PERSONVERN 2014

TILSTAND OG TRENDER

2013

GPS-SPORING AV DEMENTE

14. JUNI
Stortinget tillater helse- og omsorgstjenester å benytte seg av GPS-teknologi for å spore demente pasienter.

FACEBOOK GRAPH SEARCH LANSERES

8. JULI
Graph Search søker gjennom all informasjon som har blitt lagt ut på din egen og dine venners profiler, blant annet statusoppdateringer og kommentarer. Omfanget av informasjonen som søket kan utnytte utvides gradvis, og er forventet å ta flere år.

BIOMETRISK TEKNOLOGI PÅ IPHONE

10. SEPTEMBER
Apple lanserer iPhone 5S, som tilbyr biometrisk teknologi. Man kan nå bruke fingeravtrykk for å låse opp telefonen. Dette kan utgjøre startskuddet på allmenngjøringen av biometrisk teknologi de kommende årene.

MERKEL AVLYTTES

23. OKTOBER
Tyske myndigheter sier de har opplysninger som tyder på at USA har avlyttet Angela Merkels mobiltelefon. Merkel ringer selv til Obama.

THE GUARDIAN AVSLØRER DEN STØRSTE OVERVÅKNINGSSKANDALEN SIDEN WATERGATE

6. JUNI
The Guardian og amerikanske Washington Post melder at NSA har direkte tilgang til data fra en rekke nettgiganter (bl.a. Facebook, Gmail, Hotmail og Yahoo).

NORSK TERRORLOV UTVIDES

21. JUNI
Forbyr planlegging av terrorhandlinger uten at det har blitt inngått et terrorforbund, og forbyr besittelse av gjenstander med den hensikt å begå en terrorhandling.

HØST 2013: BRASIL VS MULTINASJONALE IT-GIGANTER

I Brasil debatteres et lovforslag som skal kunne påtvinge amerikanske IT-giganter å lagre alle data fra brasilianske innbyggere på servere i Brasil. Hensikten er å underlegge IT-selskapers virksomhet i Brasil brasiliansk personvernlovgivning, og slik begrense omfanget av amerikansk overvåkning.

SLETTING AV ULOVLIG DNA-REGISTER

1. OKTOBER
I tråd med Datatilsynets pålegg fra 2010 avgjorde Personvernnemnda at Folkehelseinstituttet (daværende Rettsmedisinsk Institutt ved Universitetet i Oslo) må slette et ulovlig DNA-register som omfatter flere tusen DNA-profiler med tilhørende persondata til pårørende, skadde, vitner, mistenkte og dømte forbrytere.

KALENDER 2014: SISTE SIDE

ISBN 978-82-92447-66-6 (trykket utgave)
ISBN 978-82-92447-67-3 (elektronisk utgave)

Utgitt: Oslo, januar 2014
Omslag og illustrasjoner: Birgitte Blandhoel
Trykk: ILAS
Elektronisk publisert på: www.teknologiradet.no og www.datatilsynet.no

PERSONVERN PÅ ALVOR

Personvernet er under mer press enn noen gang før. Derfor har Teknologirådet og Datatilsynet også i år forent krefter for å markere den internasjonale personverndagen 28. januar.

Snowden-saken, med avsløringene av amerikanske NSAs storstilte innsamling av informasjon, har satt personvern på dagsordenen på en helt ny måte. Livene våre har aldri vært mer sporbare enn nå. Driveren er den rivende teknologiutviklingen. Den har blant annet gitt folk flest muligheten til å få bedre og mer tilpassede tjenester, og til å dele bilder og informasjon kontinuerlig i sosiale medier. Teknologien gir også myndighetene mulighet til å avdekke terrortrusler og til å spore opp mistenkte. Alt dette er gode og prisverdige formål, men til sammen utfordrer de personvernet, og det blir stadig vanskeligere å holde privatlivet for seg selv.

I forbindelse med Personverndagen har vi gjort en undersøkelse som viser at folk er bekymret over utviklingen, men i stor grad fortsetter som før. Opinion Perduco gjennomførte undersøkelsen i november 2013 via webpanel. Til sammen svarte 1501 innbyggere, i alderen 15 og oppover, på undersøkelsen.

Målet med Personverndagen er å skape debatt og større bevissthet om hvordan de personopplysningene vi legger igjen blir brukt av både private virksomheter, offentlige myndigheter og privatpersoner. Viktige spørsmål er: Hvordan veier vi hensynet til personvernet opp mot andre viktige formål, som for eksempel terrorbekjempelse? Når blir bruken av personopplysninger for inngripende? Hvordan sørger vi for beskyttelse av personvernet på tvers av landegrenser? – Dette er en debatt som ikke kan vente.

28. januar 2014

Tore Tennøe
direktør i Teknologirådet

Bjørn Erik Thon
direktør i Datatilsynet

INNHOLD

PERSONVERN PÅ ALVOR 3

BRYR FOLK SEG OM PERSONVERN? 6

HVA SKJER? 7
PERSONVERNUTFORDRINGER 14

SNOWDEN-AVSLØRINGENE 16

HVA SKJER? 17
HVORFOR ER DET VIKTIG? 18
PERSONVERNUTFORDRINGER 21

NEDKJØLING I NORGE 25

TEGN TIL NEDKJØLINGSEFFEKT I NORGE 27
NEDKJØLINGSEFFEKT ETTER SNOWDEN? 29
LYSER VARSELLAMPENE NÅ? 34

KROPPSNÆR TEKNOLOGI 35

HVORFOR KROPPSNÆRT? 37
PERSONVERNUTFORDRINGEN 40

METADATA OG DEN NYE OVERVÅKINGEN 44

HVA METADATA FORTELLER OSS 46

PERSONVERNUTFORDRINGEN 51

BRYR FOLK SEG OM PERSONVERN?

Aldri har vi levd så sporbare liv som vi gjør i dag. Våre personopplysninger er spredd i et utall av virksomheter, og flere og flere av våre aktiviteter – både privat og på jobb – foregår på nett eller via mobile enheter som registrerer og samler informasjon om oss. I sosiale medier deler mange villig ut informasjon som vi for en stund siden ville regnet som privat og personlig, kun forbeholdt oss selv eller en svært liten krets av nære venner og familie. Betyr den økte delingen at vi ikke bryr oss om vårt eget personvern?

HVA SKJER?

For å belyse temaet har vi spurt folk om hvor opptatte de er av personvern. Vi har forsøkt å finne ut om verdien av personvern sees i lys av utrykket «intet å skjule, intet å frykte». Vi har sett på om folk ser seg selv og sine valg som viktige for eget personvern, eller om resultatet mest avhenger av hva andre gjør. Vi har også spurt om folk er villige til å betale for nettjenester med penger, i stedet for med personopplysninger.

MER OPPTATT AV PERSONVERN

Fra tid til annen nevnes uttrykket «Privacy is dead – get over it!»[1]. Det ser ikke ut til at folk flest har den tilnærmingen når vi ser hva de svarer på følgende spørsmål:

[1] Opprinnelig ble uttrykket kjent og mye sitert etter at Scott McNealy, direktør i Sun Microsystems, i 1999 sa følgende til en journalist: «You have zero privacy anyway. Get over it.»

Tilnærmet halvparten sier at de er blitt mer opptatt av personvern enn tidligere, mens halvparten sier at de er like opptatt av personvern som før. Så å si ingen hevder å være mindre opptatt av dette enn før.

Vi har gjentatt et spørsmål fra en undersøkelse fra 1997 og sammenliknet svarene [2]. Det er en klar forskyvning i retning av en større interesse for personvern:

[2] http://www.ssb.no/a/histstat/not/not_9748.pdf. Statistisk sentralbyrå, Elisabeth Gulløy. Undersøkelse om personvern: Holdninger og erfaringer 1997. Undersøkelsen ble utført av Statistisk sentralbyrå og finansiert av Datatilsynet og Statens informasjonstjeneste.

Flere velger alternativene «svært opptatt» eller «ganske opptatt av personvern» enn i 1997. Gruppen som velger «lite opptatt av personvern» er nesten halvert siden 1997.

I 2013-undersøkelsen merker vi oss at de yngste, gruppen mellom 15 og 29 år, i litt større grad velger alternativet «svært opptatt av personvern» (29 prosent mot gjennomsnittet på 26 prosent).

En økning i den uttrykte interessen for personvern er egentlig ikke overraskende. Noe av forklaringen kan ligge i utstrakt bruk av Internett og i den eksplosive veksten i bruk av sosiale medier. At vi deler mer med andre enn noen gang tidligere, har trolig vært med å gjøre tematikken mer virkelighetsnær og konkret.

De siste drøye fem årene har det vært flere store saker om personvern i media. Dette fører trolig med seg en økt bevissthet rundt og interesse for temaet. Debatten om datalagringsdirektivet, som vakte mye oppmerksomhet i media over lang tid, har nok også vært viktig. Ikke minst kan Snowden-avsløringene ha påvirket svarene i denne undersøkelsen. Disse avsløringene har gitt innblikk i en bruk av personopplysninger som har vært lite kjent, og som viser hvor lite stedbundne og beskyttet personopplysninger er i en stadig mer elektronisk og Internettbasert verden. Norske borgere har også sine opplysninger hos de teknologigigantene som er omfattet av avsløringen. Det handler ikke bare om noen andre – også jeg kan rammes.

INTET Å SKJULE, INTET Å FRYKTE?

Har personvern noe å si for deg? Om du bryr deg om personvern eller ikke, avhenger av om du mener at personvern har en verdi for deg, eller om du mener at du ikke har noen bruk for det. I denne sammenhengen har vi hatt særlig interesse av å se nærmere på et velkjent uttrykk og argument:

Formuleringen «intet å skjule, intet å frykte» blir ofte brukt i diskusjoner om personvern. Utrykket fremstiller personvern som noe som først og fremst beskytter personer med «skjeletter i skapet» og dårlige hensikter. Den som har rent mel i posen har jo uansett ikke noe å være redd for, blir det hevdet.

Er en slik forståelse av personvern utbredt? Sees personvern *generelt* som viktig bare for de som har noe å skjule, eller er det en verdi for alle? Figuren nedenfor viser folks holdninger til et slikt spissformulert utsagn:

Utsagnet får liten støtte: 65 prosent av respondentene er helt eller delvis uenige i utsagnet. En så klar majoritet av helt eller delvis uenige må forstås som en støtte til at personvern har verdi for alle, enten man har noe å skjule eller ikke.

Den andre enden av svarskalaen fikk mye lavere oppslutning, men er likevel verdt å merke seg. Nesten 20 prosent er helt eller delvis enige i utsagnet. Vi må altså holde muligheten åpen for at det finnes en del av oss som mener at personvern faktisk ikke er viktig for folk flest, så lenge vi ikke bryter normer og regler. Andelen på nesten 20 prosent kan nok også dels sees som et uttrykk for respondenter som mener at personvernhensyn i for stor grad legger bånd på hvordan vi som samfunn bekjemper kriminalitet eller løser andre viktige samfunnsoppgaver.

MAKT OVER EGEN SITUASJON

Vi ønsket å finne ut om folk opplever å ha stor innflytelse over hvordan deres personvern blir ivaretatt. Innflytelse vedrører forutsetningene for å bry seg. Manglende innflytelse kan lett resultere i et likegyldig forhold til eget personvern: Hva man gjør har uansett ikke noe særlig å si, det er krefter utenfor en selv som bestemmer utfallet.

Respondentene ble bedt om å rangere myndighetene, virksomhetene og seg selv, etter hvem de mente hadde størst innflytelse over eget personvern.

Som figuren viser, vurderer flertallet seg selv som viktigst. Bare 24 prosent rangerer seg selv som den minst viktige aktøren.

Folk ser seg altså som betydningsfulle for hvor godt deres personvern blir ivaretatt. Det er et godt tegn og en viktig forutsetning for å bry seg.

BETALER MED EGNE PERSONOPPLYSNINGER

Som en del av problemstillingen om folk bryr seg om sitt eget personvern, er det interessant å vite om vi er villige til å betale med penger fremfor med egne personopplysninger.

Personopplysninger er både en handelsvare og et betalingsmiddel. De fleste av oss er storforbrukere av gratistjenester på nett. Aktørene bak gratistjenestene, i form av sosiale medier, søketjenester, e-post og annet, lever i stor grad av inntektene som brukernes personopplysninger gir. På denne måten betaler mange brukere av «gratistjenester» på Internett med sine personopplysninger.

E-postleverandører, søketjenester og sosiale nettsteder vet mye om oss. Denne kunnskapen kan også bli videresolgt til andre. Ønsker vi å unngå at de registrerer, kartlegger og analyserer oss for å danne seg et bilde av hva som kjennetegner oss, våre preferanser, våre interesser og meninger?

