INFORMASJONSTEKNOLOGI OG PERSONVERN

UTVIKLINGSTREKK OG FORSLAG

Gisle Hannemyr
Dato: 2022-03-22

HANNEMYR NYE MEDIER AS, STØPERIBAKKEN 10, 3912 PORSGRUNN

Innholdsfortegnelse

1. Innledning 3
2. Basisteknologier 3
3. Privatsfæren 5
4. Arbeidslivet 8
5. Datasikkerhet 10
6. Demokrati og data 11
7. Kunstig intelligens og statens voldsmonopol 12
8. Sluttord 14

1. Innledning

Personvernkommisjonen ble oppnevnt av regjeringen i 2020. Kommisjonens oppgave er å se på samfunns- og teknologiutvikling som påvirker personvernets stilling i Norge i dag. Kommisjonen drøfter i den sammenheng digitalisering som et grunnleggende samfunnstrekk som påvirker alle individer og sektorer. Forfatter av dette notatet er av kommisjonen bedt om å levere et innspill som særlig drøfter dette området, både med hensyn til informasjonsteknologi og bruk av denne som har potensiale til å svekke personvernet, og som har potensiale til å styrke personvernet.

I oppdragsbeskrivelsen nevnes særskilt følgende fem situasjoner og utviklingstrekk:

a. Digital hverdag
b. Teknologiske fundamenter for det digitale samfunnet
c. Teknologi som automatisk registrerer virkeligheten
d. Maskinlæring og stordata
e. Samfunnssikkerhet i et digitalt samfunn

Slik jeg ser det, kan det være naturlig å skille mellom basisteknologier, som er sektorovergripende og som *muliggjør* mer spesifikke anvendelser.

Det er særlig tre av de overnevnte som er slike basisteknologier. Det er: (b) det teknologiske fundamenter for det digitale samfunnet, (c) teknologi som automatisk registrerer virkeligheten, som også gjerne kan kalles «sporingsteknologier», (d) samt maskinlæring og stordata.

Jeg har valgt å dele opp det som handler om (a) digital hverdag i to avsnitt, om utfordringer innen hhv. privatsfæren og arbeidslivet.

Under det siste punktet i oppdragsbeskrivelsen: (e) samfunnssikkerhet i et digitalt samfunn, drøfter jeg situasjoner der digitaliseringen får konsekvenser for samfunnet . Dette er delt opp i tre avsnitt. Det første handler om datasikkerhet. Det andre om demokrati. Det siste drøfter bruk av kunstig intelligens i politiet og i militæret.

Jeg vil i det etterfølgende først drøfte de tre basisteknologiene samlet, og deretter ta for meg konsekvensene for individet og for samfunnet. Avslutningsvis vil jeg drøfte hvordan de omtalte teknologier kan brukes på en etisk forsvarlig måte for å styrke personvernet og en bærekraftig utvikling.

Notatet lenker til kilder i form av URLer. Disse er alle besøkt 22. mars 2022.

2. Basisteknologier

Den epoke vi nå lever i kalles gjerne for «informasjonsalderen». Grunnlaget for denne er at kapasiteten til å lagre bearbeide og transportere informasjon har utviklet seg kontinuerlig siden starten på denne epoken på siste halvdel av 1900-tallet. Det er foreløpig ingen ting som tyder på at kapasitetsveksten kommer til å stoppe opp.

Den såkalte «Moore's Law», ble i 1965 formulert av Gordon Moore, co-grunnlegger av halvlederselskapet Fairchild. Den lyder slik: Kapasiteten til en mikrobrikke (dvs. den grunnleggende byggesteinen i all informasjonsteknologi) vil fordobles hvert annet år.»

«Loven» er kun en projeksjon basert på erfaring – den er ikke en naturlov. Men i de 57 år som har passert siden 1965 har den holdt stikk.

Denne *kvantitative* kapasitetsøkningen har i sin tur ført til *kvalitative* endringer. Den har muliggjort innsamling, lagring, transport og behandling av enorme mengder informasjon, som i sin tur har ledet fram til nye forretnings- og forvaltningsmodeller, overvåknings-teknologier, økt globalisering, og allestedsnærværende databehandling (engelsk: «ubiquitous computing»).

