sosiale medier for å sjekke hva de driver med? Er det greit at foreldre plasserer sporingsteknologi på åtteåringen i Legoland, eller på tenåringen som er alene ute på kvelden? Før hadde ikke foreldrene noe valg, de måtte stole på at det gikk bra når de slapp barna ut døra. Nå har vi teknologi som gjør det mulig for foreldre å følge med på hvor barna er til enhver tid. I årets personvernundersøkelse ønsket vi å finne ut hvilke holdninger folk har til barns rett til privatliv. I hvilken grad er det akseptabelt at foreldre sporer og overvåker sine barn, på og utenfor nett?

BARNS KRAV TIL PRIVATLIV STØTER MOT ANDRE HENSYN

Barns rett til privatliv er nedfelt i FNs barnekonvensjon. Der står det at barn ikke skal utsettes for vilkårlig eller ulovlig innblanding i sitt privatliv, i familien, i hjemmet eller i sin korrespondanse. Barn og unge har i personopplysningsloven samme rett på personvern som voksne.

Med jevne mellomrom dukker det opp debatter i mediene der ulike aktører tar til orde for at foreldre må overvåke barna for å få oversikt og kontroll med hva de driver med. Vi ville derfor finne ut hvor utbredt oppfatningen om at barn ikke har samme krav på privatliv som voksne er?

TNS Gallup har gjort undersøkelsen via sitt nettpanel, og 1091 innbyggere fra 15 år og oppover har besvart den.



Svarene viser verken en klar støtte eller en klar avvisning av påstanden om at barn og unge ikke har samme krav på privatliv som voksne. Respondentene grupperer seg ganske likt rundt alternativene «ganske uenig» og «ganske enig». At de spurte ikke uttrykker et klart syn på dette spørsmålet kan tyde på at det er vanskelig å ta stilling til. Selv om barn har krav på privatliv er de, i motsetning til voksne, avhengig av å bli passet på. Det kan være derfor mange tenker at barns rett til privatliv må vurderes annerledes enn voksnes rett til privatliv.

Kjønn, utdanning, inntekt og hvor i landet man bor har liten betydning for om man er enig eller uenig. Alder og hvem man oppgir at man bor sammen med, har størst betydning for hva folk svarer. I aldersgruppen under 30 år mener et flertall av de spurte at barn har samme krav på privatliv som voksne. Ser vi på svarene til gruppen som oppgir at de bor med sine foreldre, blir bildet enda tydeligere - 67 prosent av de som bor med sine foreldre, er uenig i påstanden av at barn ikke har samme krav på privatliv som voksne. Sistnevnte gruppe omfatter få respondenter og det hefter derfor ganske stor statistisk usikkerhet knyttet til prosentandelen. Vi har likevel valgt å ta med denne bakgrunnsvariabelen fordi denne gruppen gir uttrykk for et ganske annet syn på barns rett til privatliv enn gjennomsnittet. Gruppen som bor hjemme med sine foreldre omfatter respondenter som er nærmest til å føle på kroppen hvordan barn og

unges privatliv kan utfordres av foreldrenes behov for å følge med på hva barna driver med. Nesten alle i denne gruppen er under 30 år.

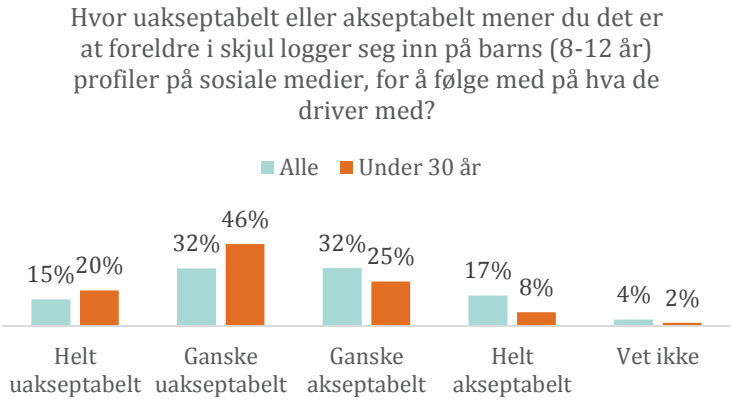
Hva sier loven?
Barn og unge har samme krav på personvern som voksne. Barns personvern er imidlertid i første rekke ivaretatt av den som har foreldreansvaret til barna. I de fleste situasjoner samtykker foreldre på vegne av sine barn der samtykke er påkrevd. I 2012 ble det lagt til en ny bestemmelse i personopplysningsloven for å gi ekstra beskyttelse av barn og unges personvern. Den nye bestemmelsen sier at personopplysninger som gjelder barn ikke skal behandles på en måte som er *uforsvarlig* av hensyn til barnets beste. Hensikten med bestemmelsen er å styrke barns personvern ved å gjennomføre ordlyden i FNs barnekonvensjon i personopplysningsloven. Med den nye bestemmelsen skal Datatilsynet for eksempel kunne gripe inn i de alvorligste tilfellene av publisering av krenkende opplysninger om barn foretatt av foreldre.

ER SNOKING OK?

Høsten 2014 raste en debatt i mediene om foresattes innsyn i egne ungdommers private kommunikasjon på Facebook og lignende medier. En far skrev en kronikk der han beskrev metodene han brukte for å tilegne seg kunnskap om ungdommenes liv utenfor foreldrekontroll[41]. En barnepsykolog fulgte opp med en uttalelse om at alle foresatte har plikt til å sjekke barnas bruk av sosiale medier[42].

I lys av denne debatten ønsket vi i årets undersøkelse å finne ut hvor akseptabelt folk synes det er at foreldre – i skjul – logger seg inn på sine barns eller ungdommers profil på sosiale medier. Vi ønsket også å undersøke om folk synes det er mer akseptabelt at foreldre i skjul logger seg inn på de mindre barnas profil på sosiale medier enn at de gjør det samme på de eldste barnas profiler.

[41] http://www.vg.no/nyheter/meninger/kronikk-en-raatten-ungdomskultur-og-dumme-foreldre/a/23309225/
[42] http://www.vg.no/nyheter/innenriks/oppvekst/barnepsykolog-sjekk-ungenes-facebook/a/23309769/



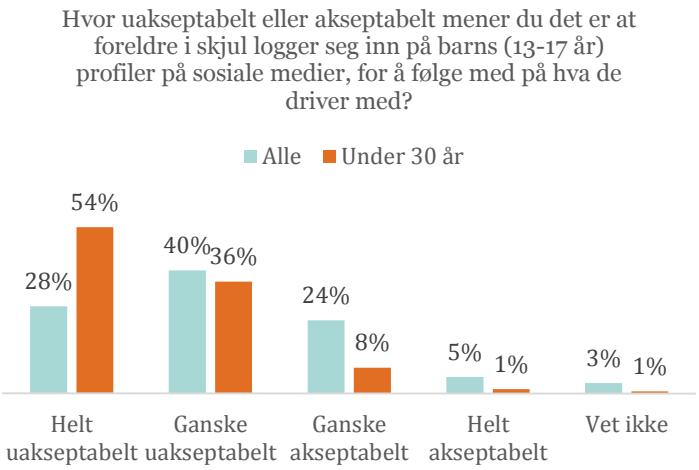
Respondentene er akkurat som i synet på barns rett til privatliv, delt i synet på om det er uakseptabelt eller akseptabelt å logge seg inn på barnets sosiale profil i skjul. Omtrent like mange mener det er akseptabelt som uakseptabelt.