For å belyse dette har vi spurt folk om de kunne tenke seg å betale for å unngå at nettsamfunnet de bruker kartlegger og analyserer personopplysningene deres. Spørsmålet er kun stilt til personer som brukte ett eller flere sosiale medier (83 prosent av utvalget).

Sosiale nettsamfunn analyserer dine nettvaner og preferanser for å kunne kartlegge deg, bl.a. for at annonsører kan tilby deg tilpasset reklame.

Kunne du tenke deg å betale 100 kroner i måneden for å unngå at nettsamfunnet du bruker kartlegger og analyserer dine personopplysninger?

Kun åtte prosent er villige til å betale 100 kroner i måneden for å unngå at nettsamfunnet de bruker kartlegger og analyserer personopplysningene deres. Nesten 80 prosent er ikke villige til å betale 100 kroner for dette.

Tolkningene skal ikke trekkes for langt. Særlig kan man lure på om 100 kroner var for høyt, og at et lavere beløp ville ha gitt andre resultater[3].

At så få var villige til å betale 100 kroner, kan indikere at betalingsviljen er lav. Tallene er imidlertid ikke egnet som et generelt mål på betalingsvillighet for å unngå kartlegging og analyse av egne personopplysninger. Derimot er svarene et godt utgangspunkt for ettertanke og videre diskusjon om temaet betaling med personopplysninger: Er vi villige til å betale for tjenester som vi er vant til at er gratis for å unngå noe som kan ses på som personvernulemper? Og i så fall, hvor lav må prisen være for at ikke bare en liten gruppe vil si ja?

I en undersøkelse i EU-landene fra 2011 ble deltakerne spurt om hvor komfortable de var med at gratistjenester på Internett bruker informasjon fra deres nettaktivitet til å skreddersy reklame etter hobbyer og interesser[4].

48 prosent av de som brukte sosiale nettsamfunn og delingssider på Internett svarte at de var meget eller ganske komfortable med at tjenestene brukte informasjonen deres på en slik måte. Til sammenligning svarte 47 prosent at de var ganske eller meget ukomfortable. Indikasjonene om betalingsvilje i vår undersøkelse og EU-undersøkelsen gir et samlet inntrykk av at mange faktisk ikke føler seg særlig ukomfortable med gratistjenesters kartlegging og analyse av deres personopplysninger. Hvis valget står mellom å betale med 100 kroner eller med personopplysninger, er villigheten høyere til å betale med personopplysninger. Det er grunn til å stille spørsmålet: Er dette er et felt hvor mange i liten grad bryr seg?

Antageligvis er svaret dels ja, men andre forklaringer er også rimelige: Mange synes nok at denne bruken av personopplysninger ikke er så problematisk. En annen forklaring kan være at folk har vent seg til at «det bare er slik». Dessuten kan det være at mange verken forstår betydningen av, eller er bevisste på, hva som skjer med deres personopplysninger.

---

[3] Noen bruker også mange nettsamfunn. Ordlyden «nettsamfunnet du bruker» var ment å rette oppmerksomheten mot det nettsamfunnet den enkelte respondent oppfattet som viktigst for seg, men vi kan ikke utlukke at en del kan ha svart med henblikk på hva det ville kostet for alle nettsamfunnene til sammen. I tillegg kan spørsmålet ha blitt forstått av enkelte som at det eneste man får igjen for 100 kroner, er fravær av tilpasset reklame, noe enkelte kanskje heller vil ha enn ikke-tilpasset reklame.

[4] Special Europabarometer 359, «*Attitudes on Data Protection and Electronic Identity in the European Union*», 2011. http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

PERSONVERNUTFORDRINGER

FOLK VIL HA PERSONVERN

Tallene fra undersøkelsen viser en økt interesse for personvern, og bekrefter at dette er noe folk bryr seg om. Det at folk er mer opptatt av personvern enn tidligere, betyr imidlertid ikke nødvendigvis at de setter strenge grenser for hva de vil dele med hvem.

Slik vi ser det, må tallene om økt interesse for personvern først og fremst forstås som at personvern oppleves som relevant og viktig. At personvern har verdi for de aller fleste av oss, støttes også av at respondentene i stor grad tar avstand fra påstanden om at «bare de som har noe å skjule har behov for personvern».

PERSONVERN OG ANDRE HENSYN

Personopplysninger som betalingsmiddel gir utfordringer som vil være med på å prege personvernet i tiden fremover. Personopplysninger har blitt en handelsvare. Det har vokst fram en stor industri med internettbaserte selskaper som i stor grad baserer seg på å kartlegge personopplysninger – ofte for å kunne tilby annonsører målrettet reklame.

For den enkelte internettbruker kan denne forretningspraksisen skape personvernutfordringer. Ny teknologi og smarte datasystemer gjør det lettere å identifisere og analysere hver enkelt av oss. Fenomenet omtales som Big Data. Stadig aggregering og sammenstilling av data fra forkjellige kilder kan gi en følelse av at noen vet alt for mye om oss. Vi ser i økende grad at personopplysninger blir brukt til nye formål. For det enkelte menneske er det vanskelig å få et godt grep på hva som skjer med deres personopplysninger i store og kompliserte systemer, noe som vedrører folks mulighet til å ha kontroll med egne opplysninger.

Et viktig aspekt ved personvernet er selvråderett. At du kan velge selv, betyr også å kunne si ja, eksempelvis til å dele informasjon som man tidligere mente bare tilhørte den private sfære. Vi skal være svært forsiktig med å sette likhetstegn mellom stor delingsvilje og det å ikke bry seg om personvern. I en del sammenhenger er det heller et uttrykk for et skifte i holdninger til hva folk ser som beskyttelsesverdig eller privat. Samtidig bør nok ikke dagliglivets mange

små valg ses som et direkte uttrykk for hva den enkelte selv synes er godt personvern.

Hvordan folk ser på personvern, hvor grensene går for hva som er privat, og hva som føles som akseptabel bruk av personopplysninger, er i kontinuerlig endring. Å ha et aktivt og bevisst forhold til personvern kommer ikke av seg selv. Vi ønsker derfor velkommen en åpen debatt om hva personvern er for folk flest, og bør være, i tiden som kommer.

SNOWDEN-AVSLØRINGENE

«Har du ikke noe å skjule, har du heller ikke noe å frykte.» Budskapet har vært sentralt i den amerikanske etterretningens forsvar av den omfattende overvåkingspraksisen, som ble avslørt av Snowden-dokumentene. Men er det virkelig slik at folk flest ikke behøver å bekymre seg over at nærmest all deres sporbare aktivitet kan bli samlet inn og kartlagt?

HVA SKJER?

I begynnelsen av juni 2013 kom de første medieoppslagene om at amerikanske sikkerhetsmyndigheter utførte massiv overvåking av tele- og datatrafikk. Det var blant annet The Guardian og The Washington Post som avslørte at National Security Agency (NSA) har hatt tilgang til data fra selskaper som Microsoft, Yahoo, Google, Facebook, Skype, YouTube og Apple.

Kilden til avsløringene er Edward Snowden som jobbet som datatekniker i CIA og på kontrakt for NSA. Snowden forlot USA før avsløringene, og fikk innvilget midlertidig asyl i Russland i august. Mens tilhengere kaller ham en menneskerettsaktivist og varsler, har amerikanske myndigheter siktet ham for spionasje.

I følge sjefen for NSA, general Keith Alexander, har Snowden lekket mellom 50 000 og 200 000 dokumenter. I tillegg til å avsløre at amerikansk etterretning har overvåket telefonsamtalene til en rekke internasjonale ledere, viser dokumentene at NSA har hatt adgang til enorme mengder data om folk flest. Gjennom programvaren Xkeyscore har USA hatt tilgang til enorme databaser med e-post, chattehistorikk og surfestatistikk via amerikanske selskaper. Dokumentene viser også at amerikanske myndigheter har spionert på alliertes ambassader, FN og EUs kontorer i Washington og New York[5].

Den 19. november meldte Dagbladet at ett av Snowden-dokumentene viste at NSA hadde overvåket mer enn 33 millioner mobilsamtaler i Norge i en periode på 30 dager ved årsskiftet 2012/13. Nyheten skapte mye oppmerksomhet fra både media og øverste politiske ledelse i Norge. Kort tid etter slo sjef for Etter-

[5]http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

retningstjenesten, generalløytnant Kjell Grandhagen, fast at dette ikke dreide seg om amerikansk overvåking, men om norsk etterretning som overvåket telefontrafikk i Afghanistan. Norsk etterretning deler denne type data med blant andre amerikanske NSA, og i følge Grandhagen var det bakgrunnen for Dagbladet-saken[6].

2013 ble året da myndighetenes overvåking kom i fokus. Snowden-dokumentene avslørte også at den britiske etterretningstjenesten GCHQ, gjennom prosjektet «Tempora», hadde avlyttet fiberoptiske kabler som frakter internasjonal telefon- og internettrafikk[7]. Avsløringene fra USA og England har skapt ny debatt om den svenske FRA-loven. Denne loven gir det svenske forsvaret rett til å gjennomføre signalspaning på telefon- og internettrafikk som passerer Sveriges grenser via kabel[8]. Minst 80 prosent av Norges internettrafikk går via Sverige[9].

HVORFOR ER DET VIKTIG?

POLITISKE RINGVIRKNINGER

Snowden-avsløringene skaper politiske ringvirkninger på tvers av grenser. President Obama kansellerte et besøk til Moskva i protest mot at Russland har gitt Snowden midlertidig asyl. Den brasilianske presidenten Dilma Rousseff avlyste et offentlig besøk til Washington i protest mot at USA har spionert på henne. En rasende Angela Merkel anklaget USA for å spionere på henne, noe som førte til at Det hvite hus uttalte at nye kontrollmekanismer for NSA kan være nødvendig.

Arbeidet med en ny EU-forordning som skal regulere og samkjøre personvernlovgivningen i Europa, har stått mer eller mindre i stampe blant annet på grunn av amerikansk lobbyvirksomhet som har motarbeidet hindringer av fri flyt av personopplysninger mellom Europa og USA. I oktober stemte imidlertid medlemmene i EU-parlamentets komité for sivile rettigheter for å støtte et utkast til ny lovtekst. Denne slår fast at all data som behandles i Europa skal reguleres av europeiske regler. Formuleringen i lovteksten gikk igjennom som

[6] http://www.nrk.no/norge/avviser-overvaking-av-nordmenn-1.11366261
[7] http://en.wikipedia.org/wiki/2013_global_surveillance_disclosures
[8] http://www.datatilsynet.no/verktoy-skjema/Publikasjoner/Analyser-utredninger/Utredning-om-signalspaning-i-Sverige1/
[9] http://www.tu.no/it/2013/11/20/80-prosent-av-norsk-nett-trafikk-gar-gjennom-svenske-kabler

et resultat av et endret politisk klima i Europa i kjølvannet av overvåkingsavsløringene i 2013[10].

EUs justiskommisær Viviane Reding satte også spørsmålstegn ved den eksisterende Safe Harbour-avtalen som regulerer overføringer av personopplysninger i forretningstransaksjoner mellom Europa og USA. Avtalen er basert på selvregulering og retningslinjer. Reding uttalte at i lys av det som har kommet fram i Snowden-saken, er hun ikke sikker på at denne type avtale er tilstrekkelig for å beskytte europeiske borgeres personvern[11].

PERSONOPPLYSNINGER ER BIG BUSINESS

Mye står på spill for internettbaserte selskaper hvis livsgrunnlag baserer seg på behandling av folks personopplysninger. The Information Technology and Innovation Foundation, en Washington-basert tenketank, har beregnet at Snowden-saken kan koste selskaper med servere i USA mellom 21 og 35 milliarder dollar over de neste tre årene hvis kundene velger å migrere til selskaper som ikke er basert i USA[12]. Hva den faktiske effekten blir vet vi ikke, men mange av de amerikanske selskapene har tatt grep for å begrense skadeomfanget av avsløringene.

Google sjef Eric Schmidt uttrykte sjokk og sinne, og sa at avsløringene viser overtramp fra myndighetenes side. Flere av de amerikanske selskapene har annonsert at de nå arbeider med å styrke informasjonssikkerheten i systemene sine[13]. For eksempel har Twitter begynt å kryptere private beskjeder som sendes direkte mellom brukere – som en direkte konsekvens av Snowden-avsløringene[14]. En del av selskapene har offensivt støttet et lovforslag om å forby myndighetenes innsamling av store mengder data om millioner av amerikanere. Forslaget foreslår også økt åpenhet om forholdet mellom privat næringsliv og amerikanske sikkerhetsmyndigheter[15].