Kapasitetsøkningen har blant annet gjort det praktisk mulig å behandle det som gjerne kalles «stordata». Dette er en samlebetegnelse som er knyttet til teknologi og analyse-metodikk for datamengder som er for store, for mangeartede og for ustrukturerte til at man kan benytte tradisjonelle teknikker innen elektronisk databehandling for å hente informasjon ut av dem.

Også teknologi som automatisk registrerer virkeligheten (sporingsteknologier) har vokst fram som en følge av den kapasitetsøkningen som er beskrevet over. Dette er teknologier som trer i stedet for menneskets sanseapparat og som automatisk registrerer en enorm mengde ulike data, og som gjennom bruk av en mengde sensorer legger grunnlaget for at de adferdsprofiler som vil bli omtalt senere, i avsnittene «Privatsfæren» og «Arbeidslivet». Slike sensorer finnes i offentligheten og i privatsfæren, f.eks. i veikryss, langs og på offentlig og privat transport, på kommunikasjonsplattformer, i mobiltelefoner, i robotstøv-sugere, i høyttalere, i nettlesere, og ikke minst i from av «smarthus-teknologi» og annen forbrukerelektronikk. Spennvidden i teknologien som brukes til dette er enorm. For eksempel: Et videokamera som gjenkjenner ansikter og analyserer sinnsstemninger, tradisjonelle kontakter i en «smart» dør-sensor, RFID (Radio-Frequency Identification) som benytter radiobølger til å spore kjøretøy og andre fysiske gjenstander, «smart dust» (nanopartikler med bitte små datamaskiner) som for eksempel samler inn og registrerer helsedata fra blodstrømmen til en person. Samtlige sensorer har imidlertid til felles at de kan overføre de data de samler inn over Internett for at de kan sammenstilles og analyseres. Sensorer som befinner seg i fysiske gjenstander og kropper, og som leverer data for stordata-analyse betegnes gjerne med begrepet «Internet of Things», eller initial-ordet «IoT».

Det som kjennetegner sporingsteknologiene, er at de frembringer enorme datamengder – både persondata og anonyme data – og legger grunnlag for at automatisk databehandling av disse. Ofte er det trivielt å gjøre om anonyme data til persondata ved å kombinere dem med andre data som er offentlig tilgjengelig. I 2015 hevdet Noah Deneau at han kunne identifisere muslimske taxi-sjåfører basert på data om 175 millioner taxi-turer ved å finne de sjåførene som var inaktive på de tidspunkter på døgnet når muslimer plikter å be[1].

Inntil ganske nylig var vi ikke i stand til å nyttiggjøre oss slike enorme datamengder, og de praktiske konsekvensene av bruk av sporingsteknologier var derfor begrenset. Dette har endret seg dramatisk siden årtusenskiftet. Det som da skjedde, var at kapasiteten til å behandle data økte til et punkt hvor maskinlæring (dvs. kunstig intelligens) basert på

[1] https://mashable.com/archive/redditor-muslim-cab-drivers

stordata ga resultater som var så gode at det ble mulig å tjene penger på den. Inntjeningen foregår blant annet ved å tilby individuell og persontilpasset reklame. Dette omtales gjerne som mikromålretting.

Det som skjer ved behandling av sporingsdata er at det benyttes statistiske metoder til å lete etter *adferdsmønstre* i de enorme mengdene personlige sporingsdata man har tilgang til. Slike adferdsmønstre brukes i sin tur til å produsere en profil av en person som kan inneholde forbrukerpreferanser, rase/etnisitet, politisk oppfatning, tro, fagforenings-medlemskap, helsetilstand og seksuell legning. En slik profil er profitabel fordi den gjør det mulig å mikromålrette reklame og andre budskap mot personen på en langt mer fokusert måte enn ved tradisjonell markedsføring og informasjonsformidling.

Sosialpsykologen Shoshana Zuboff benytter i boka «The Age of Surveillance Capitalism» (2019) begrepet *overvåkningskapitalisme* om dette fenomenet, og hevder at denne formen for kapitalisme:

> "unilaterally claims human experience as free raw material for translation into behavioural data [which] are declared as a proprietary *behavioural surplus*, fed into advanced manufacturing processes known as 'machine intelligence', and fabricated into *prediction products* that anticipate what you will do now, soon, and later."