Vi er overrasket over at så mange synes dette er akseptabelt. Å logge seg inn på barnets lukkede profil på sosiale medier, og i tillegg gjøre dette i skjul, er en inngripende fremgangsmåte for å følge med på hva barnet driver med. Det finnes andre måter å følge med på. Foreldre kan snakke med barnet og de kan sette seg ned sammen med barnet slik at barnet selv kan vise hva som skjer på de sosiale mediene der de deltar.

Vi tror forklaring på at så mange finner denne fremgangsmåten akseptabel, er at barna i dette tilfellet er under 12 år. Mindre barn krever tettere oppfølgning. Mange føler nok at dette rettferdiggjør, eller nødvendiggjør, at man tar i bruk mer inngripende metoder for å følge med på hva barna driver med, enn hva som er naturlig overfor eldre barn. Som vi skal se støtter langt færre bruk av denne fremgangsmåten overfor ungdommer.

Aldersgruppen under 30 år skiller seg ut ved at de tar tydelig avstand fra denne fremgangsmåten for å følge med på barns nettliv, også overfor de minste barna. Et stort flertall, 66 prosent, i denne gruppen synes det er uakseptabelt at foreldre i skjul logger seg inn på profilene til barn under 12 år. Aldersgruppen under 30 år har, til forskjell fra de eldre aldersgruppene, vokst opp med Internett. Det er generasjonen av såkalt *digitalt innfødte*. Store deler av deres

sosiale omgang og aktiviteter utspiller seg i sosiale medier. Denne aldersgruppen opplever nok derfor i større grad dette som en inngripende form for foreldrekontroll enn de som er eldre og som ikke har tilsvarende erfaring med å vokse opp på nett. Dette er også den aldersgruppen i undersøkelsen som har den ferskeste erfaringen med å være under foreldrenes omsorg. Personvernundersøkelsen i fjor viste også at aldersgruppen under 30 år i noe større grad enn de de over 30 år oppga at de var «svært opptatt» av personvern[43].



Undersøkelsen viser at flertallet av de spurte mener det er uakseptabelt at foreldre i skjul logger seg inn på ungdommenes profiler på sosiale medier.

Kun 5 prosent mener det er helt akseptabelt å logge seg inn på profilen til et barn mellom 13 og 17 år i skjul. Dette kan tyde på at de fleste støtter og respekterer ungdommens rett til å ha et privatliv.

Aldersgruppen under 30 år er særlig tydelig på at det er uakseptabelt av foreldre å i skjul logge seg inn på ungdommens profiler på sosiale medier. Ni av ti tar avstand fra denne fremgangsmåten for å følge med på hva barna driver med.

[43] http://www.datatilsynet.no/Global/04_planer_rapporter/Persovern_tilstandogtrender_2014.pdf

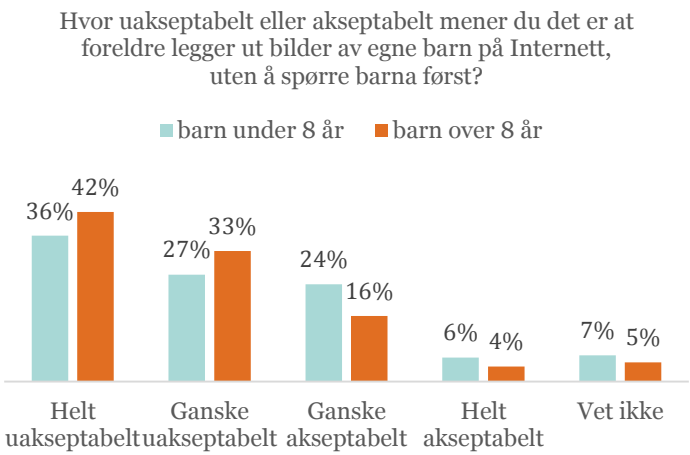
Bakgrunnsvariablene kjønn, utdanning, inntekt og hvor i landet man bor har liten betydning for hva respondentene svarer på disse to påstandene.

DELING AV BILDER AV BARN

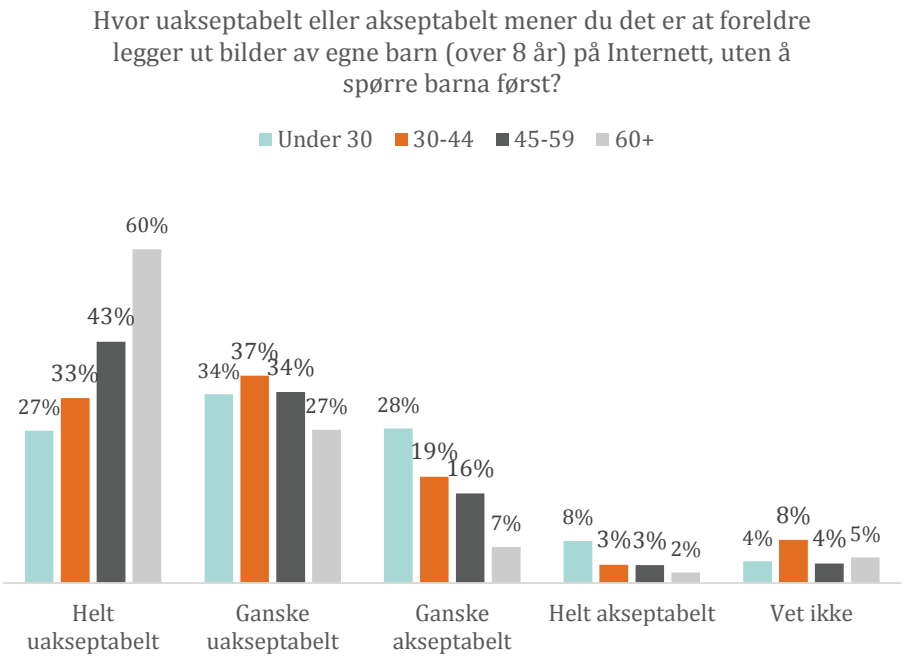
Foreldre deler ivrig bilder av sine barn på nett. De fleste deler bilder som viser gode øyeblikk, fine minner fra ferier og prestasjoner i idrett og fritid. Men mange foreldre deler også bilder som barna kanskje, enten i dag eller senere, opplever som pinlige og flaue.