Kinesiske myndigheter har brukt avsløringene som utgangspunkt for å advare kinesiske selskaper mot å stole på amerikanske selskaper. Flere europeiske selskaper har brukt muligheten til å promotere sine løsninger som sikre og

---

[10] http://www.theguardian.com/world/2013/oct/22/meps-data-privacy-rules-snowden-nsa-gchq
[11] http://www.theguardian.com/world/2013/oct/17/eu-rules-data-us-edward-snowden
[12] http://www.techpolicydaily.com/technology/backlash-commercial-diplomatic-spillovers-nsa-revelations/
[13] http://money.cnn.com/2013/11/04/technology/google-nsa-snowden/
[14] http://www.wired.co.uk/news/archive/2013-11/25/twitter-encryption
[15] http://www.theguardian.com/world/2013/dec/09/nsa-surveillance-tech-companies-demand-sweeping-changes-to-us-laws

personvernvennlige i motsetning til sine amerikanske konkurrenter. En undersøkelse viser at drøyt 40 prosent av norske virksomheter har blitt mer skeptiske til sky-tjenester etter Snowden-avsløringene[16]. Det norske selskapet Jottacloud lanserte en «snokefri» bedriftsløsning, og 30 000 nye kunder åpnet konto hos selskapet i månedene etter avsløringene[17].

DU ER DEL AV HØYSTAKKEN

Men det er ikke bare politiske relasjoner og amerikanske selskaper som er rammet av overvåkingsavsløringene. Innsamlingen av enorme mengder data om folk flest er kanskje det som har sjokkert mest. Istedenfor å lete etter målrettet informasjon om individer, samler NSA inn et bredt spekter av telefontrafikk, kontaktlister og annen aktivitet på sosiale medier, og i e-post- og chattehistorikk. I følge ett av de lekkede dokumentene ble det samlet inn 444 743 e-postadresselister fra Yahoo, 105 068 fra Hotmail, 82 857 fra Facebook, 33 697 fra Gmail og 22 881 fra andre selskaper på én enkelt dag i fjor[18]. Analyse av denne type data gjør det mulig å finne skjulte forbindelser og å kartlegge nettverk mellom mennesker. Lederen for NSA, general Keith Alexander, uttalte til Washington Post at «Du trenger en høystakk for å finne nåla.»[19]

Befolkningsundersøkelsen vi gjennomførte mot slutten av 2013 viste at så å si alle (94 prosent) nordmenn over 15 år har hørt om Snowden-saken. Vi spurte hva de mener om den amerikanske overvåkingen. Hele 72 prosent uttrykker bekymring ved å indikere at overvåkingen er «uakseptabel» eller «bekymringsverdig, men nødvendig». At 27 prosent svarte at de syns overvåkingen er «bekymringsverdig, men nødvendig» illustrerer at det kan være vanskelig for folk flest å bedømme i hvilken grad et overvåkingstiltak er nødvendig for å avverge terror eller alvorlig kriminalitet. Kun 12 prosent mener at overvåkingen er uproblematisk.

[16] http://www.logistikk-ledelse.no/aktuelt/cloud_datametrix.htm
[17] http://www.tu.no/it/2013/09/02/folk-vil-ha-norsk-lagring-for-a-unnga-amerikansk-overvaking
[18] http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html
[19] http://www.nationalsecuritylawbrief.com/the-necessity-of-the-haystack-to-find-the-needle-a-look-into-the-controversial-nsa-bulk-collection-program/

PERSONVERNUTFORDRINGER

FRA HARPUN TIL TRÅL

Snowden-avsløringene har vært en øyeåpner for mange når det kommer til hvilke overvåkingsmuligheter teknologien gir oss i dag. Økt lagringskapasitet og prosesseringskraft gjør at overvåkere kan samle inn, lagre og analysere enorme mengder data, uten at den enkelte av oss er klar over det.

Tradisjonell etterretning har jobbet med innhenting av informasjon om spesifikke personer som er under mistanke. De lekkede Snowden-dokumentene avdekket imidlertid en overvåkingspraksis der amerikansk etterretning samler inn informasjon som omfatter et stort antall mennesker som ikke er under mistanke for noe kriminelt.

Formålsbestemthet er et sentralt personvernprinsipp i både norsk og europeisk lovgivning. Det vil si at personopplysninger bare skal samles inn for bestemte formål og at disse må være legitime. Jo mer inngripende tiltaket er, jo mer tungtveiende må formålet være. På den annen side er det også bred

aksept for behovet for overvåking, blant annet for å motvirke terror. Men hvor går grensen for at overvåkingen blir et for stort inngrep i privatlivet til folk flest?

SUGERØR INN I DIN PRIVATE PROFIL

Bruk av telekommunikasjon, og spesielt Internett, har blitt en naturlig del av folks hverdag. PRISM-programmet er NSAs største enkeltkilde til informasjon, og går ut på at NSA samler inn informasjon om privatpersoner gjennom amerikanske selskaper. Mange ble overrasket over at NSA hadde et sugerør inn til informasjon om enkeltindivider via private selskaper på en systematisk og omfattende måte. Noen kilder hevder at NSA har direkte tilgang til serverne til selskapene, men denne påstanden tilbakevises av selskapene selv som sier de kun gir ut informasjon når de blir lovpålagt det[20].

Det at mye av livene våre er sporbart gjør oss ekstra sårbare. Når en aktør, i denne sammenheng amerikansk etterretning, har tilgang til både innholdsdata og metadata som viser hvor vi er, når vi er der og hvem vi snakker med, er det mulig å tegne et skremmende detaljert bilde om hver enkelt av oss.

BEHOV FOR ÅPENHET OG KONTROLL

Debatten og mediedekningen av Snowden-avsløringene viser at både politikere og folk flest har begrenset kunnskap om hva slags type etterretning som foregår, og hvem den omfatter. Debatten i kjølvannet av Dagbladets påstand om at USA hadde overvåket 33 millioner norske mobilsamtaler, viser at det er mye usikkerhet rundt overvåking og hvilke teknologiske virkemidler både nasjonale og utenlandske etterretningstjenester har.

Behovet for et visst nivå av hemmelighold i etterretningen er åpenbart. Det bør imidlertid være mulig å gi mest mulig generell informasjon om hvordan de hemmelige tjenestene jobber; hvilken type informasjon som samles inn, hva den brukes til og hva som skal til for at etterretningstjenesten kan innhente data. Denne type informasjon er viktig for å gi folk oversikt over sannsynligheten for at de blir overvåket eller ikke. Åpenhet bidrar til å skape tillit. Det er også en forutsetning for at folk skal kunne ivareta sine rettigheter.

[20] http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

For å opprettholde prinsipper om åpenhet og etterrettelighet bør det være mekanismer som gjør folk flest trygge på at myndighetene bruker sine virkemidler etter loven, og kun der det er nødvendig. I en tale i januar 2014 annonserte president Obama at han ønsker å iverksette innstramninger av den amerikanske etterretningspraksisen. Blant annet ønsker han å få på plass strengere regler for NSAs tilgang til metadata, begrensninger i overvåking av allierte ledere, og mer åpenhet om når selskaper får pålegg om å gi ut informasjon til etterretningstjenestene. Innsamlingen av data i stort omfang fortsetter imidlertid, om enn muligens med strengere kontroll[21].

I Norge har EOS-utvalget mandat til å føre tilsyn med de hemmelige tjenestene. Snowden-avsløringene har tydeliggjort viktigheten av å ha slike kontrollorgan. I tillegg til faktisk å avdekke ulovligheter, har utvalget en oppdragende effekt på tjenestene de har tilsyn med.

BØR FOLK VÆRE BEKYMRET?

I 2013 har omfanget og dybden av myndighetenes overvåking fått økt oppmerksomhet. Folk flest har fått vite at både vår egen og utenlandsk etterretning har kapasitet til å samle inn store mengder data som kan tegne et detaljert bilde av hver enkelt av oss.

At etterretningstjenestene kun er underlagt reglene i landet de hører til, og ikke i landet hvor man opererer, skapte debatt høsten 2013. Blant annet foreslo generalsekretæren i Europarådet, Thorbjørn Jagland, å få på plass internasjonale lover som beskytter folk mot utenlandsk etterretning[22]. Dagens praksis innebærer at du har rettigheter som regulerer i hvilken grad og hvordan du kan bli overvåket av din nasjonale myndighet, men at du er fritt vilt for andre lands etterretningstjenester – for eksempel vårt naboland Sverige, eller USA. Vennligsinnede land deler etterretningsdata. Det betyr at Sverige har mulighet til å dele data de har om norske internettbrukere med norsk etterretning. I praksis betyr det at norske borgeres rett til personvern ikke gjelder hvis deres informasjon blir plukket opp av fremmede etterretningstjenester.

Den omfattende overvåkingspraksisen, og mulighetene for overvåking teknologien tilbyr, utfordrer våre rettigheter og vår integritet som individer. Også våre verdier, og hva det innebærer å være et demokratisk samfunn, blir ut-

[21] http://www.wired.com/threatlevel/2014/01/obama-nsa/
[22] http://www.vg.no/nyheter/innenriks/artikkel.php?artid=10137019

fordret. Du kan lese mer om hvordan vissheten om at vi blir overvåket kan påvirke tankemønstre og adferd, i kapittelet «Nedkjøling i Norge».

Vi spurte folk om de mener at personvern er viktig for et fritt og demokratisk samfunn. Tilslutningen til utsagnet er stor; åtte av ti er delvis eller helt enige.

Personvern regnes som en frihetsrettighet i EUs personverndirektiv, og som en menneskerett i Den europeiske menneskerettskonvensjonen. I tillegg til frihetsperspektivet, vil man i tradisjonell forståelse også sette personvern i sammenheng med demokrati som samfunnsform. Hvis vi går mot et samfunn der borgerne til en hver tid må regne med at noen ser dem over skulderen, vil vi få et annet type samfunn enn det vi er vant til i dag. Rollene til både myndigheter og borgere endres, og det samme gjelder forutsetningene for deltakelse i samfunnet.

NEDKJØLING I NORGE

«En utilbørlig innblanding i den enkeltes personvern kan både direkte og indirekte begrense den frie utvikling og utveksling av ideer. En krenkelse av den ene rettigheten kan både være årsak og konsekvens av en krenkelse av den andre.»

FNs spesialrapportør på ytringsfrihet, Frank La Rue[23]

Snowden-saken har vist at vi må ta høyde for at personlig informasjon som vi legger igjen på Internett, før eller senere kan bli utsatt for et uventet, og for mange av oss også et uønsket, blikk. Våre oppdateringer på Facebook, søk på Google, meldinger på Twitter, samt hvem vi sender en sms eller ringer til, inngår i den gigantiske digitale høystakken som analyseres for å avsløre mistenkelige mønstre. Men det er ikke bare etterretningstjenestene som har appetitt på våre data. Andre offentlige myndigheter, så vel som kommersielle virksomheter, ønsker å vite mest mulig om oss for å effektivisere og skreddersy tjenester og reklame.

Hvordan påvirker det oss når vi vet at noen til enhver tid kan titte oss over skulderen? Mennesker som vet at de kan bli iakttatt endrer oppførsel fordi konteksten er en annen – tillitten til omgivelsene endres. Hvis vi er usikre på hvem som har tilgang til opplysningene vi legger igjen, er vi tvunget til å ta hensyn til denne usikkerhetsfaktoren. Vi vil begynne å tenke gjennom hva vi skriver, hva vi foretar oss og hvem vi har kontakt med.

Fenomenet omtales som nedkjølingseffekt, kalt «chilling effect» på engelsk. En sentral følge av nedkjølingseffekten er press på ytringsfriheten, som i neste konsekvens kan svekke demokratiet ved at borgerne begrenser sin deltakelse i åpen meningsutveksling. Men nedkjølingseffekt handler også om at usikkerhet relatert til hvordan våre personopplysninger blir brukt, kan føre til at vi unnlater å gjøre helt ordinære gjøremål. Vi kan for eksempel unngå å låne en bestemt bok på biblioteket eller å ringe psykologen, i frykt for hvordan disse opplysningene eventuelt kan bli brukt senere.

[23] http://rt.com/news/communication-surveillance-violates-human-rights-285

UTFORDRENDE Å MÅLE

Å måle graden av nedkjølingseffekt i samfunnet er en krevende øvelse. Hvor mange som har kjøpt en bestemt bok, meldt seg inn i en forening eller trykket "liker" på en artikkel på nett, kan telles. Det er imidlertid mye vanskeligere å kvantifisere *fravær av handling*, det vil si hvor mange som har *unnlatt å* kjøpe den bestemte boka, melde seg inn i en forening eller trykke på liker-knappen. Videre kan nedkjølingseffekt inntreffe uten at vi nødvendigvis er bevisst dette selv. Vi kan gradvis legge om våre vaner som en ubevisst respons på usikkerhet knyttet til hvordan opplysningene vi legger igjen blir brukt.