3. Privatsfæren

Digitale tjenester og plattformer benyttes i stadig flere sammenhenger, og de aller fleste av oss lever liv sammenvevd med et utall av disse. Nettstedet W3Techs rapporterer at 65 % av alle nettsteder benytter minst ett sporingsverktøy[2]. Prosentandelen er høyere i offentlig sektor i Norge. Fra en rapport fra Teknologirådet: «Kommersiell sporing i offentlig sektor[3]» framgår det at 38 av 41 statlige og kommunale virksomheter (93 %) har sporings-verktøy på sine nettsteder.

I praksis betyr dette at dersom en besøker nettsteder, kan man ikke unngå å bli eksponert. Sporingsverktøyene er i praksis til stede overalt og det er ikke mulig å beskytte seg mot å bli sporet og profilert.

Enkelte har hevdet at det bør gis et særlig sterkt vern for persondata vi ikke har kontroll over, som for eksempel biometriske data eller data om ansiktsmimikk (sinnsavlytting, engelsk: *affective computing*). Siden det må antas at vi kan kontrollere egen adferd, er det ikke er nødvendig å gi adferdsdata et like sterkt vern. Jeg mener et slikt skille er illusorisk. Selv om det nok er mulig for en person å kontrollere enkelthandlinger, innebærer bruken av stordata og kunstig intelligens imidlertid at det vil kreve overmenneskelig disiplin dersom en person skal kunne justere sin adferd på en slik måte at det vil endre personens profil i overvåkningskapitalistenes databaser.

Stort sett flyr bruken av sporingsverktøy under radaren. Inntil nå har det meste av diskursen omkring sporing handlet om sporingskapsler («cookies»). Men dette er bare én

[2] https://w3techs.com/technologies/overview/traffic_analysis

[3] https://teknologiradet.no/publication/kommersiell-sporing-i-offentlig-sektor/

av mange slike verktøy (og et av de få som teknologikyndige faktisk i en viss grad kan beskytte seg mot). I rapporten fra W3Tech listes det opp 127 ulike sporingsverktøy, der de fleste av disse er ukjente, også for forfatteren av dette notatet.

Så langt har aktørene som utsetter sine egne kunder og besøkende for sporingsteknologi bare i begrenset grad tatt inn over seg hvor inngripende slik overvåkning er. Ifølge en NRK-reportasje sender nettsidene til 6 av 9 stortingspartier besøksdata til Facebook[4]. Mekanismen det er snakk om heter «Facebook Pixel», som har mye til felles med Googles «fingerprinting» nevnt ovenfor. Et «Pixel» er en sporingskapsel som er bakt inn en nettside, og som fungerer slik at når noen besøker nettsiden, samhandler brukerens nettleser med Facebook og overfører diverse sporingsinformasjon, *direkte* fra nettleseren til Facebook.

Høyres IT-sjef Kim Are Sveen sier til NRK: «Høyre deler ingen data med Facebook. Det er brukerne av Facebook som eventuelt velger å gjøre dette.» Utsagnet er teknisk sett korrekt, informasjonen flyter direkte fra brukerens nettleser til Facebook. Ettersom det er Høyre som tilrettelegger for sporingen ved å bake inn Facebooks sporingsteknologi i nettsidene sine, bør det diskuteres om Høyre er helt uten ansvar for at Facebook får tilgang til disse sporingsdataene knyttet til personer som besøker Høyres nettsider, eller om dette kan reguleres bedre.

Facebooks gjenytelse til de politiske partiene som lar dem benytte denne sporingsteknologien er at de kan få innsyn i adferdsprofilene til de som besøker nettstedet, og det er sannsynligvis nyttig for partiene på mange ulike måter – ikke minst for å måle effekten av utspill og kampanjer. Men ved tilrettelegge for at Facebook kan samle inn slike data muliggjør de som tilrettelegger for dette bruk av slike adferdsdata på måter de neppe kan overskue.