Før man publiserer portrettbilder på nett må man be om samtykke fra den eller de som er avbildet. Publiserer man familiebilder skal man derfor ha samtykke fra alle som kan identifiseres på bildene. Ved publisering av bilder av barn og unge, samtykker foreldrene på vegne av barnet – det vil si at de tar avgjørelsen om et bilde skal publiseres eller ikke. Derfor er det viktig at foreldre viser aktsomhet når de legger ut bilder av barna. Foreldre bør for eksempel spørre barna om lov før de legger ut bilder av dem, selv om det ikke er et krav at man skal gjøre dette. Da vil foreldrene være gode forbilder og bidra til å lære de unge kjøreregler for hva de kan legge ut på nett om seg selv, og at de skal respektere andres grenser for hva de vil ha liggende ute på nett.

Vi ønsket å finne ut i hvor stor grad folk synes det er akseptabelt eller uakseptabelt at foreldre legger ut bilder av barna sine uten å spørre først.



Med tanke på det enorme volumet med bilder av barn som legget ut på nett hver dag, er det overraskende at så få mener det er akseptabelt å legge ut bilder av barn uten spørre først. Kun seks prosent synes det er helt akseptabelt å legge ut bilder av barn under åtte år uten å spørre først, og bare fire prosent synes det er helt akseptabelt å publisere bilder av barn over åtte år uten å spørre først. Majoriteten svarer at det er helt eller ganske uakseptabelt å gjøre dette. Svarene viser litt større aksept for å legge ut bilder av barn under åtte år enn av barn over åtte år, uten å spørre først. I motsetning til for de foregående påstandene, er det også flere som gir uttrykk for et klart syn på dette spørsmålet. Svaralternativet «helt uakseptabelt» får størst oppslutning når det gjelder begge aldersgruppene. Selv om flertallet av de spurte mener at barna skal spørres før foreldrene legger ut bilder av dem, er det grunn til å være kritisk til hvorvidt flertallet av befolkningen faktisk gjør dette i praksis.



Aldersgruppen under 30 år har på de foregående spørsmålene skilt seg ut som den gruppen som har gitt sterkest uttrykk for barns rett til personvern. På dette spørsmålet er det imidlertid den yngste aldersgruppen som har minst problemer med at bilder av barna legges ut uten at det spørres først. Det er

den eldste aldersgruppen – besteforeldregenerasjonen – som er mest kritisk til dette. Dette henger trolig sammen med at de eldre ikke i samme grad er vant til delingskulturen på Internett, og at de derfor generelt er mer skeptisk til å legge ut bilder på nett. Kanskje skyldes det også en annen holdning til det å dele privat informasjon. De under 30 år er mer vant til at det legges ut bilder av dem uten at de blir spurt først.

Menn synes i noe høyere grad enn kvinner at det er akseptabelt å legge ut bilder av barn, både over og under åtte år, uten å spørre først.

EN SPORET BARNDOM

Foreldre som bekymrer seg for barna sine når de er ute på egenhånd, kan etter hvert velge og vrake blant tekniske løsninger som følger med på hvor barna er. En ørliten sporingsbrikke kan festes på klærne til barnet. En «app» som gjør det mulig å kontrollere hvor barnet er kan installeres i podens smarttelefon. Foreldre kan også velge å utstyre sine barn med fargerike arm- og ankelbånd, utstyrt med GPS og panikk-knapp som barnet kan trykke på hvis det behøver hjelp. Enkelte armbånd kommer også med innebygget mikrofon slik at foreldrene kan høre hva som skjer hvis de ikke klarer å nå barnet på annen måte[44].

> *«Barn og eldre er ideelle kunder for kroppsnær teknologi»*
>
> Dr. Jong-seok Park, CEO i LG Electronics Mobile Communications Company[45]

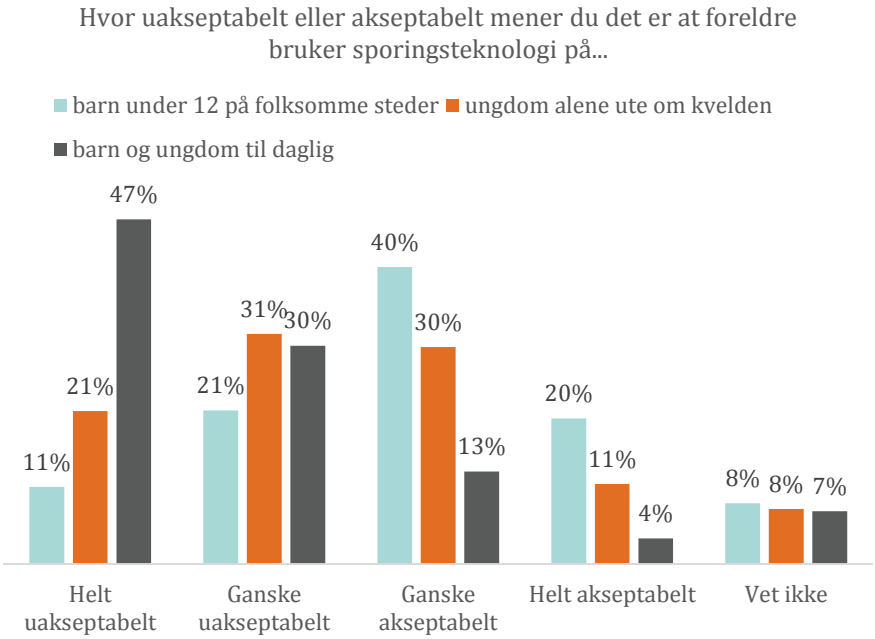
I likhet med eldre med nedsatt funksjonsevne, har også barn et ekstra omsorgsbehov. De kan gå seg vill, de kan bli utsatt for uønsket og farlig oppmerksomhet eller de kan komme opp i farefulle situasjoner fordi de ikke kan vurdere risiko godt nok. Personer med demens kan få mer frihet når de bruker sporingsutstyr som sikrer at de blir funnet igjen hvis de går seg bort. Men får barn mer frihet hvis de er prikker på et kart på foreldrenes telefoner?

I fjorårets personvernundersøkelse spurte vi om folk kunne tenke seg å bruke GPS-sporing på henholdsvis eldre og barn. 76 prosent svarte at de kunne tenke seg å bruke GPS-sporing på eldre eller andre familiemedlemmer med

[44] http://www.cbsnews.com/news/wearable-gps-tracking-for-children-to-ease-parents-minds/
[45] http://koreabizwire.com/introducing-lg-kizon-a-wearable-designed-for-kids/14367

særlig omsorgsbehov. 25 prosent svarte at de kunne tenke seg å bruke slikt utstyr på egne barn[46].