Vi har forsøkt å få et inntrykk av om det er generelle tendenser til nedkjølingseffekt ved å spørre folk om de har unnlatt å gjøre noe fordi de er usikre på hvordan opplysningene kan bli brukt senere. Nedkjølingseffekt er her ikke knyttet opp mot myndighetsovervåking spesielt. Vi holder det åpent med henblikk på *hvem* som er potensielle bruker av opplysningene. I personvern-undersøkelsen har vi imidlertid også ønsket å finne ut om Snowden-avsløringene spesielt, har ført til nedkjølingseffekter i Norge, og har derfor stilt noen spørsmål direkte knyttet konkret til denne saken.

TEGN TIL NEDKJØLINGSEFFEKT I NORGE

Tallene i undersøkelsen viser tendenser til en generell nedkjølingseffekt i Norge[24]. Tallene viser at en vesentlig andel av befolkningen har unnlatt å gjøre enkelte aktiviteter fordi de er usikre på hvordan opplysningene kan bli brukt senere. Det er verdt å merke seg at så mange som 26 prosent har unnlatt å skrive under på opprop og at 16 prosent har unnlatt å foreta bestemte søk på nett. Til sammenligning oppga også 16 prosent i en amerikansk undersøkelse at de hadde avstått fra å foreta internettsøk på bestemte tema[25]. Den amerikanske undersøkelsen var imidlertid rettet utelukkende mot skribenter, en gruppe mennesker som nok har reflektert mer enn gjennomsnittet over hvordan sporene de legger igjen kan brukes av andre. At en like stor prosentandel har svart det samme i vår undersøkelse, rettet mot befolkningen som helhet, er derfor mer oppsiktsvekkende. En betydelig andel av helt alminnelige borgere sensurerer altså seg selv fordi de er usikre på hvordan opplysningene kan bli brukt senere.

Usikkerhet knyttet til hva opplysningene faktisk kan brukes til, kan være mange. Det at folk oppgir at de har unnlatt å gjøre enkelte ting, skyldes nødvendigvis ikke usikkerhet knyttet til hvordan myndighetene kan komme til å bruke opplysningene. Det kan også skyldes usikkerhet knyttet til hvordan opplysningene kan bli brukt i en fremtidig ansettelsesprosess, i markedsføringssammenheng eller av et forsikringsselskap. Vi er antageligvis blitt mer bevisste på at de digitale sporene vi legger igjen ikke alltid blir borte, og at de kan dukke opp i nye og uventede sammenhenger. Alle underskriftskampanjene og oppropene vi har underskrevet opp gjennom årene kan, når de sammenstilles, tegne et tydelig bilde av oss.

Å utøve selvsensur er en naturlig del av det å ferdes på nett. Å være bevisst hvordan man ytrer seg og fremstår er en type "selvsensur" som skjer både på og utenfor nettet. Men hvis vi får en får en utvikling der stadig flere for eksempel unnlater å melde fra om kritikkverdige forhold eller å skrive under på viktige saker fordi man er usikker på hvordan opplysningene kan bli brukt senere, kan dette få alvorlige konsekvenser. Det berører i siste instans selve fundamentet for et åpent og velfungerende demokrati.

---

[24] Det er imidlertid vanskelig å trekke bastante konklusjoner om tallene viser en svak eller sterk tendens når vi ikke har andre direkte sammenlignbare tall.

[25] http://america.aljazeera.com/watch/shows/america-tonight/america-tonight-blog/2013/11/21/survey-1-in-6-writershaveselfcensoredbecauseofnsasurveillance.html

NEDKJØLINGSEFFEKT ETTER SNOWDEN?

Kan vi se tegn til nedkjølingseffekt i Norge som en *direkte* følge av Snowden-avsløringene? I USA har Electronic Frontiers Foundation anlagt sak mot NSA på vegne av 22 organisasjoner som mener de har opplevd nedkjølingseffekt som en direkte konsekvens av NSAs overvåking[26].

For det første gjenspeiler nok svarprosenten hvor vanskelig det er å legge om på sine digitale vaner selv om man føler ubehag knyttet til hvordan etterretningstjenestene arbeider. For det andre er det nok fortsatt slik at majoriteten av befolkningen i Norge ikke opplever å være interessante for etterretningstjenestene. De fleste vil tenke at overvåkingen er rettet mot grupper de ikke inngår i eller har befatning med selv – de føler seg ikke rammet på et personlig nivå. Dette til tross for at Snowden-avsløringene nettopp har vist at dagens etterretningsmyndigheter samler inn data om folk flest, ikke kun bestemte grupper. For det tredje er det antageligvis også mange som tenker at selv om myndighetene ser gjennom alle deres data, så betyr ikke det noe ettersom man ikke har noe å skjule allikevel. Dessuten har nordmenn generelt høy tillit til myndighetene. Folk har tillit til at etterretningstjenestene ikke vil misbruke informasjonen som samles inn, og at det derfor er trygt å fortsette som før.

Undersøkelsen vår viser at Snowden-saken ikke har hatt en sterk nedkjølingseffekt på norske borgere. Seks av ti oppgir at denne konkrete saken ikke har påvirket deres handlinger. Dette til tross for at majoriteten av de spurte i undersøkelsen mener at overvåkingen enten er uakseptabel eller bekymringsverdig. Dette kan skyldes flere forhold.

Åtte prosent av de spurte har imidlertid tenkt seg om en ekstra gang før de brukte visse ord i sin korrespondanse og i internettsøk. Det er med andre ord indikasjoner på en svak nedkjølingseffekt etter Snowden-saken. Ser vi på tallene fordelt på alder, slår nedkjølingseffekten signifikant mer ut i aldersgruppen 15–29 år. Åtte prosent av de spurte i den yngste aldersgruppen, har endret bruken av visse tjenester, mot i gjennomsnitt fem prosent i de høyere aldersgruppene. At det er flere blant de unge som har endret på sine kommunikasjonsvaner, kommer antageligvis av at denne gruppen består av de mest aktive og allsidige brukerne av digitale tjenester. De lever store deler av sine liv på nett og føler seg kanskje derfor i større grad utsatt og sårbare for overvåkingstrykket enn de som er eldre.

TAP AV TILLIT TIL INTERNETT?

Kan Snowden-avsløringene føre til at vi stoler mindre på Internett og derfor vil bruke Internett mindre? I USA har flere internettjenester stengt dørene i etterkant av Snowden-avsløringene, blant annet Lavabit og Silent Circle, to leverandører av krypterte e-postløsninger. Lavabit forklarte nedleggelsen av tjenesten med at de «ikke ville stå i ledtog med myndighetene i overvåkingen av det amerikanske folk»[27].

Groklaw, et mye brukt nettforum viet juridiske debatter, stengte i sommer tjenesten fordi grunnleggeren av nettstedet ikke var komfortabel med å eksponere deltakerne i forumet for myndighetsovervåking[28]. Nedleggelsen av Groklaw og tilsvarende selskap, blir omtalt som eksempel på såkalt nedkjølingseffekt.

[27] http://www.theguardian.com/technology/2013/aug/08/lavabit-email-shut-down-edward-snowden
[28] http://gigaom.com/2013/08/20/through-a-prism-darkly-fear-of-nsa-surveillance-is-having-a-chilling-effect-on-the-open-web/

Det norske selskapet Jottacloud, som tilbyr nettskyløsninger, opplevde en voldsom kundetilstrømning etter Snowden-saken. Rett etter at saken sprakk, gikk eierne ut og garanterte at de ikke ville gi ut lagret informasjon til myndigheter eller andre aktører uten rettslig kjennelse[29]. Dette førte til at de fikk mange nye kunder, også fra USA.

Tap av tillit til Internett som kanal og arena for meningsutveksling, vil ikke bare ha negative konsekvenser for et levende og aktivt demokrati, det vil også ha alvorlige konsekvenser for den digitale økonomien. Det kan etter hvert være mange brukere, både selskap og privatpersoner, som for eksempel ikke ønsker å benytte e-handelsløsninger der de vet at hver eneste transaksjon blir indeksert og sporet av ulike lands myndigheter. Særlig europeiske virksomheter kan velge bort amerikanske skytjenester for å beskytte kundenes personvern.

OVERVÅKING HAR KONSEKVENSER

Sett at norsk og utenlandsk etterretning overvåker og lagrer alle norske borgeres elektroniske kommunikasjon og nettbruk. Er dette noe folk bryr seg om? Åpenhet er tidens melodi – vi deler alt med alle på nett uansett. Og dessuten, hvis vi har rent mel i posen har vi vel ikke noe å være urolig for?

45 prosent av befolkningen oppgir at selv om all elektronisk kommunikasjon og aktivitet på nett ble overvåket, ville de fortsette som før. Det at så mange svarer at et slikt massivt overvåkingstrykk ikke betyr noe for dem, avspeiler nok først og fremst nordmenns høye grad av tillit til myndighetene. Som kommentert i spørsmålet over, føler vi oss trygge på at myndighetene ikke vil

[29] http://e24.no/digital/snowden-saken-ga-kundeboom-for-norsk-nettsky/21106285

bruke opplysningene som samles inn på en utilbørlig måte, selv om overvåkingen også omfatter oss selv.

Det at folk ikke justerer sin oppførsel er imidlertid ikke det samme som at folk er likegyldige, eller synes det er greit å bli overvåket. Som sagt viser vår undersøkelse at 72 prosent av de som svarte på undersøkelsen uttrykte bekymring etter å ha blitt kjent med Snowden-avsløringene. Det er imidlertid et langt skritt fra å *ytre* at man føler et ubehag, til at ubehaget faktisk fører til reelle endringer i hvordan man oppfører seg i det daglige – altså at ubehaget leder til nedkjølingseffekt. Forskning har vist at folk har kognitive problemer med å overskue at opplysninger avgitt i ett konkret tilfelle kan brukes til andre og uforenelige formål på et senere tidspunkt[30]. Vi evner rett og slett ikke helt å ta denne problemstillingen inn over oss.

Selv om mange svarer at de vil fortsette som før til tross for omfattende overvåking, er det likevel en betydelig andel som oppgir at overvåkingen ville påvirket deres kommunikasjonsvaner.

[30] http://www.coll.mpg.de/publications/3258

Undersøkelsen viser tydelig at massiv *myndighetsovervåking* ville hatt en nedkjølingseffekt. Nesten tre av ti ville da vært mer forsiktig med hva de søkte etter på nett, mens nesten to av ti ville vært mer forsiktig med hvem de hadde kontakt med. Dette er høye tall som viser at en inngripende myndighetsovervåking ville rokket dramatisk ved rammebetingelsene for et fritt og åpent demokrati.

LYSER VARSELLAMPENE NÅ?

Sikkerhet og personvern blir ofte satt opp i mot hverandre. Men i stedet for å se på dette som begreper i konflikt med hverandre, bør man heller erkjenne at de tvert i mot er gjensidig avhengig av hverandre. Begge verdiene er nødvendige om vi skal ha et fungerende demokratisk samfunn. Ivaretakelse av tillit er i denne sammenheng et stikkord. En stadig mer inngripende overvåking kan føre til tap av tillit til myndighetene med nedkjølingseffekt som en konsekvens. Mister myndighetene tillitten i befolkningen vil det være vanskelig å styre effektivt. I et klima preget av lav tillit vil det også være utfordrende for etterretningsmyndighetene å gjøre en effektiv jobb – folket vil ikke lenger være på myndighetenes side i kampen om å verne felles verdier. Et for sterkt overvåkingstrykk, vil medføre tap av både personvern og sikkerhet[31].

Vår undersøkelse viser at Snowden-saken har hatt en svak nedkjølingseffekt blant norske borgere. Selv om kun åtte prosent av befolkningen oppgir å ha lagt bånd på sin kommunikasjon, er det ett tall vi bør ta på alvor. I aldersgruppen 15 til 29 år svarer imidlertid flere enn én av ti at de har tenkt seg om før de brukte visse ord og uttrykk i kommunikasjon eller i internettsøk. En viktig forutsetning for et fritt og åpent demokrati er at *ingen* skal frykte konsekvensene av å ytre seg.

Det er vanskelig å måle nedkjølingseffekt og det finnes få tall å sammenligne med. Hvor høye nedkjølingstall må til før varsellampene begynner å lyse for alvor? I mangel på historiske data, vet vi ikke om tendensen til nedkjølingseffekten er stigende. Vi vet imidlertid at det samles inn stadig mer opplysninger om oss og at kapasiteten til å lagre og analysere dem øker dramatisk. Både myndigheter og kommersielle virksomheter ønsker å vite mest mulig om oss. Det vil trolig fremover bli mer utfordrende for den enkelte å ha oversikt over hvem som har opplysninger om oss og til hvilke formål de benyttes. For å unngå at dette resulterer i en økende nedkjølingseffekt er det derfor avgjørende at både myndigheter og kommersielle aktører ivaretar folks tillit. Alternativet kan bli en nedkjølingseffekt som forringer det samfunnet vil ha, og som vi forsøker å beskytte.