I den rapport fra Teknologirådet som omtales over framgår det at 13 av de offentlige nettstedene som er analysert, bruker verktøy som gjør «opptak» av hva personer som besøker nettstedet foretar seg. Det vil si at de registrerer hvilke deler av en nettside den besøkende scroller til, hva den besøkende klikker på, og hva den besøkende skriver inn i skjemaer og andre tekstfelt – også dersom den besøkende ombestemmer seg og velger ikke å lagre det det vedkommende har skrevet. Dette er en sporingsteknologi som nærmest kan sammenlignes med kommunikasjonskontroll. Kommunikasjonskontroll er noe som kun politiet har lov til å benytte, og som ikke kan settes i verk uten at det foreligger en rettslig kjennelse.

Mange selskaper som benytter sporingsteknologier, gir inntrykk av at brukerne har full kontroll over hvordan persondata samles inn og brukes ved å spørre om tillatelse. Realiteten er at dersom man ikke godkjenner sporing, så fungerer ikke nettstedet. I tillegg opererer mange nettsteder med personvernerklæringer som både er mangelfulle og uforståelige. Med mindre man har teknisk kompetanse og innsikt i de sporingsteknologiene som man eksponeres for, er det umulig å forstå hva som egentlig skjer. Mange brukere gir derfor

[4] https://nrkbeta.no/2019/07/12/nettsidene-til-6-av-9-stortingspartier-sender-dine-besoksdata-til-facebook/

tillatelse til sporing ved å klikke på «Jeg forstår» uten at de har forstått hva de har gitt tillatelse til.

Det mest populære sporingsverktøyet ifølge Teknologirådet er «Google Analytics». Det var i bruk på 36 av 41 nettsteder. «Google Analytics» bruker en lang rekke sporings-teknologier, med «fingerprinting» som en av de mest framtredende. «Fingerprinting» innebærer at man henter diverse sporingsdata fra nettleseren, og at disse sporingsdata *til sammen* er tilstrekkelig unike til at personen kan entydig identifiseres. Verktøyet gir Google svært detaljert informasjon om hvilke nettsider personen besøker, hvilke nettsider personen kom fra, og hvor lenge personen besøker nettsiden før vedkommende klikker seg videre til neste.

Flere undersøkelser viser at forbrukere foretrekker nettjenester finansiert av reklame, framfor å betale for dem. En undersøkelse av forbrukere i USA[5] oppgir for eksempel at 85 % foretrekker gratistjenester finansiert av annonser, mens en tilsvarende undersøkelse i EU[6] oppgir at 92 % ville slutte å bruke de gratistjenestene de allerede benytter dersom en betalingsvegg ble innført.

Det er ikke tvil om at mange av de *tjenestene* som leveres av selskaper som har en forretningsmodell basert på innsamling og profilering av adferdsdata er både populære og nyttige. Facebook, for eksempel, har skapt en plattform som ikke bare har demokratisert publisering, men også langt på vei løst problemet med å *synliggjøre* publisert innhold. De aller fleste bloggere sliter med å skaffe seg lesere. Dersom de i stedet skriver på Facebook, vil Facebook sørge for at de blir sett. Turlag arrangerer utflukter ved hjelp av Facebook, skoler holder foreldre oppdatert ved hjelp av Facebook, osv. For å forstå fenomenet Facebook må man også forstå at det finnes mange gode grunner til at mange oppriktig *liker* Facebook, og ikke ønsker å miste tilgang til tjenesten i hverdagen.

Samtidig har Facebook også en problematisk side. Interne dokumenter fra selskapet Meta (som eier Facebook, Instagram, WhatsApp og mange andre plattformer) ble på slutten av 2021 lekket av varsleren Frances Haugen. Disse dokumentene viser selskapet var klar over at deres algoritmer ledet tenåringer med dårlig selvbilde til innhold som fremmet spiseforstyrrelser. Dokumentene viste også at selskapet med vilje viste fram innhold som var ekstremt, polariserende eller kunne karakteriseres som hatprat, fordi slikt innhold skaper engasjement hos brukerne, og dermed også økt bruk. Ifølge Haugen er ledelsen i selskapet også klar over at dette er skadelig, men ikke villig til å gjøre det som er nødvendig for å minske skaden dersom slike endringer samtidig reduserer inntjeningen. Haugen tok i en høring for i kongressen til orde for at Meta, og andre selskaper med tilsvarende forretningsmodell burde reguleres på samme måte som for eksempel tobakksindustrien, som også satt på intern kunnskap om at produktene de tjente penger på var skadelige, men forsøke å skjule denne kunnskapen fra offentligheten.