I årets undersøkelse ønsket vi å finne ut hvor akseptabelt folk synes det er at foreldre bruker sporingsteknologi på egne barn og ungdommer.



Undersøkelsen viser tydelig at det ikke er støtte blant folk til å spore barn og unge til daglig. Hele 77 prosent mener dagligdags bruk av sporingsteknologi på egne barn er uakseptabelt.

Folk er imidlertid mer åpne for å bruke sporingsteknologi på barn i helt konkrete situasjoner. Et stort flertall av de spurte, til sammen 60 prosent, oppgir at de synes det er akseptabelt å bruke sporingsteknologi på barn under 12 år på folksomme steder. Å bruke sporingsteknologi på ungdommer når der er alene ute om kvelden, har imidlertid langt mindre støtte. Et mindretall av de spurte, 41 prosent, mener dette er akseptabelt.

[46] http://www.datatilsynet.no/verktoy-skjema/Publikasjoner/Personvernundersokelser/Personvernundersokelsen-2013-delrapporter/

Menn og kvinner har tilnærmet lik holdning til det å ta i bruk sporingsteknologi overfor egne barn. Aldersgruppen under 30 år skiller seg ut som den aldersgruppen som er mest avvisende til å ta i bruk sporingsteknologi på barn.

Fra et personvernperspektiv er det et viktig prinsipp at man skal kunne bevege seg fritt uten at man blir kontrollert og overvåket hele tiden. Personvern handler om autonomi og muligheten til å få utvikle sin egen personlighet uten å hele tiden å være observert og kontrollert av andre. Dette er vel så viktig for barn som for voksne.

Teknologien gjør det mulig å følge med på hvor barna er til enhver tid. Kommersielle krefter vet å utnytte foreldres bekymring for sine barn til å selge nye produkter. Vil det at teknologien finnes bidra til å skape et sosialt press om å ta den i bruk? Vil foreldre som ikke utstyrer barna med sporingsutstyr før de sender dem ut døra, bli sett på som uansvarlige i fremtiden? Vår undersøkelse viser at vi foreløpig ikke er kommet dit i dag.

TINGENES INTERNETT

«Tingenes internett» betyr at gjenstander som termostaten, joggeskoene og bilen blir smarte. De utstyres med sensorer og nettilkobling og kan automatisk samle, tolke og dele informasjon om når du står opp, hvor effektivt du trener, og hvor aggressivt du kjører bil.

HVA ER TINGENES INTERNETT?

I januar i år var det tingenes internett alle snakket om på CES-konferansen (Consumer Electronics Show), som er en årlig trendmåler for IT-bransjen. Samsung-sjef Yoon Boo-Keun erklærte i sin tale at samtlige Samsung-produkter innen fem år vil være klare til å koble seg på internett. [47]Det vil si at utviklingen de siste årene fra TV til smart-TV som er på nett, også vil skje med eksempelvis frysere og vaskemaskiner.

De enorme mengdene informasjon som i dag er tilgjengelige på internett, er i stor grad generert av mennesker som taster inn tekst, tall eller søkeord, eller tar bilder og video som lastes opp på nett. Tingenes internett, derimot, handler om at smarte ting automatisk genererer informasjon fra vårt fysiske liv, uten at vi bruker tid på det eller legger merke til det.

HVORDAN GJØRE DUMME TING SMARTERE

Datamaskiner som før var store og dyre, er nå på størrelse med en fingertupp og koster mindre enn en kopp kaffe.

Mens PC-er og smarttelefoner har skjerm og tastatur som vi bruker aktivt når vi surfer på nett, betaler regninger eller spiller spill, er de smarte tingene små, nesten usynlige og registrerer omgivelsene uten at vi trenger å gjøre noe selv.

[47] http://www.ft.com/intl/cms/s/0/9df9a21c-9556-11e4-8fc1-00144feabdc0.html#axzz3PHbtkIfO

Nær sagt alle ting kan bli smarte ved å utstyre dem med:

- **Sensorer** som kan måle temperatur, bevegelse, luftfuktighet mm.
- **Prosessorer** som kan telle eller gjøre beregninger på målingene som gjøres, som gjennomsnittstemperatur over tid eller telle antall personer som har passert et målepunkt.
- **Lagringsenheter** som kan lagre måledataene og beregningene for senere bruk.
- **Nettilkobling** som gjør det mulig å overføre data og instruksjoner til og fra tingen.
- **Batteri** som sørger for at de smarte tingene faktisk virker.

FRA SMARTE TING TIL PERSONLIGE TJENESTER

Når ting kobles til internett kan vi lage tjenester på flere nivåer, fra det enkle til det avanserte.

I sin enkleste form innebærer tingenes internett at vi kan overvåke og styre tingene rundt oss. For eksempel kan vi få en alarm hvis stekeplaten går over en gitt temperatur, sette på varmeapparatet i bilen fra sofaen eller sørge for at lysene blir dimmet kl. 22 hver kveld.

Flere sensorer kan kobles sammen i nett. Smarttelefonen eller nettbrettet gir oversikt over sensorene, gjør beregninger og styrer dem slik at de til sammen oppfører seg optimalt. For eksempel kan den beregne når bilen trenger service basert på informasjon fra sensorene i bilen, i stedet for antall kilometer kjørt som i dag.

Tingene kan også lære av tidligere erfaringer og av omgivelsene, og automatisk tilpasse seg brukernes vaner. Den smarte termostaten Nest lærer seg i løpet av en uke når familien legger seg og hvor mye den da skal senke temperaturen i huset. Enda mer avansert er Google-bilen som kan kjøre selv, fange opp trafikkbildet rundt seg, og tilpasse seg omgivelsene for å kjøre trygt.

Ut fra informasjonen de smarte tingene samler inn og genererer, kan det lages nye tjenester. Smarte hus kan sende varsler og alarmer når noe urovekkende skjer i huset. Sensorer på komfyren varsler familiemedlemmer når noen har

glemt å skru av en plate. Hvis ingen reagerer kan de sende en alarm til et vaktselskap eller brannvesenet.

Her ligger også muligheter for enorme samfunnsmessige gevinster. Energieffektiviseringen vi kan oppnå med smarte hus, smarte biler og smart trafikkkontroll kan spare samfunnet for mye energisløsing. Tryggheten som smarthustjenester gir kan gjøre at eldre kan bo lengre hjemme, og vil potensielt kunne spare samfunnet og enkeltpersoner for mange ressurser.

HJEMMESEIER FOR SMARTE DINGSER

I 2010 startet Tony Fadell opp Nest Labs sammen med Matt Rogers fordi han ikke klarte å finne en termostat som gjorde det han ønsket. Resultatet ble smarttermostaten Nest, som lærer av oppførselen din.