[31] van der Hilst, Rozemarijn: *"Putting Privacy to the Test: How Counter-Terrorism Technology is Challenging Article 8 of the European Convention on Human Rights*", University of Oslo, 2013, Oslo

KROPPSNÆR TEKNOLOGI

De siste 20 årene har avanserte datamaskiner kommet stadig nærmere oss. På 1990-tallet ble PCen på kontorpulten til en laptop i fanget og skuldervesken. Det siste tiåret har de fleste nordmenn lagt datamaskinen i lomma som smartmobil og tatt den med oss over alt vi ferdes. Vi står nå foran det neste spranget – å bære teknologien direkte på kroppen.

Denne typen teknologi har fått navnet *wearables*, eller kroppsnær teknologi. Sensorer og datachips har blitt bedre, billigere og så små at de kan plasseres på kroppen, hjelmen eller klærne uten å komme i veien for det vi ellers skal gjøre. Siden vi allerede har koblet opp smarttelefonene til Internett via 3G eller 4G, trenger kroppsnære dingser bare f.eks. Bluetooth for å være på nett. Det forventes en åttedobling av markedet frem mot 2017. Det finnes allerede nå en rekke produkter, som for eksempel:

- Et av de kanskje mest ambisiøse eksemplene på kroppsnær teknologi så langt, er Google-brillen (*Google Glass*). For tiden prøves den ut av 10 000 betabrukere og utviklere i USA, med tanke på markedslansering i 2014. På samme måte som smarttelefonen, er Google-brillen en plattform med mange teknologier. I tillegg til telefon, har brillen en datamaskin med nettilknytning, en liten skjerm som kan vise informasjon på brilleglasset, og et kamera som kan ta bilder og video i HD.
- Samsung lanserte sin *Galaxy Gear* klokke i fjor. Du kan ringe og ta i mot tekstmeldinger, i tillegg til å ta bilder og video med et lite kamera på siden av klokkeremmen.
- *Recon Instruments Snow2* er en liten skjerm du kan feste utenpå skibrillene. Den viser deg informasjon tilpasset der du er, som din fart og løypekart. Den kan enkelt kobles til smarttelefonen, et kamera eller andre sensorer. Snart kommer det en sykkelvariant.
- *Narrative* er en klips med et lite kamera og GPS som du fester på kragen. Den tar to bilder i minuttet, og på slutten av dagen finner en algoritme frem høydepunktene for deg.

- Armbåndet *Jawbone* kan telle skritt og måle søvnmønster. Kobler du det til smarttelefonen, får du oversikt over hvor aktiv du er, og motiverende råd for en bedre helse.

HVORFOR KROPPSNÆRT?

Fire av fem nordmenn har smarttelefon, og vi sjekker den 150 ganger om dagen[32]. Men det tar tid å ta mobilen opp av lommen og skru på kameraet. Hva om vi kan ta bilder umiddelbart, og redusere tiden det tar fra vi ønsker å gjøre noe til vi faktisk gjør det?

FORSTERKET VIRKELIGHET

Teknologi for forsterket virkelighet (*augmented reality*) kobler informasjon med det du faktisk ser på. Ved å integrere informasjon inn i synsfeltet ditt, bryter man ned skillet mellom å se på skjermen og å se på verden. Det finnes flere slike tjenester på smarttelefonen allerede. Når du vender mobilkameraet mot en bygning, finner *Wikitude* din lokasjon, kjenner igjen det du peker på og leter frem og viser deg relevant informasjon.

Kroppsnær teknologi kan bringe mobile tjenester enda nærmere brukeren. Målet er å bringe kraften i mobiltelefonen ut av lomma og frem i synsfeltet ditt, slik at relevant informasjon blir tilgjengelig idet du trenger den.

Når brukeren har på seg digitale briller, kan tjenesten kontinuerlig ta bilder av omgivelsene, og lete frem informasjon som den tror er interessant. Letemannskaper som skal inn i en farlig situasjon, kan få projisert kartinformasjon og relatert informasjon oppå det de ser på gjennom brilleglassene. Slik kan de lettere orientere seg både før og idet de går inn i situasjonen.

EN PERSONLIG ASSISTENT SOM VET HVA DU VIL

Tjenestene på smarttelefonen blir mer og mer personaliserte og tilpasset den situasjonen du befinner deg i for øyeblikket. Google tjenesten "Nå" har som mål å være en personlig assistent som gir deg informasjon når det er mest sannsynlig at du trenger den. Den kobler informasjon fra bl.a. e-posten og

[32] Kleiner Perkins Internet trends 2013, 6. juni 2013:"A Few More Thoughts On Our Internet Trends Report"

kalenderen din med ordene du søker på og informasjon om hvor du er, og gir deg informasjon som passer dine planer og interesser. Det kan være informasjon om forsinkelser på flyet du skal ta, eller raskeste vei i rushtrafikken når det nærmer seg den tiden du normalt reiser hjem.

Når teknologi for forsterket virkelighet kobles til den personlige assistenten på den digitale brillen, kan du få presentert skreddersydd informasjon umiddelbart i synsfeltet. Du sparer de sekundene det tar å ta opp mobilen fra lomma for å sjekke noe, og kan t.o.m. få opp informasjonen *før* du ber om den.

I vår undersøkelse kunne én av fire – og nesten halvparten i alderen 15–29 år – tenke seg å ta i mot tips på Google-brillen om at en butikk i nærområdet fører den varen de leter etter. Hvis t-banen du pleier å ta hjem er forsinket, kan brillen gi beskjed og vise på kartet at det nå i stedet lønner seg å ta bussen to kvartaler unna.

ANSIKTSGJENKJENNING

Algoritmer for mønstergjenkjenning kan gjenkjenne ting, bygninger og personer i bilder og video. Mønstergjenkjenning kan fortelle deg at det for eksempel er Colosseum du ser på.

En viktig type mønster er et menneskes ansikt. Tilgang til ett bilde der du er identifisert, er nok til å gjenkjenne deg automatisk på andre bilder. Profilbildet ditt i Facebook er knyttet opp til navnet ditt, og kan brukes som utgangspunkt for slike søk.

I løpet av en dag vil du se mange ansikter. Digitale briller følger øyene dine. De er også en datamaskin, som med programvare for ansiktsgjenkjenning kan identifisere menneskene du møter. Det kan være nyttig for å hjelpe oss å huske folk.

I vår undersøkelse kunne én av fem tenke seg å be Google-brillen om å hjelpe seg å kjenne igjen mennesker de ikke kjenner igjen selv. Når brillen gjenkjenner et ansikt, kan de finne frem informasjon som for eksempel når dere møttes sist. Det vil også kunne hjelpe mennesker med demens.

KROPPSKAMERAET SOM VITNE

Digitale kameraer er nå rimelige, har høy kvalitet, og er så små og lette at de kan plasseres på nær sagt alle ting. Det blir enkelt å gjøre opptak uten å måtte

trekke opp et kamera eller en mobiltelefon fra lommen. Du kan gi en enkel talekommando, eller kanskje bare blunke, for at kameraet skal ta et bilde.

Kameraene kan kobles trådløst til smarttelefonen, der bildene kan behandles og deles videre, for eksempel i sosiale medier, med arbeidsgiver eller med offentlige instanser som politiet.

Lagring er dessuten blitt så billig at det er mulig å filme hele tiden – for f.eks. å være føre var om en skulle ha behov for dokumentasjon. I vår undersøkelse kunne 36 prosent tenke seg å bruke Google-brillen til å ta opp video av en farlig trafikksituasjon (f.eks. en forbikjøring). Nesten 45 prosent av mennene og over halvparten av de mellom 15 og 29 år kunne tenke seg dette. Over én million russiske sjåfører har montert kameraer i bilen for å kunne dokumentere sine krav overfor forsikringsselskapet.[33] Under en drapssak i Ålesund viste det seg at en syklist tilfeldigvis hadde filmet gjerningsmannen med et kamera festet på sykkelen sin rett før gjerningen fant sted.[34]

Kroppsnære kameraer er i økende grad blitt tatt i bruk av politi og vaktselskaper. Politiet i land som Sverige, Danmark, Tyskland, Frankrike, Storbritannia og noen steder i USA, har tatt i bruk kroppsnære videokameraer for å dokumentere pågripelser og andre hendelser.

Tidlig bruk av slike videokameraer har allerede vist positive effekter. Tiltalte sier seg skyldig tidligere når de blir konfrontert med opptakene av sine handlinger. Folk i slagsmål roer seg ofte raskt ned når de får vite at de blir filmet. Klager fra publikum om politivold eller maktmisbruk kan bli avgjort raskere og med mindre byråkrati. I Rialto i California har vold mot politiet falt med 59 prosent etter at de begynte å bruke kameraer.[35]

Dørvakter på noen utesteder i Oslo har begynt å filme bråkmakere med kameraer de har festet på brystet. På den måten kan de både unngå at en situasjon eskalerer, og bruke opptakene til å vise politiet hva som faktisk har skjedd, hvis det skulle bli nødvendig. Det har vist seg at bråkmakerne som regel forsvinner frivillig.

---

[33] The Economist, 16. november 2013: 13. "Ubiquitous cameras: The people's panopticon",
[34] Dagbladet, 6. september 2013: "Vitne til Dagbladet: - Jeg filmet drapsmannen på Aksla-fjellet"
[35] New Scentist, kktober 2013: "Body-worn cameras put police evidence beyond doubt". Politiet i Rialto brukte tidligere bl.a. et kamera som de festet på skulderen. De vurderer nå å bruke Google Glass. Kontinuerlig overføring av GPS-posisjonen gjør at operasjonssentralen kan vite hvor patruljene til enhver tid er, samtidig som patruljene kan vise dem hvordan en situasjon utvikler seg, fra sitt perspektiv.

PERSONVERNUTFORDRINGEN

Kroppsnær teknologi gir oss et utvidet sanseapparat. Samtidig blir teknologien mindre synlig for andre når den smelter sammen med kroppen. Vi må også regne med at det vil bli lagret mye mer informasjon om hva vi gjør og hvor vi beveger oss.

Dette vil gi virksomheter, myndigheter og privatpersoner mulighet for å utlede hvor vi har vært, og hva vi har gjort når. Til sammen kan de sette sammen puslespillbrikkene om våre liv til et omfattende bilde. Det gjelder ikke bare de som står foran kamera, men også de som står bak.

Spørsmålet er dermed om våre normer, bransjens egne regelverk og vårt etablerte lovverk er tilstrekkelig i møte med kroppsnær teknologi. Vil vi ha behov for at myndighetene engasjerer seg, eller bør de la innovasjonen få spillerom og se an utviklingen?

VÅR EGEN PERSONVERNFELLE

Enhver interessant bruk av teknologi som lover forsterket virkelighet, er en potensiell personvernfelle: Jo mer informasjon du gir fra deg, desto bedre blir tjenesten. Tjenestene er i sin natur kontekstspesifikke – leverandørene må vite hvor du er og fester blikket, hva du gjør, og hva du ønsker å vite.

Selv om det er du som befinner deg bak kameraet, samles det inn store mengder personinformasjon om deg selv. Du bruker tjenestene for å analysere og lære om verden, men i realiteten gir du fra deg enda mer informasjon. Det kan være vanskelig, kanskje nesten umulig, fullt ut å forstå konsekvensene av bruken.

Vi brukere kan trenge mer hjelp og veiledning enn lange og komplekse vilkår vi må godkjenne for å få ta i bruk en ny app eller tjeneste, og som kanskje de færreste tar seg tid til å lese og forstå.

Vi kan se for oss ulike måter å fremme god bruk av kroppsnær teknologi på:

Selvregulering: Godkjenningsordninger som bransjen som helhet blir enige om, eller som de enkelte markedsaktørene fastsetter, kan være med på å trygge bruken av kroppsnær teknologi. Google har for eksempel krav til bruk og deling av personlig informasjon for utviklere av apper til Google-brillen.

Aktørene kan imidlertid endre kravene når de selv ønsker det, og tilpasse dem til sine egne interesser. I internettøkonomien er disse interessene nært knyttet til innsamling av persondata – enten for å lage personlige tjenester, pushe reklame eller for å selge personopplysninger videre til andre.

Det kan også stadig komme nye app-butikker på markedet med andre godkjenningsordninger. Og hva med applikasjoner som distribueres gjennom andre kanaler?