[5] https://pauldughi.medium.com/would-you-rather-have-ads-or-pay-for-on-line-content-25af91fe0b6d

[6] https://datadrivenadvertising.eu/wp-content/uploads/2017/09/EuropeOnline_FINAL.pdf

Et dramatisk eksempel på bruk av persondata er beskrevet i en rapport[7] om spillselskapet «Sky Bet» sin bruk av adferdsprofiler. Selskapet hadde registrert 186 adferdsmønster på en av sine kunder, og brukte disse mønstre for å målrette kommunikasjonen mot ham slik at han utviklet spillavhengighet. Når han til slutt brøt med selskapet og fikk det etterforsket hadde han en gjeld på £ 80 000, og var blitt suicidal. I rapporten står det dette om selskapets bruk av adferdsprofiler:

> "Such profiles include indicators of personal vulnerabilities and addictive behaviours, which can then be used to target the most vulnerable."

I Norge har vi lange tradisjoner for å minske forbruket av skadelige produkter ved å gjøre dem dyrere for forbrukerne ved å kreve en avgift til staten som må betales av brukeren (jf. tobakk og alkohol). Et mulig nasjonalt tiltak mot disse selskapene kunne derfor å avgiftsbelegge *bruken* av dem. Avgiften kunne kreves inn av brukerens Internett-leverandør og faktureres sammen med avgiften for båndbredde.

Det er imidlertid ingen tvil om at kjernen i problemet er at denne forretningsmodellen er svært lønnsom. Et mer radikalt grep ville derfor være å *forby* denne forretningsmodellen. En sannsynlig konsekvens ville være at de attraktive «gratis» tjenestene som er blitt laget for er å høste inn persondata, vil forsvinne. På kort sikt ville det sannsynligvis føre til at de mange brukerne av disse «gratis» tjenestene ville protestere mot forbudet. Men på lengre sikt ville det gi plass til entreprenører som utvikler *nye* attraktive tjenester som erstattet de som blir borte pga. forbudet, men der forretningsmodellen er mindre skadelig (f.eks. brukerbetaling).

4. Arbeidslivet

Et resultat av digitaliseringen er den såkalte «gig-økonomien», der arbeidstakere ikke tilbys fast ansettelse, men i stedet tilbud om å registrere seg som selvstendig næringsdrivende der de mottar enkeltstående oppdrag, som regel ved hjelp av en «app» på mobiltelefonen. De siste årene har det dukket opp selskaper organisert på denne måte innenfor en rekke bransjer, fra persontransport (Uber og Lyft), hjemlevering av mat og dagligvarer (Foodora, Wolt og Instacart), renholdstjenester (Care, Weclean og Vaskehjelp.no) og internettbaserte småoppdrag innenfor oversetting, tekstbehandling, spørreundersøkelsesutfylling og design (Amazon Mechanical Turk og Upwork).

Gig-økonomien lar studenter og andre som ønsker å tjene litt penger når det høver seg, men som ikke ønsker de bindinger som en fast ansettelse innebærer, en mulighet til å skaffe seg inntekt. Den gir også en lavterskel-inngang til arbeidslivet for personer med hull i CV-en eller mangelfull utdanning. Den gjør det dessuten rimeligere å skalere virksomheten opp eller ned etter behov, sammenlignet med en virksomhet som ansetter sine medarbeidere.

---

7 https://www.thisismoney.co.uk/money/markets/article-10444901/Suicidal-gambling-addict-groomed-Sky-Bet-hooked.html

Gig-økonomien har også en lang rekke problemer, ikke minst at de som arbeider i den ekskluderes fra de sosiale rettighetene og det arbeidsrettslige vernet som følger med et fast ansettelsesforhold, uten at dette drøftes videre her, hvor fokuset er på personvern.