I løpet av en uke har termostaten dannet seg godt bilde av hvor ofte og hvor mye du justerer temperaturen, og når på døgnet det skjer. Etter den første uken gjør den det selv automatisk. Ved hjelp av sensorer plassert på ulike steder i huset registrerer Nest-termostaten aktivitet, og mangel på aktivitet. Sensorene registrerer blant annet temperatur, lys fra omgivelsene, luftfuktighet og bevegelse for å optimalisere den automatiske prosessen og forstå bedre hvordan familien lever.

Nest holder et øye med forbruket ditt og sender deg en rapport hver måned, hvor den også gir deg stjerne i margen hvis du har vært en flink energisparer. Nest er koblet til Wifi, og kan – uavhengig av hvor du er – kontrolleres via en app som også kan motta alarmer og varsler.

I tillegg til termostaten har Nest også produsert en smart røykvarsler. Den kan merke om røyken kommer fra brent brød eller karbonmonoksid, og sier muntlig fra hva det er og hvor. Den gir også beskjed på mobilen i tilfelle du ikke er hjemme.

Det vi ser er at Nest skaper noe mer enn et par produkter, de tilbyr også tjenester som energi og forbrukssparing, og sikkerhet og trygghet for familien og hjemmet. Det er disse tjenestene som gjør tingenes internett virkelig interessant. Tingene kjenner deg og dine vaner, både på nett og i den fysiske verden, og tilpasser tjenestene deretter. Teknologien går i ett med hverdagen og vi merker knapt at noe skjer.

DET SMARTE NORSKE HUS

Energiselskapet Lyse tilbyr nå 160 000 husstander å sørge for at boligens strøm, lys, varme, alarm og inngangsdør snakker sammen, slik at familien enkelt kan fjernstyre hjemmet fra mobilen.

Bakgrunnen for dette er at myndighetene krever at alle bygninger i Norge installerer smarte strømmålere, også kalt AMS (Advanced Metering Systems) innen 1.1. 2019. Målet er å øke bevisstgjøringen om eget strømforbruk. Myn-

dighetene ønsker at kundene skal bruke tjenester som analyserer data fra strømmåleren og hjelper dem å optimalisere energiforbruket sitt.[48]

I Norge har Lyse begynt å installere både automatiske strømmålere og styringssystemer som gjør det mulig å sette opp ulike sensorer i hjemmet som kommuniserer med hverandre. Systemet styres fra en app på mobilen, en fjernkontroll eller et panel på veggen.[49]

Noen av varslene fra sensorene i huset kan kobles til eksterne tjenestetilbydere. Tyverialarmen sendes til et alarmselskap og brannalarmer til brannvesenet. Disse rykker ut når det er behov for det, noen som skaper trygghet for beboerne. Her er det ikke sensorene som er hovedproduktet. Det er *tjenestene* som er produktet, og det er tryggheten for at noen rykker ut ved behov som kundene er interessert i å betale for.

DE ELDSTE SKAL BLI DE FØRSTE

Vi blir flere og vi blir eldre. Velferdsteknologi er et av politikernes viktigste virkemidler for å få til gode omsorgstjenester til den eldre delen av befolkningen slik at de kan bo trygt hjemme. Flere selskaper tilbyr nå pakker med velferdsteknologiske sensorer og løsninger. De gjør det enklere å bo hjemme for personer med spesielle behov.

Smarte ting gjør jobben sin i bakgrunnen, og er nesten usynlige. Tingene smelter sammen med omgivelsene. De trenger ikke skjermer og paneler. Det krever lite teknisk kunnskap å bruke dem. Tingenes internett egner seg derfor godt for eldre som gjerne vil bo trygt hjemme lenge. Fallsensorer kan merke om du faller, og varsle omsorgstjenesten automatisk hvis det skulle skje. Digitale pilledispensere kan minne deg på å ta riktig dose tabletter til riktig tid. Hjemmesykepleieren kan følge med og gi en påminnelse hvis du likevel hopper over pillene.

Samfunnsmessig kan slike tjenester gi flere gevinster; i tillegg til mindre energiforbruk kan det gi økt trygghet i hjemmet og mindre behov for sykehjemsplasser, og dermed også bedre ressursbruk i helse- og omsorgstjenesten.

---

[48] "Forskrift om måling, avregning og samordnet opptreden ved kraftomsetning og fakturering av nettjenester" stiller krav til at strømnettselskapene i Norge skal ha installert avanserte måling- og styringssystemer (AMS) i alle målepunkt i sitt konsesjonsområde innen 1. januar 2019. De skal etter 1. januar 2015 rapportere periodisk om fremdrift til Norges vassdrags- og energidirektorat frem til 2019. Enova og NVE har utlyst en egen konkurranse for å fremme storskala pilotprosjekter for å finne informasjonsløsninger som kan bidra til at de nye målerne gir redusert strømforbruk.
[49] https://www.smartly.no

NÅR TING BLIR VANSKELIGE

Internett har mye informasjon om vår atferd som vises gjennom hva vi søker på, hvordan vi oppfører oss på sosiale medier og hvilke bilder vi deler. Tingenes internett kan samle atferdsdata om hvordan vi faktisk beveger oss og oppfører oss i den fysiske verden. Tingenes internett gjør det også mulig å gi tilbakemeldinger direkte til folk mens de holder på med noe.

INTERNETT BLIR FYSISK

I januar 2014 kjøpte Google opp selskapet Nest Labs for 20 milliarder kroner. Hvorfor vil Google, en av verdens største og mest innovative selskaper bruke så mye penger på Nest?

Google har vokst seg store på å gjøre våre digitale dataspor på nettet om til penger:

- Google mestrer kunsten å samle data fra våre nettsøk, våre eposter og våre YouTube-besøk.
- De analyserer disse datasporene mens vi sitter foran skjermen, for å forutsi hvilken informasjon, hvilke produkter eller hvilke tjenester vi er mest interessert i der og da, og knytte oss til nettopp dette innholdet.
- Og sist men ikke minst, videreselge kunnskapen om vår atferd på nettet, våre interesser og ønsker, til ulike annonsører.

Få, om noen, forstår vår oppførsel på nettet bedre enn Google. Men det er altså i den virtuelle verden, ikke i det fysiske rom. Når vi ikke bruker en nettleser eller en app på mobilen, vet Google foreløpig lite om vårt atferdsmønster. Dette er muligens i ferd med å forandre seg med Nest-oppkjøpet.

For med Nest får ikke Google bare en termostat og en røykvarsler, men en mulighet til å samle og lære fra atferdsdata fra hjemmene våre – og med det muligheten til å forstå hvilke behov vi har og hva vi ønsker oss.