Merkeordning: Kan myndighetene stimulere til god bruk ved å innføre en merkeordning – en slags "svanemerking" for personvernet? Elementer i en slik merkeordning kan for eksempel være krav til:

- lagring og sikring av data fra utstyret
- hvordan data fra utstyret brukes og deles
- transparens

Nytt regelverk: Er personvern- og forbrukerlovgivningen god nok? Ett alternativ kan være at myndighetene regulerer bruken av kroppsnær teknologi på spesifikke områder eller situasjoner direkte i et regelverk. Hvordan skal myndighetene kontrollere etterlevelsen, uten å gripe for langt inn i den kontrollertes privatliv?

FARVEL ANONYMITET?

Folk som bruker kroppsnær teknologi rettet mot omverdenen, blir i praksis behandlere av store mengder informasjon. Når de tar bilder av folk rundt seg, bidrar de til å kartlegge oss, uten at vi trenger å legge merke til at det skjer. Det vil ikke nødvendigvis fremgå tydelig når vi blir tatt bilde av eller blir gjenkjent og identifisert.

Hvordan andre deler og offentliggjør bilder, kan få store konsekvenser for deg, uten at de nødvendigvis forstår rekkevidden av det. Personer og virksomheter som får tilgang til informasjonen, kan sammenstille den med ytterligere datakilder. Det kan være en fremtidig arbeidsgiver, forsikringsselskapet eller en ny flamme.

Ansiktsgjenkjenning står i en særstilling i denne sammenhengen. Når du blir identifisert i ett bilde, kan andre bruke det som en nøkkel til å få tilgang til

mye mer informasjon om deg. Sammenstilt med annen informasjon, kan de finne ut hvor du har vært, og hva du har gjort når. Det kan være tid og sted for alle demonstrasjoner du har vært med på.

Det som skjer når brillen identifiserer deg, er at algoritmer for ansiktsgjenkjenning sammenligner bildet av deg med alle bildene de har tilgang til. Hvis algoritmen finner minst ett bilde av deg med informasjon om identiteten din, har brillen automatisk identifisert deg med stor sannsynlighet. Profilbildene på LinkedIn og Facebook, eller på nettsidene til arbeidsgiveren din, er knyttet til navnet ditt, og plutselig ikke så uskyldige lenger.

Privatpersoners bruk av ansiktsgjenkjenning faller stort sett utenfor personopplysningslovens regler. Ett eksempel på privat bruk kan være å gjenkjenne ansikter og sortere alle bilder i sitt eget digitale fotoalbum etter person, noe som er ganske uskyldig. Men kobler noen derimot de private bildene av deg med åpen informasjon på Internett, kan de ved å bruke teknikker for mønstergjenkjenning og dataanalyse lage ganske avanserte oversikter over dine sosiale nettverk, adferd og interesser. Slik privat bruk av mønsterkjenning kan virke personvernkrenkende, men faller utenfor dagens regelverk.

I Norge er lovreguleringen teknologinøytral. Bruk av teknikker for mønstergjenkjenning og ansiktsgjenkjenning er ikke regulert spesifikt i norsk lov. For å vurdere lovligheten, må man vurdere hvordan ansiktsgjenkjenning blir brukt i hvert enkelt tilfelle. De vanlige personvernprinsippene som formål og samtykke vil være viktig i vurderingen.[36]

Samtykke som kriterium for å godkjenne ansiktsgjenkjenning kan imidlertid være vanskelig både å gi og å overholde. Det vil i praksis være umulig å kreve samtykke fra alle man møter i løpet av en dag. Og hva ber vi egentlig om samtykke til? Selv om man skulle gi sitt samtykke til å bli tatt bilde av, vil man antakelig ikke med det mene at andre skal kunne gjøre ansiktsgjenkjenning av bildene.

Vi kan se for oss ulike måter å regulere bruken av ansiktsgjenkjenning på:

Selvregulering: Myndighetene kan velge å overlate til selskapene å etablere regelverk som fremmer god bruk av ansiktsgjenkjenning. De har både interes-

[36] Europeiske datatilsynsmyndigheter har vedtatt en felles uttalelse om bruk av teknologi for ansiktsgjenkjenning på Internett og i mobile tjenester. Samtykkekravet er et sentralt tema i anbefalingene. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf

ser og insentiver for at deres løsninger skal bli tatt i bruk. Google tillater for eksempel ikke appene som bruker Google-brillen å bruke ansiktsgjenkjenning, og det må synes på brillen når kameraet er på.

Kanskje vi kan stole på at Google kun godkjenner applikasjoner som ikke bruker ansiktsgjenkjenning, men hva med små selskaper som ikke nødvendigvis har samme interesse i å fremstå som seriøse på dette området?

Nytt regelverk: Dagens regelverk beskytter privat bruk av ansiktsgjenkjenning i liten grad. Bør myndighetene rett og slett forby ansiktsgjenkjenning til privat bruk? Eller bør det blir forbudt å legge ut bilder av andre usladdet, fordi bildet da per definisjon er "tagget"? Og hva vil det i så fall ha å si for ytrings- og pressefriheten? Er dette mulig å håndheve?

Normer og sosial kontroll: Kan det være at sosial kontroll på sikt bidrar til å justere bruken til et nivå som de fleste av oss finner akseptabelt? Vil den enkelte av oss justere de forventninger vi har til omgivelsene våre, slik at vi i større grad aksepteres at vi behandler opplysninger om hverandre?

PROFESJONELL BRUK AV KROPPSKAMERAER

Bruk av kroppskameraer skiller seg fra fastmonterte overvåkingskameraer på ett viktig punkt: de muliggjør også at folk kan overvåke overvåkerne. En slik gjensidighet krever imidlertid at noen viktige spørsmål avklares:

- Hvem kan bruke opptakene og til hvilke formål?[37] I politisaker kan det for eksempel være et krav at datalagringssystemet for videobevis er tilgjengelig for advokater og tiltalte.[38]
- Bør det kreves at hele det filmede hendelsesforløpet gjøres tilgjengelig? Hvis bare deler av hendelsesforløpet filmes, kan det vris til den ene partens fordel.
- Hva er rimelig lagringstid og regler for sletting?
- Bør det komme klart frem at det filmes, for eksempel i form av en skjerm vendt mot publikum?
- Er det greit at vi får et arbeidsliv der de ansatte i større grad pålegges å dokumentere sin arbeidsdag i form av bilder og video?

[37] Oslo By, 18. september 2013: "Roer ned bråkmakerne med kamera på brystet"
[38] ACLU, 9. oktober 2013: "Police Body-Mounted Cameras: With Right Policies in Place, a Win For All"

METADATA OG DEN NYE OVERVÅKINGEN

”…nobody is listening to your telephone calls. That´s not what this program is about. (…) They are not looking at people´s names, and they are not looking at content.”39

Barack Obama, 7. juli 2013

Etter de første Snowden-avsløringene tidligere i år, imøtegikk president Obama kritikken ved å si at NSA ikke rører ved innholdet i kommunikasjonen til vanlige amerikanere. Men hvis etterretningstjenestene ikke lytter til innholdet, hva er det da de gjør?

Snowden-avløringene har tydeliggjort minst to viktige trender i moderne etterretningspraksis.

For det første ser vi at etterretningstjenester har flyttet fokuset vekk fra selve *innholdet* i kommunikasjonen til data som forteller noe om hvilken sammenheng og i hvilke omgivelser innholdet deles. Spørsmål som ”hvor befant du deg?” erstatter ”hva gjorde du der?”, ”hvem snakket du med?” erstatter ”hva snakket du om?”, osv.

Begrepet metadata har blitt et nøkkelord i moderne overvåking. Informasjon som mange tidligere kanskje oppfattet som ufarlig og lite personsensitiv, er i dag selve råstoffet for mye etterretning.

For det andre ser vi en bevegelse vekk fra målrettet og begrenset informasjonsinnsamling til masseovervåking. Rapporter om at NSA daglig samler inn nær 200 millioner tekstmeldinger[40] og gjør nærmere 5 milliarder registreringer fra basestasjoner i mobilnett over hele verden[41], viser et tydelig skifte i moderne etterretningspraksis. Metadata er med på å legge til rette for slik masseovervåking.

---

[39] http://www.whitehouse.gov/the-press-office/2013/06/07/statement-president

[40] http://www.aftenposten.no/nyheter/uriks/NSA-samler-inn-millioner-av-tekstmeldinger-daglig-7436656.html#

[41] http://www.nordlys.no/nyheter/Utenriks/article7025317.ece

Begge disse trendene både understøttes og drives frem av den raske utviklingen innen moderne IKT. Og mens samfunnet digitaliseres i rasende fart, ser vi et voksende gap mellom hva etterretningstjenester har lov til å gjøre og det de faktisk *kan* gjøre.

Vår digitale kommunikasjon og dens biprodukter gir etterretningsorganisasjoner anledning til å kartlegge aktiviteter, sosiale relasjoner og bevegelsesmønstre til nesten hvem som helst, hvor som helst i verden – uten å være fysisk tilstede eller lytte til innholdet i samtaler og skriftlig kommunikasjon.

Selv om interessen for slik informasjon kanskje ikke er ny i etterretningsbransjen, har den teknologiske utviklingen gjort det vesentlig enklere å ta i bruk slik informasjon – og det er nettopp dette nye mulighetsrommet Snowden-avsløringene har satt i søkelyset.

Når det finnes færre tekniske begrensninger på hva etterretningstjenster kan gjøre, blir det desto viktigere å være var på hva de bør gjøre og hva de ikke bør gjøre.

HVA METADATA FORTELLER OSS

Metadata betegnes ofte som ”data om data” og genereres automatisk når vi bruker ulike digitale verktøy og tjenester. De er nødvendige bestanddeler for at datasystemer skal kunne vite hvordan de skal forvalte, behandle og presentere informasjonen for deg som bruker.

HVA ER METADATA?

Metadata er informasjon som beskriver, forklarer, lokaliserer eller på andre måter forenkler prosessen med å hente frem, bruke og forvalte en gitt informasjonsressurs i et digitalt økosystem – slik som for eksempel en e-post. Den forteller bl.a. hvem e-posten er fra og hvor den skal sendes. I en e-postutveksling kan metadata typisk inneholde informasjon om:

- avsenders og mottakers navn, e-postadresse, IP-adresse og server
- tid, dato og tidssone

Også det digitale bildet i vedlegget til e-posten vil ofte ha metadata knyttet til seg som forteller

- når bildet ble tatt (og hvis kameraet kjenner eieren, også hvem fotografen var)
- hvor bildet ble tatt
- teknisk informasjon om bildefilen (piksler, dimensjon, oppløsning, orientering, osv.)
- kameramodell og kamerainstillinger

Etter hvert som informasjonen vår har blitt mer digital, har også bruken av metadata økt i omfang. Betrakter man slike data isolert, kan de ofte virke uskyldige og lite interessante. Med riktig analyse og kontekst kan metadata imidlertid gi innsikt i svært personsensitiv informasjon – som for eksempel sosiale relasjoner, politisk orientering, bevegelsesmønstre, helsesituasjon og seksuelle preferanser.

Metadata tilknyttet en vanlig Twitter-melding, med bl.a. navn, lokasjon, tidspunkt og språk. Kilde: http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance

KONTEKST AVSLØRER INNHOLD

Når metadata blir satt i riktig sammenheng, kan slik informasjon tegne et svært detaljert bilde av hvem du er, hva du gjør og hvem du omgås[42]:

- Metadata avslører ikke innholdet i en samtale, men kan vise at du ringte gynekologen din, pratet i 23 minutter og like etter ringte en abortklinikk.
- Metadata avslører ikke innholdet i en samtale, men kan vise at du ringte Kirkens SOS krisetelefon fra gangbrua over E18.
- Metadata avslører ikke innholdet i din kommunikasjon, men kan vise at du benyttet deg av en nettdatingtjeneste for homofile.

Når metadata settes i riktig kontekst, kan de altså være vel så avslørende som – om ikke mer avslørende enn – innholdsdata.

I februar 2013 publiserte forskningstidsskriftet Nature en oppsiktsvekkende studie gjennomført av forskere ved MIT og universitetet i Louvain, som viser at kun fire tidsangitte lokasjonsmetadata (informasjon om hvor og når du var på et sted), er nok til å til å tilskrive 95 prosent av befolkningen et unikt bevegelsesmønster[43] . Med andre ord er det kun 5 prosent av befolkningen det er umulig å skille fra hverandre – nesten alle legger fra seg et unikt metadata-avtrykk. Slike metadata genereres automatisk når mobiltelefoner kobler seg til mobilantenner eller WiFi-nettverk. Til sammenligning behøver man hele 12 punkter for å definere ditt unike fingeravtrykk. Fordi våre daglige mobilitetsmønstre ofte er unike og varierer svært lite, er kun noen få punkter og litt kontekst nok til å identifisere de fleste av oss.

Mens slike bevegelsesmønstre tidligere kun var tilgjengelige for teleoperatørene, gjør utbredelsen av smarttelefoner denne informasjonen nå tilgjengelig i helt nye datastrømmer på Internettet, for eksempel gjennom applikasjoner. Selv anonymiserte metadata kan krysskobles med annen informasjon for å identifisere individer.

[42] https://www.eff.org/deeplinks/2013/06/why-metadata-matters
[43] http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html

EN NASJONAL DATABASE FOR PERSONLIGE RELASJONER

Når metadata aggregeres og analyseres, kan informasjonen være svært personverninngripende, ikke bare for personen som overvåkes, men også for personer vedkommende har kontakt med elektronisk.

I juni 2013 lanserte studenter ved MIT tjenesten Immersion[44]. Den lar deg visualisere de sosiale nettverkene dine ved hjelp av metadata hentet fra e-postleverandører som for eksempel Gmail. Slike nettverk blottlegger tydelig dine nære relasjoner, ulike grupper av mennesker du jobber med, og hvem som fungerer som bindeledd mellom disse gruppene - både i jobbsammenheng og privat. Den viser hvem dine venner og bekjente er, hvem du var sammen med før du møtte din nåværende partner, og hvem du har mistet kontakten med i ulike faser av livet. Er du journalist, kan et slikt metadata-nettverk lett avsløre hvem som har vært kilden til dine ulike artikler.

Metadata innsamlet over tid kan altså tegne svært intime bilder av våre liv: hvem vi har kjær, hvem våre venner er, hvem vi jobber med, hvor vi befinner oss, hvor vi står politisk, osv[45].

Derfor har NSAs innsamling og lagring av metadata blitt omtalt som en ”nasjonal database for personlige relasjoner”[46].

RÅSTOFF FOR DEN NYE OVERVÅKINGEN

Hvorfor har metadata på mange måter blitt den nye oljen i moderne etterretning?

For det første har volumet av digital informasjon eksplodert. Vår daglige bruk av e-post, smarttelefoner og ulike internettjenester gir opphav til en enorm informasjonsmengde, som for kun få år siden var nærmest utenkelig. Nye digitale verktøy gjør at vi kommuniserer hyppigere enn før, og vi gjør det i stadig flere kanaler. Det gir opphav til nye informasjonskilder.

Samtidig har evnen til å lagre og bearbeide informasjon styrket seg veldig bare det siste tiåret – mens prisen har sunket kraftig. Metadata forenkler arbeidet med å bearbeide denne informasjonsrikdommen.

---

[44] https://immersion.media.mit.edu
[45] https://www.aclu.org/blog/technology-and-liberty-national-security/my-life-circles-why-metadata-incredibly-intimate
[46] http://www.wired.com/opinion/2013/06/phew-it-was-just-metadata-not-think-again/

For det andre beveger slik informasjon seg daglig på kryss og tvers av landegrenser. Internett er blitt en bærer for mye av verdens kommunikasjon, og nettjenester som Google og Twitter er i dag globale leverandører.

Den digitale kommunikasjonen er gjerne innom mange ulike land, selv om både sender og mottaker befinner seg i samme land. For etterretningstjenester betyr dette et redusert behov for dyre fysiske lytteposter i utlandet som skal fange opp viktig informasjon. Nær 90 prosent av verdens online-kommunikasjon passerer gjennom USA[47], og informasjonen som styrer denne kommunikasjonen lagres ofte hos (et fåtall) amerikanske skytjenester.

For det tredje skiller metadata seg fra innholdsdata på måter som gjør den spesielt egnet i overvåkingsøyemed:

- Metadata er såkalt strukturert informasjon, noe som gjør at den lett kan leses av en datamaskin. Det legger til rette for å bruke maskiner for å analysere større datamengder enn ved tradisjonelle overvåkningsmetoder, og åpner samtidig dørene for masseovervåking.

- Som vi har sett, er det relativt enkelt å utlede innhold når tilhørende metadata settes i riktig sammenheng. Med store datamengder gjør metadata det enklere å organisere informasjonen, se etter mønstre og kartlegge sosiale relasjoner mellom individer. Når teknikker for storskala dataanalyse – såkalte Big Data-teknikker – brukes på metadata, kan utfallet ofte være mer verdifullt og informasjonsrikt enn selve innholdsdataene.

- Innholdsdata kan være vanskelige og ressurskrevende å analysere også for mennesker. De stiller bl.a. krav til kunnskap om ulike språk, sosiolekter og uttrykksformer, og åpner dermed for usikre tolkninger. Med metadata unngår man disse problemene.

Samlet gjør disse egenskapene metadata særlig egnet som informasjonskilde i moderne etterretning, og vi ser at den teknologiske utviklingen gjør det enklere å utnytte dette mulighetsrommet.

Evnen til å "lytte til" digital kommunikasjon er en nødvendig forutsetning for at etterretningstjenester skal kunne løse sine oppgaver. Samtidig er det viktig å passe på at vi ikke strekker strikken for langt, slik at det går ut over personvernet og demokratiske rettigheter.

---

[47] http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents

PERSONVERNUTFORDRINGEN

Metadata er et naturlig biprodukt av det digitale samfunnet. Når bruken av digital kommunikasjon fortsetter å øke i omfang, vil også metadata genereres og gjøres tilgjengelige i stadig større grad.

Vi har sett at tilsynelatende uskyldige metadata kan brukes til å tegne svært avslørende bilder av våre liv, og at slik informasjon egner seg svært godt i etterretningssammenheng.

Etterretningspraksisen i USA etter terrorangrepene 9. september 2001 har utviklet seg parallelt med den hurtige fremveksten av Internett og det digitale samfunnet. Mange bransjer jobber i dag på helt andre måter enn for kun få år siden. Da er det naturlig at også etterretningsvirksomheter er en del av denne endringsprosessen.

Digital informasjon har eksplodert både i omfang og variasjon, og samtidig åpnet nye mulighetsrom for etterretningsbransjen, særlig gjennom metadata.

Metadata er, til forskjell fra mange typer innholdsdata, både billige og enkle å aggregere og analysere maskinelt. Til tross for at NSA har brukt metadata til å overvåke millioner av mennesker, antyder lekkasjer fra Snowden at NSAs metadataprogram ikke koster mer enn om lag én prosent av organisasjonens årlige budsjett[48].

De fleste land har lovverk og tilsyn som regulerer hvordan etterretnings- og sikkerhetstjenester skal utøve sin virksomhet, og på hvilket grunnlag de kan overvåke ulike deler av befolkningen. Men nettopp fordi overvåking tidligere var både dyr og teknisk krevende, begrenset det omfanget for de fleste etterretningstjenester. De tekniske og økonomiske barrierene har vært en vel så viktig beskyttelse mot masseovervåking som lovverk og tilsyn. Snowden-avsløringene viser tydelig at disse barrierene nå er i ferd med å viskes ut. Det reiser nye utfordringer.

Denne utviklingen synes bare å tilta i årene som kommer, og gjør at vi må revurdere politikken på området. Metadata er en nødvendig del av vårt digitale samfunn. Hva kan vi så gjøre for å beskytte oss mot overvåking? Hva kan vi som enkeltindivider gjøre? Hvordan ser vi våre egne etterretningstjenester i

[48] http://www.technologyreview.com/view/516691/soaring-surveillance/

kortene? Og hvordan kan vi som land beskytte oss mot overvåking fra andre nasjoner?

HAR VI RETT TIL Å VÆRE ANONYME PÅ NETT?

Mens det i dag finnes mange metoder for å kryptere og sikre innhold og nettverksforbindelser i vår digitale kommunikasjon, er det mye vanskeligere å sikre seg fullstendig mot å legge igjen metadata-spor i vår omgang med hverdagsteknologi som telefonsamtaler, internettsøk, bruk av sosiale medier, digitale kamera, osv.[49]

Telefontjenester som Silent Circle[50] og RedPhone[51] sørger eksempelvis for krypterte telefonsamtaler over Internett, men det er likevel vanskelig å skjule for eksempel nummeret man ringer til og fra, fordi denne informasjonen er nødvendig for å gjennomføre samtalen. Avsløringer om at NSA bevisst har svekket kommersiell krypteringsteknologi, har ført til ytterligere usikkerhet rundt slike verktøy[52].

Det finnes likevel noen verktøy som på ulike måter "vanner ut" metadata-spor og gjør dem vanskeligere å tyde. Tor[53] gir for eksempel brukeren anonymitet på nett ved at IP-adressen holdes skjult. Slike verktøy kan imidlertid være krevende for folk flest å ta i bruk, og er i tillegg ofte for langsomme til at de brukes i daglig sanntidskommunikasjon.

Har myndighetene likevel en rolle å spille i å sørge for at nordmenn har sikker og kryptert kommunikasjon, og at vi etterlater oss færrest mulig spor på Internett? Her vil vi i så fall måtte avveie motstridende hensyn.

Enhver anledning til å forbli anonym på nett, vil kunne utnyttes og misbrukes av kriminelle, og gjøre det vanskeligere for myndighetene å forebygge kriminalitet og alvorlige trusler.

Dessuten finnes sterke kommersielle insentiver for at vi skal legge igjen metadata-spor. På samme måte som Amazon gir sine brukere tilpassede kjøpsanbefalinger, er store deler av Internett-økonomien bygget på kjennskap til bru-

---

[49] http://www.pcworld.com/article/2042096/does-encryption-really-shield-you-from-governments-prying-eyes.html
[50] https://silentcircle.com
[51] https://whispersystems.org
[52] http://www.wired.com/threatlevel/2013/09/nsa-backdoored-and-stole-keys/
[53] https://www.torproject.org

kernes behov og godt tilpassede tjenester. Ved full anonymitet vil vi miste disse fordelene.

DEMOKRATISK KONTROLL, TILSYN OG ÅPENHET

Snowden-avsløringene har vist at den hurtige teknologiske utviklingen utfordrer regelverket og tilsynsmekanismene som i dag regulerer virksomheten til etterretningstjenestene. De må videreutvikles, både i takt med teknologien og endringer i etterretningspraksis.

Amerikanske myndigheter har fått kritikk for ikke å kunne føre tilstrekkelig tilsyn med sine etterretningstjenester. Ett eksempel er den føderale FISA-domstolen, som bl.a. regulerer NSAs tilgang til trafikk- og lokaliseringsmetadata. Høringer i domstolen er unntatt offentligheten, og har fått kritikk for manglende transparens og åpenhet. Det finnes heller ingen uavhengig juridisk instans som sjekker om sikkerhetsmyndighetene faktisk opptrer i tråd med lovverk og retningslinjer[54].

Med en FISA-klarering har NSA fått anledning til å samle inn, lagre og analysere telefoni-metadata, ikke bare til en mistenkt, men også til alle denne personen har vært i kontakt med og alle disse igjen har vært i kontakt med, i maksimalt tre ledd[55]. Hvis hver person har 40 kontakter, betyr dette at over 2,5 millioner mennesker kan trekkes inn i én enkelt sak[56]. En slik vid tilgang åpner for en massiv overvåking som lett kan oppleves som å stå i misforhold til legitime informasjonsbehov.

I sin NSA-reformtale 17. januar 2014, tok president Obama til orde for visse innstramninger i bruken av telefoni-metadata, bl.a. at vært søk i innsamlet materiale krever en rettslig kjennelse og at søket maksimalt kan involvere personer to ”hopp” vekk fra en mistenkt. Han foreslo også et uavhengig ”personvern-panel” som skal bistå FISA i kompliserte saker. Samtidig gjorde han det klart at metadata-innsamlingen var en viktig del av etterretningskraften og at praksisen vil fortsette, om enn i en noe revidert form[57].

---

[54] http://www.theguardian.com/commentisfree/2013/jun/19/fisa-court-oversight-process-secrecy
[55] http://www.theguardian.com/world/2013/jul/17/nsa-surveillance-house-hearing
[56] https://www.aclu.org/time-rein-surveillance-state-0
[57] http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence

Masseovervåking med metadata i Norge?

I Norge knyttes debatten rundt metadata og overvåking først og fremst til Datalagringsdirektivet – et foreslått direktiv som pålegger lagring av abonnements-, lokaliserings- og trafikkmetadata for ulike typer telefoni, e-post og internettilgang[58]. Dataene lagres hos telefoni- og internettleverandører i seks måneder, og skal kun utleveres til nasjonale myndigheter ved etterforskning av en tilstrekkelig alvorlighetsgrad, og da kun metadata knyttet til én bestemt sak eller person. Trafikk- og lokaliseringsdata skal kun utleveres til politi- og påtalemyndighet (samt PST/Finanstilsynet), og kun etter pålegg av en domstol.