Kanskje ikke så oppsiktsvekkende i seg selv, men tenkt deg nå at disse tingene er koblet til hverandre og deler data på tvers. På samme måte som f.eks. søkehistorikken og andre digitale spor vi legger igjen på nettet hjelper Google å forutsi våre ønsker og behov online, er datastrømmene fra Nest nøkkelen til å forstå vår atferd og forutsi våre behov i hjemmet. Med tjenesten Google Now

har selskapet allerede vist interesse for å kunne forutsi hva vi ønsker oss i hverdagen når vi ikke sitter foran maskinen.

Nest posisjonerer seg nemlig som en slags kommandosentral for smarte elektroniske apparater i hjemmet. De lager ikke apparatene selv, men har laget konseptet "Works with Nest". Målet er å koble termostaten og røykvarsleren til alle mulige produkter, som lyspærer og dørlåser. «Works with Nest» har eksistert i et halvt års tid, og selskaper som Logitech og Dropcam lager allerede produkter som kompatible med Nest. Jawbones smartarmbånd 24UP registrerer blant annet søvn og skritt. Når det kobles til Nest, kan temperaturen automatisk tilpasses om du sover eller er våken.

Det er altså ikke tingene Google er interessert i, men heller datastrømmene som produseres når alle tingene begynner å jobbe sammen og lære av hverandre.[50] Tingens internett er en billig og enkel måte å samle verdifulle atferdsdata om våre liv.

På samme måte som Google har blitt en markedsplass for brukertilpasset annonsering på nettet, kan Google bruke datastrømmene fra våre hjem til å lage helt nye markedsplasser. Er f.eks. vaskemaskinen din i ferd med å bli sliten, kan Google forutsi dette før den går i stykker og la ulike aktører få konkurrere om å tilby deg beste pris på reparasjon eller en ny vare. Google kan til og med bruke atferdsdata fra millioner av hjem til å fortelle deg hvilke varer som er aller best tilpasset ditt brukermønster, på samme måte som Amazon i dag foreslår varer som kan interessere deg – og igjen la ulike aktører få konkurrere om å tilby nettopp deg best pris på en slik vare.

Det er ikke bare Google som interesserer seg for datastrømmene i tingenes internett. Apple har sin HomeKit, og i neste versjon av Apples operativsystem for smarttelefoner vil det høyst sannsynlig være mulig å styre smarte ting i hjemmet fra mobilen. Samsung og Intel har sammen laget et såkalt IoT-consortium, mens IBM, BT og ARM har gått sammen med 40 andre selskaper for å bygge "HyperCat" – en plattform for å behandle og analysere nye datastrømmer fra tingenes internett.[51]

Kampen om å kontrollere dataene om deg og din atferd gjennom tingenes internett er altså allerede godt i gang.

---

[50] Mauritius declaration on the internet of things, Balaclava, 14 october 2014
[51] http://thenextweb.com/dd/2014/07/19/internet-things-narrative-change/

FORSIKRING: FRIVILLIG TVANG?

IBM tilbyr sine ansatte aktivitetsmonitoren Fitbit. En sunn og god livsstil belønnes med rabatter og tilbud[52]. Deltakelse i programmet er frivillig, men veien til "sterkt anbefalt" eller "påkrevd" kan være kort.

Mens man i dag må ha en helseattest for å tegne livsforsikring, vil man om få år kanskje få en betydelig rabatt mot at man frivillig går med en aktivitetsmonitor som deler data med forsikringsselskapet. En sunn livsstil belønnes med ytterligere rabatter, mens en usunn livsstil gir høyere premie. Kanskje kan forsikringsselskapet også gi oss små dytt og vink i retning av en oppførsel som minimerer risikoen for selskapet.

Mens annonsørinntekter fra reklame har vært med på å drive frem store deler av internettindustrien, spår noen at forsikringstjenester vil være driveren bak tingenes internett[53].

Kanskje ikke så rart. Atferdsdata fra tingenes internett kan gi forsikringsselskapene mer detaljert kunnskap om hvordan vi faktisk oppfører oss i dagliglivet – i motsetning til statistisk kunnskap om hvordan andre vi ligner har oppført seg tidligere. Oppdager de at de løper en høyere risiko med akkurat deg, så kan de raskt iverksette tiltak[54].

- Var du litt slapp og droppet treningen både i forrige uke og uken før? Eller unnet du deg litt ekstra søtt på ferien? Livsforsikringspremien kan oppjusteres automatisk.
- Har du latt være å ta med bilen på verksted selv om service-lampen har vært tent i flere dager? Da ble bilforsikringspremien din nettopp mye dyerere.

I en undersøkelse med 5000 respondenter sa 38 prosent seg villige til å dele data fra bilen for å kunne oppnå en lavere forsikringspremie.[55]

---

[52] http://www.forbes.com/sites/parmyolson/2014/04/17/the-quantified-other-nest-and-fitbit-chase-a-lucrative-side-business/

[53] http://www.theregister.co.uk/2014/05/23/the_internet_of_things_helps_insurance_firms_reward_punish/

[54] http://www.thebaffler.com/blog/insurance-vultures-and-the-internet-of-things/

[55] http://1.tu-auto.com/LP=796?utm_campaign=2706%2006JAN15%20Non%20BD%27s&utm_medium=email&utm_source=Eloqua&elq=8710db85e5cc410494a4f41454302e68&elqCampaignId=616

I vår nye undersøkelse fra 2014[56] svarer 38,9prosent at de vil tillate at Statens Vegvesen sporer bilen og kjøremønstre hvis det kan føre til bedre flyt i trafikken. 49 prosent av mennene og 36,8 prosent av kvinnene svarte nei. Selv om over halvparten stiller seg negativ er det likevel interessant å se at nesten 40 prosent er villige til å frigjøre data mot, i dette tilfellet, bedre trafikkflyt.

Vi ser altså en vilje til å dele data så lenge insentivene er gode nok. Men vil vi egentlig at forsikringsbransjen skal få så god innsikt i vår daglige atferd? Og hva skjer med de som ikke er villige til å dele sine atferdsdata? Vil de i det hele tatt ha råd til å la være?

NUDGING – ET DYTT FOR VELFERDSSTATEN?

Sensorene smelter inn i tingene, husene og omgivelsene våre og forsvinner inn i bakgrunnen. Her registrerer de våre daglige aktiviteter og rutiner for bedre å forstå vår atferd, våre behov og ønsker. Når et atferdsmønster registreres og analysers i sanntid, er det lettere for en aktør å gripe inn til rett tid, enten for å forsøke å endre atferden eller for å forsøke å holde den vedlike:
Har du lyst til å komme i bedre form? Bilen forteller deg at det er bedre å ta sykkelen til jobb i dag. Været er fint, det er kø på motorveien og naboen har gjort det samme. På vei til jobb forteller både smartsykkelen og smartarmbåndet deg at du er godt på vei til å nå ukens mål hvis du legger på ett gir og tar i litt i neste oppoverbakke.