Til forskjell fra praksis i USA, er metadata i Datalagringsdirektivet underlagt en åpen domstol. Innsamlingen og lagringen gjøres av teleoperatørene og ikke av myndighetene. Reguleringen gir heller ikke politi- og sikkerhetsmyndigheter full tilgang til alle metadata tilknyttet det sosiale nettverket rundt en mistenkt. I så måte har reguleringen rundt bruken av Datalagringsdirektivet en innebygget beskyttelse mot statlig masseovervåking av den typen Snowden-avsløringene har avdekket.

Likevel kan det være betimelig å revurdere Datalagringsdirektivet og kontrollmekanismene rundt bruken av metadata i lys av disse avsløringene. Lagring og analyse av innholdsdata har tradisjonelt blitt sett på som en betydelig større krenkelse av frihet og personvern, enn lagring av metadata. Forkjempere for Datalagringsdirektivet i Norge har lagt vekt på at direktivet ikke omfatter lagring av innholdsdata eller medfører avlytting av norske borgere[59]. Det har utvilsomt vært et viktig premiss for at direktivet har fått politisk gehør.

Bør vi i lys av Snowden-avsløringene vurdere om også metadata er tilstrekkelig regulert og beskyttet i Norge?

Bør vi reformere EOS-utvalget?

I Norge er det EOS-utvalget som fører løpende kontroll med Norges etterretnings- og overvåkings og sikkerhetstjenester.

---

[58] https://www.datatilsynet.no/Global/04_analyser_utredninger/2011/2011-11-15-Direktiv2006-24-EF.pdf
[59] http://www.aftenposten.no/meninger/debatt/article3637670.ece

Teknologien spiller en stadig større rolle i moderne etterretning. Da er det viktig at våre tilsynssystemer videreutvikles, både i takt med teknologien og endringer i etterretningspraksis.

Særlig blir det viktig å sørge for at EOS-utvalget til enhver tid har den nødvendige kompetansen, de riktige ressursene, og innsikt i hvilke konsekvenser nye datadrevne overvåkningsteknikker kan ha for både rettssikkerhet, personvern og viktige samfunnsverdier. I dag har sekretariatet tung juridisk kompetanse med en teknisk sakskyndig som jobber på timebasis[60]. Er det behov for å styrke den tekniske kapasiteten og er de nåværende kontrollmetodene riktig tilpasset det nye teknologiske mulighetsrommet?

Den økende informasjonsutvekslingen mellom etterretningstjenester i ulike land gjør det dessuten vanskeligere å drive demokratisk tilsyn. EOS-utvalget rapporterer i årsmeldingen for 2012 at utvalget er avskåret fra å søke i E-tjenestens datasystemer, nettopp pga. slik informasjonsutveksling[61]. Dette resulterer i at E-tjenesten underlegges en svakere kontroll enn ønskelig.

Ny teknologi som muliggjør automatisert og nær øyeblikkelig analyse av enorme mengder digital informasjon, har revolusjonert moderne etterretningspraksis. Etter hendelsene 22. juli 2011 har PST fått tydelig signal om å styrke bruken av IKT[62]. Da er det naturlig at tilsynet styrkes samtidig. Hvordan kan vi sikre at EOS-utvalget er skrudd sammen slik at det vil fortsette å føre et robust demokratisk tilsyn med våre etterretnings- og overvåkningstjenester også i fremtiden?

FRA INTERNETT TIL NASJONALE NETT

Uansett hvor god nasjonal regulering og tilsyn er, kan vi fort oppleve at dataene våre er rettsløse i utlandet. Hvordan kan vi sikre oss mot utenlandske aktører som ikke er underlagt norsk lov og tilsyn?

---

[60] http://www.eos-utvalget.no/hXGXCTgZfKYp.35.idium
[61] http://www.eos-utvalget.no/filestore/MLDFORK2012.pdf
[62] http://www.regjeringen.no/upload/JD/Dokumenter/Rapporter/2012/Ekstern_gjennomgang_av_PST.pdf

Hvor skal våre data ligge?

I kjølvannet av Snowden-avsløringene opplevde den norske skytjenesten Jottacloud en markant vekst i kunder som ønsket en lagringstjeneste med norske personverngarantier[63].

Flere land vurderer tiltak som skal sørge for at elektroniske data holdes på nasjonale datasentre. Et lovforslag som nå vurderes i den brasilianske nasjonalforsamlingen tar til orde for at internettaktører som er aktive i Brasil, som for eksempel Facebook og Google, må sette opp lokal infrastruktur i landet slik at data knyttet til brasilianske brukere lagres i Brasil og ikke i vilkårlige datasentre i utlandet. Videre vurderer Brasil, i likhet med Tyskland, å etablere nasjonale, krypterte e-posttjenester.

Geografisk plassering av data er viktig fordi det bestemmer hvilken jurisdiksjon dataene kommer inn under. Foreksempel vil data som en nordmann lagrer på en tjeneste i USA komme inn under amerikansk lovgiving som "the USA Patriot Act". Dersom amerikanske myndigheter får tilgang til dataene gjennom denne loven, har ikke tjenestetilbyder lov til å fortelle nordmannen at dataene er blitt brukt på denne måten. Geografisk plassering er derfor viktig for å sikre dataene gjennom nasjonal lovgivning. Det kan muligens også bidra til å heve terskelen for overvåking fra andre land.

Slike forslag har fått kritikk for å være dyre, innovasjonsbegrensende, og et første steg i retning av en ”balkanisering” av Internett[64]. Mange frykter at en slik utvikling vil bety slutten på Internett som en driver for innovasjon og økonomisk vekst. For et lite land som Norge, kan det dessuten være vanskelig å etablere en bærekraftig nasjonal Internett-infrastruktur, slik som for eksempel Kina har gjort.

I lys av Snowden-avsløringene er det likevel nødvendig å vurdere hvilke grep norske myndigheter bør ta for å sikre at data om norske brukere er best mulig sikret gjennom norsk personvernlovgivning. Bør visse typer data, som for eksempel data fra helseapplikasjoner til norske brukere, pålegges lagring i Norge eller land som tilbyr tilsvarende personverngarantier?

Norge har dessuten svært gode forhold for store datasentre, med billig og grønn energi, rikelig med kalt vann og store, kjølige fjellhaller. Google har

---

[63] http://www.tu.no/it/2013/09/02/folk-vil-ha-norsk-lagring-for-a-unnga-amerikansk-overvaking
[64] ”Brazil sparks furore over internet privacy bill”, Financial Times, 11. november 2013

allerede etablert datasenter i Finland og Facebook har gjort tilsvarende i Sverige[65]. Bør myndighetene legge forholdene bedre til rette, slik at tjenesteleverandører velger å lagre sine data i Norge?

Regulering av norsk internettrafikk

En ting er hvor data lagres. En annen er hvordan man regulerer flyten av data på Internett.

Selv om norsk lov stiller visse krav til hvor personsensitive data skal lagres og overføres, er den ikke nødvendigvis tilstrekkelig tilpasset vår digitale hverdag. Mens en e-post med personopplysninger til en adressat i utlandet betraktes som overførsel til utlandet og reguleres deretter, vil samme e-post til en adressat i Norge ikke betraktes som slik overførsel, selv om e-posten er innom servere i utlandet på veien[66]. Dette gjør oss sårbare i en tid hvor mye av vår kommunikasjon rutes via utlandet.

Gjennom vår daglige bruk av digitale verktøy, produserer vi data og metadata som ofte er innom flere land. I dag rutes eksempelvis 80 prosent av internetttrafikken mellom Norge og resten av verden via Sverige[67].

Flere land vurderer derfor ulike tiltak som skal sørge for at lokal datatrafikk i størst mulig grad rutes nasjonalt eller regionalt, og ikke via uønskede land. Tanken bak slike initiativ er at for eksempel en e-post mellom to norske borgere i Oslo og Bergen ikke skal behøve å ta "omveien" om for eksempel Sverige eller USA. Ved å gripe inn i den underliggende tekniske infrastrukturen til Internett, kan man gjøre overvåking og spionasje fra andre land noe vanskeligere.

I Norge har Venstre tatt til orde for en ny internettkabel til det europeiske fastlandet[68], slik at ikke brorparten av norsk internettrafikk lenger behøver å gå via Sverige og gjøres tilgjengelig for svensk etterretning. Tyskland har bedt om en evaluering av hvorvidt europeisk internettrafikk i størst mulig grad kan holdes innenfor EU, og dermed vekk fra andre land[69].

---

[65] http://www.forskningsradet.no/prognett-bia/Nyheter/Gronn_datakraft/1253969413314?lang=no
[66] http://www.datatilsynet.no/Sektor/Overfoering/
[67] http://www.nrk.no/fordypning/her-gar-din-nett-trafikk-1.11403663
[68] http://www.venstre.no/artikkel/52409
[69] http://www.theguardian.com/world/2013/nov/01/nsa-surveillance-cause-internet-breakup-edward-snowden

Bør norske myndigheter ta sterkere grep for å kontrollere norsk internettrafikk?

Selv om slike tiltak kanskje ikke gir noen garantier mot at utenlandsk etterretningsvirksomhet oppretter lytteposter i nasjonal infrastruktur[70], kan det likevel bidra til å heve terskelen for overvåking utenfra. Samtidig vil det kunne gjøre oss mindre avhengig av infrastrukturen i for eksempel Sverige og gi oss et større diplomatisk armslag i internasjonal etterretningsvirksomhet.

Så lenge vi ønsker å kunne kalle opp en utenlandsk nettside, er overførsel av både data og metadata over infrastruktur i utlandet uungåelig. Dette vil alltid innebære en viss risiko. Kan norske myndigheter likevel gjøre noen grep som vil gjøre oss mindre sårbare? Og hvilke konsekvenser vil slike tiltak ha for Internettet slik vi kjenner det i dag?

[70] http://www.washingtonpost.com/world/europe/germany-looks-at-keeping-its-internet-e-mail-traffic-inside-its-borders/2013/10/31/981104fe-424f-11e3-a751-f032898f2dbc_story.html

2014

EU-DOMSTOLEN TAR BESLUTNING OM DLD

Det er ventet at EU-domstolen skal ta stilling til om EU-direktivet for datalagring (DLD) er ulovlig. Dette med bakgrunn i en anbefaling fra generaladvokaten i EU-domstolen om at direktivet ikke er kompatibelt med grunnleggende rettigheter.

LANSERING AV GOOGLE-BRILLENE

Google-brillene (Google Glass) kommer – sannsynligvis våren 2014. Brillene har en liten innebygd datamaskin, en mini-skjerm og videokamera. Teknoentusiaster spår at brillene vil revolusjonere hvordan vi samler inn og bruker informasjon i hverdagen, mens skeptikere frykter at brillen gjøre et uakseptabelt innhugg i privatlivet til både brukeren og de rundt.

UTPRØVING AV KJERNEJOURNAL

Testingen av Nasjonal kjernejournal vil fortsette i 2014, og er første steg i arbeidet med å få en elektronisk løsning som gir tilgang til viktige helseopplysninger og gjør akuttmedisinsk helsepersonell bedre i stand til å yte forsvarlig helsehjelp. I løpet av 2014 skal myndighetene sannsynligvis avgjøre om ordningen skal utvides og gjøres nasjonal.

PRESIDENT OBAMA SETTER GRENSER FOR NSAS OVERVÅKNINGSPROGRAM

17. januar opplyste Obama at han ønsker strengere regler for NSAs tilgang til metadata og begrensninger i overvåking av allierte ledere. Myndighetene skal ikke lenger kunne lagre slike data. Tilgangen vil fremdeles reguleres av en rettsinstans som er unntatt offentligheten, men kjennelser vil bli offentliggjort i større grad enn tidligere. Nye retningslinjer for overvåkningen av utenlandske borgere ble nevnt.

NY PERSONVERNREGULERING I EU

Personverndirektivet i EU regulerer behandling og utveksling av personopplysninger, og er gjennomført i Norge gjennom personopplysningsloven. EU-kommisjonen fremmet i januar 2012 forslag til revisjon av regelverket. Det har vært stor uenighet rundt en del av endringene og det er usikkert når det nye regelverket kan vedtas, men Europakommisjonen mener at det kan skje våren 2014.

POLITIREGISTERLOVEN

1. juli trer den nye politiregisterloven i kraft, og det blir stilt en rekke nye krav til politiets registre. Loven vil blant annet regulere behandling av trafikkdata som innhentes av politiet. I tillegg vil loven skape ensartet praksis og bedre forutsigbarhet med hensyn til vandelskontroll og utstedelse av politiattester.

NY HELSEREGISTERLOV OG PASIENTJOURNALLOV

Den nye pasientjournalloven skal regulere hvordan helseopplysningene dine skal brukes til å yte helsehjelp, mens den nye helseregisterloven omhandler bruk av helseopplysninger til andre formål, for eksempel forskning. De nye lovforslagene skal behandles av Stortinget i løpet av året.

Teknologirådet

Datatilsynet