Små dytt kan hjelpe oss treffe riktige beslutninger og gjøre om på dårlige vaner. Og teknologien gir oss et lite vink når vi gjør dårlige valg vi kanskje ikke engang er klar over at vi gjør. På samme måte som GPS-en i bilen gir fra seg en liten lyd når du kjører over fartsgrensen.

Dette kalles nudging. Små dytt som er ment å endre vår atferd i en positiv retning og gjøre oss til bedre mennesker.

Storbritannia, USA og Danmark har alle opprettet egne enheter som ser på hvordan slike små vink kan hjelpe myndighetene med å løse problemer som overvekt, alkoholmisbruk og klimautfordringene[57]. Med ferske atferdsdata fra tingenes internett, får slike programmer helt nye muligheter: bedre forståelse av hva som fungerer og ikke fungerer, samt muligheten til å ”nudge” gjennom tingene når vi handler.

---

[56] Undersøkelsen er kort beskrevet i forordet i rapporten.
[57] http://www.economist.com/node/21551032

- Begynner det å bli tomt i vannmagasinene? Den smarte dusjen forteller deg at du allerede har dusjet lengre enn gjennomsnittet og at det er fint om du kan være med å spare vann.
- Har du hjerteproblemer og glemmer å ta pillene dine, blinker et lite lys på pilleglasset for å minne deg på at du må huske å ta dem. Pilleglasset sender samtidig en beskjed til din hjemmepleier eller dine nærmeste når du åpner det[58]. Kanskje pilleglasset også rapporterer til pasientjournalen?

Ved å gi oss informasjon om vår oppførsel i sanntid og samtidig gi oss en reell mulighet til å endre oppførsel, kan myndighetene påvirke oss til å gjøre andre valg enn vi kanskje ellers ville gjort[59]. Og summen av disse små justeringene i hverdagen kan hjelpe oss å løse større problemer som samfunnet står overfor.

Men hvem skal bestemme hva som er god, dårlig eller usunn oppførsel? Er det oss eller myndighetene? Eller er det selskapene som analyserer våre atferdsmønstre og utvikler algoritmene som skal bestemme om en gitt handling er god eller dårlig?

Hvilke interesser skal våre atferdsendringer være med å optimalisere og hva skjer hvis man ikke er med på leken? Hvilke individuelle eller kollektive ulemper får man ved å melde seg ut?

Tingenes internett vil kanskje blåse vind i seilene til nudge-entusiastene, men går vi mot et samfunn der vi er bedre rustet til å treffe gode valg for oss og andre, eller mot et samfunn der vi passivt leverer data til algoritmer som på ukjent vis forsøker å styre vår oppførsel?

FARVEL SAMTYKKE?

Vil du låne sykkelen til naboen, spør du først om lov. Hvis et forskningsprosjekt ønsker å bruke dine helsedata, så spør de deg først om lov. Informert samtykke er et viktig verktøy for å regulere bruk og eierskap i hverdagen.

Dette gjelder også data vi legger igjen på nettet. Du skal informeres om hvilke data som samles inn, hvordan de brukes og deles, og du skal kunne ha et ord med i laget om hvordan de skal brukes.

---

[58] http://www.rxvitality.com
[59] http://www.wired.com/2011/06/ff_feedbackloop/all/

Men dette har det vist seg å være svært vanskelig å få til: samtykkeerklæringer på nett er ofte utformet av tjenesteleverandøren, innhyllet i et kryptisk juridisk språk, og gir deg sjelden noe annet valg enn å godta alle betingelsene eller gi avkall på hele tjenesten. Når du i tillegg støter på flere slike erklæringer i løpet av en dag, er det få som gjør annet enn å godkjenne uten å tenke videre på det, fremfor å ta seg bryet med å lese igjennom enda en lang og komplisert erklæring.

Hvilken fremtid har informert samtykke i tingenes internett?

Det er lett å forestille seg at samtykkeerklæringer vil sprette opp som paddehatter når tingene rundt deg kobles på nett og begynner å samle inn data fra omgivelsene. Men hvor spretter de opp, når tingene ikke har en skjerm å vise deg avtalen på? Hvordan skal du da kunne gi et informert samtykke?

Kanskje får du avtalen sendt til deg på mobilen når du befinner deg i nærheten av en ny tilkoblet ting, men det er ikke vanskelig å forestille seg hvor støyende det vil være når alle tingene rundt oss begynner å sende slike erklæringer.

For tingenes internett skal jo ikke være støyende. Teknologien skal forsvinne inn i bakgrunnen og helst forstyrre så lite som mulig. Kanskje betyr det også at informert samtykke slik vi kjenner det vil forsvinne. Istedenfor å forholde deg til hver enkelt ting, vil du kanskje gjøre en stor samtykkeavtale med selskapet som kontrollerer dataflyten mellom tingene - Google, Apple eller Samsung. Praktisk? Kanskje. Men hvem er den sterkeste parten i den avtalen og kan du i det hele tatt ta deg råd til å si ”nei” hvis det betyr at du ikke får tilgang til tjenestene?

BLIR PERSONVERNUTFORDRINGENE MINDRE SYNLIGE?

Etter hvert som tingene vi omgir oss med utstyres med sensorer og kobles til internett får vi et slags utvidet sanseapparat som vi kan ha stor nytte av. Men samtidig blir denne teknologien mindre synlig for oss når den bygges inn i kjente ting vi allerede har et forhold til i hverdagen.

Hvordan skiller vi en smart brødrister fra en dum brødrister? Og hvordan vet vi om den er koblet på nettet eller avslått? Sporingsteknologi som iBeacons and WiFi-fangere er allerede i bruk flere steder, men er samtidig små og vanskelige å få øye på.

Når teknologien forsvinner inn i bakgrunnen på denne måten, og veves inn i hverdagen vår, kan det fort blir vanskelig å utvikle et bevisst forhold til hva

den faktisk gjør med oss. Tingene på internett kan snakke med hverandre uten at du nødvendigvis er oppmerksom på det. Når teknologien i tillegg både er praktisk og nyttig, kan vi fort bli passive datagivere.

Vil vi i det hele tatt kunne unngå tingenes internett om vi ønsker? Hvordan skal vi koble oss av eller skjerme oss fra en teknologi vi ikke kan se?

...ELLER MER SYNLIGE?

På nettet forholder vi oss gjerne til ulike nettsider i en nettleser. Selv om du vet hva du ser på skjermen, er du kanskje ikke like bevisst på hva som skjer i kulissene? Hvem som følger nettoppførselen din og hvordan de gjør det? Nettet har en synlig side, men samtidig er store deler av maskineriet usynlig og obskurt for de fleste nettbrukere.

Med tingenes internett kan det ved første øyekast virke som om dette usynlige maskineriet bare vil vokse seg større:

- Når stadig flere ting kobles til internett, vil både mengden og omfanget av datainnsamlingen fortsette å øke.
- Stadig flere vil være interessert i dataene for å tilby ulike tjenester, og dermed vil også stadig mer data flyte mellom ulike aktører.

Men mens datainnsamling på nettet ofte er usynlig og obskur, er tingene vi omgir oss med hver dag konkrete og håndfaste. Vi har brukt dem tidligere og vet hvilken funksjon de skal oppfylle. Og når internettet flyttes ut av den virtuelle verden bak skjermen og inn i det fysiske rom, har vi kanskje bedre forutsetninger for å forstå og mene noe om hva som er rimelig bruk av data og hva som ikke er det? Hva som er å regne som rimelig bruk er jo tross alt ofte avhengig av hvor man er og i hvilken sammenheng man er der: vi forventer en annen type oppførsel på møterommet på jobben, enn vi gjør på puben på hjørnet.

Når teknologien veves inn i våre fysiske omgivelser, blir det kanskje lettere å oppdage bruk som bryter med sosiale normer[60]. Var det kanskje nettopp en slik respons vi så på Google Glass – en teknologi som operer i sjiktet mellom den fysiske og den digitale og virtuelle verden? Lenge før produktet var å finne i butikkhyllene, hadde begrepet "glasshole" fått et fotfeste i språket. Samtidig

[60] http://www.theguardian.com/technology/2014/jul/28/internet-of-things-privacy

har ulike restauranter, barer, kinoer og strippeklubber innført forbud mot teknologien fordi man raskere så hvordan teknologien kommer i konflikt med sosiale normer.

TING SOM KAN GJØRES

Internettet er i en tydelig forandring. Selv om det er vanskelig å spå hvordan tingenes internett vil slå ut, er det sikkert at det vil by på mange nye muligheter. Men også nye utfordringer - ikke minst for personvernet. Kan vi ta lærdom av erfaringene vi har gjort med nettet?

1) Reell oversikt for brukeren

Store deler av datainnsamlingen på internett er i dag skjult for brukeren. I tingenes internett forventes også mye av datainnsamlingen å være usynlig. Samtidig vil omfanget sannsynligvis øke. Bør (forbruker)myndighetene ta tidlige grep for å utvikle et dashbord som gir folk en enkelt forståelig oversikt over hvilke samtykkeerklæringer de har inngått, hvordan dataene brukes og hvor disse befinner seg? Kanskje kan et slik dashboard også gi "personvernkarakter" som kan hjelpe brukeren å forstå hvordan samtykkeerklæringen hun har inngått griper inn i personvernet?

2) En new deal for internett-økonomien

Internett-økonomien fikk vokse frem uten streng regulering fra myndighetens side. En slik tilnærming kan være viktig for å stimulere innovasjon og nyvinnig i en fase hvor teknologien er i ferd med å modnes. Dessuten kan det være vanskelig å regulere en teknologi som er i rask endring. Mange vil derfor mene at teknologiindustrien i størst mulig grad bør regulere seg selv.

På den annen side viste bl.a. finanskrisen at selvregulering ofte kan komme til kort. Internett-økonomien baserer seg på utstrakt handel med persondata som samles uten at folk forstår omfanget av dette eller får høste verdiene selv. Det er ikke sikkert at dette er en bærekraftig forretningsmodell på sikt.

Norske myndigheter tok tidlig grep for å regulere petroleumsvirksomheten på norsk sokkel. Kan myndighetene nå i en tidlig fase ta et fastere grep om tingenes internett og stake ut en kurs som sikrer at denne teknologien også kommer det norske samfunn og norske borgere til gode? Kan vi utarbeide et nytt dataforlik som bedre balanserer maktforholdet mellom brukeren og selskapene som forvalter datastrømmene i tingenes internett?

3) Hvite flekker på kartet

I dag er det vanskelig å finne steder på nettet hvor man ikke legger igjen elektroniske spor. Med tingenes internett vil denne sporingen strekke seg ut av den virtuelle verden og inn i det fysiske rom. Vi har allerede landskapsvernområder og nasjonalparker for å beskytte viktige naturverdier. Finnes det steder i det offentlige eller private rom som bør fredes for tingenes internett? Hvor vi har rett til å være anonyme og ikke etterlater oss elektroniske fotavtrykk? Bør det f.eks som hovedregel være ulovlig å samle atferdsdata i det offentlige rom?

2015

TINGENES INTERNETT
I januar i år var det tingenes internett det alle snakket om på CES-konferansen (Consumer Electronics Show), som er en årlig trendmåler for IT-bransjen. Samsung-sjefen Boo-Keun Yoon annonserte at alle Samsungs produkter vil kunne kobles til internett innen fem år.

VELFERDSTEKNOLOGI TAS I BRUK I KOMMUNENE
Hittil har bruk av velferdsteknologi skjedd utprøvende og i prosjekter. I 2015 vil vi se at dette tas i bruk i ordinære kommunale helse- og omsorgstjenester.

NY PERSONVERNFORORDNING I EU
Det er ventet at den nye personvernforordningen blir endelig vedtatt siste kvartal 2015. Den nye forordningen vil erstatte dagens personverndirektiv fra 1995.

NY TERRORPAKKE
Regjeringen har varslet en ny «pakke» med terrorbekjempende tiltak. Det vil sannsynligvis bli fremmet forslag om at PST skal få drive såkalt dataavlesning, for eksempel ved å overvåke folks tastaturer. Det er allerede foreslått at politiet skal få adgang til å bruke IMSI-fangere, av samme typen som Aftenposten nylig avslørte at er utplassert i Oslo sentrum.

NY HELSEREGISTERLOV OG PASIENTJOURNALLOV
Pasientjournalloven gir mulighet for tilgang til pasient-opplysninger på tvers av virksomheter. Personvern-konsekvensene kan være uklare.

POLITIET TESTER DRONER
Politidirektoratet har startet opp et prøveprosjekt for å se på hvordan politiet kan benytte seg av droner i fremtiden. Droneprosjekt er en del av det såkalte Endringsprogrammet som skal dimensjonere fremtidens politietat i kjølvannet av kritikken fra 22. juli-kommisjonen.

TERROREN I PARIS KAN GI ENDRINGER I SCHENGEN-AVTALEN
Schengen-avtalens regler om bevegelsesfrihet er et av EUs mest verdsatte prinsipper. Men i etterkant av Paris-terroren har motstanden mot avtalen økt i styrke. Da innenriks- og justisministre fra tolv EU-land møttes i Paris etter terrorangrepene åpnet de for å diskutere endringer Schengen-avtalens regler for bevegelsesfrihet, for enklere å kunne følge med på reisende de mistenker planlegger terror.

Teknologirådet

Datatilsynet