Sentralt i gig-økonomien er innhøsting og bearbeiding av persondata. Organiseringen av virksomheten er som regel automatisert, ved at det er datamaskiner utstyrt med kunstig intelligens som mottar, fordeler og følger opp, oppdrag. Dette gjøres primært av kostnadsgrunner, siden å benytte kunstig intelligens er raskere og rimeligere enn å betale mennesker for å gjøre dette. Datamaskiner kan dessuten optimalisere logistikken bedre enn det mennesker kan.

I en rapport fra PrivacyInternational[8] benyttes uttrykket «Algorithmic management» for å beskrive hvordan disse virksomheten styres. Det defineres slik:

> "Algorithmic management can be defined as a set of technological tools and techniques to remotely manage workforces, relying on data collection and surveillance of workers to enable automated or semi-automated decision-making."

Av rapporten framgår det at til tross for at Personvernforordningen gir den registrerte rett til innsyn i både egne personopplysninger og i behandlingen av dem, var det svært vanskelig å utøve denne rettigheten for de som var underlagt denne typen styring.

Selskapene bruker blant annet persondata de samler inn til å beregne «verdien» av en arbeider, noe som blant annet brukes til å fastsette lønn og tildele oppdrag, men de uten at virksomheten gir innsyn i dette tallet, eller opplyser om hvordan det regnes ut. Resultatet er at mange av de som arbeider i gig-økonomien, føler seg maktesløse i forhold til virksomheten. Jeg er kjent med at særlig Fellesforbundet nå utreder bredt hvordan rettighetene til gig-arbeidere kan styrkes. I en slik utredning bør også gig-arbeideres personvern gis plass.

Ifølge LO er bruken av overvåking i det tradisjonelle norske arbeidslivet også økende[9].

En avgjørelse fra Personvernnemnda (PVN-2017-18) handlet om hjemmel for bruk av GPS-data som automatisk ble registrert av bussens billetteringssystem. I samband med en konflikt omkring overtidsbetaling hadde busselskapets ledelse hentet ut disse dataene for å kontrollere om det var arbeidet overtid. Dette førte til at overtidskravet ble underkjent og sjåføren ble ilagt en advarsel. Datatilsynet mente at busselskapet ikke hadde rettslig grunnlag for å benytte av GPS-data fra bussens billetteringssystem til kontroll av overtid, og ila gebyr. Personvernnemnda kom til motsatt konklusjon, og at mente at busselskapet hadde hjemmel for bruk av sensordataene fra GPS-systemet til kontrollformål. Et mindretall av nemndas medlemmer sluttet seg imidlertid til Datatilsynets vedtak. I den samband anførte mindretallet et obiter dictum knyttet til utviklingen av sensor- og sporingsteknologier og hvordan «usynlige» sensorer på mange arbeidsplasser utplasseres *uten at* formålet med dem er å overvåke de ansatte, men som gjennom funksjonsglidning likevel blir *benyttet* til dette. og at de dermed bidrar til å svekke arbeidstageres personvern.

---

[8] https://privacyinternational.org/long-read/4709/managed-bots-surveillance-gig-economy-workers

[9] https://www.dn.no/arbeidsliv/lo-sjefen-om-xxl-varsler-vi-har-dessverre-sett-en-urovekkende-okning-av-overvakning-i-arbeidslivet-over-mange-ar/2-1-1160721

Mindretallet viste i den forbindelse til at det innenfor miljøretten er akseptert at et føre-var-prinsipp skal legges til grunn ved utøving av offentlig myndighet, og det bør vurderes som et tilsvarende prinsipp bør gjøres gjeldende for arbeidsretten når det gjelder hjemmel for å benytte personopplysninger som kan utledes fra sensor- og sporingsdata.

Føre-var-prinsippet innebærer at når menneskelig aktivitet og/eller teknologisk utvikling kan føre til moralsk uakseptabel skade som er vitenskapelig sannsynlig, men usikker, så skal forvaltningen treffe vedtak for å unngå eller minske skaden. Kontrolltiltak og overvåkning i arbeidslivet ved hjelp av sporings- og sensorteknologi kan fort komme ut av kontroll og føre til irreversible endringer i arbeidslivet som igjen vil true arbeidsmiljøet til fremtidens ansatte. Jeg ønsker å sende den ballen videre til kommisjonen, og oppfordrer til at man drøfter et slik føre-var-prinsipp i arbeidsmiljøloven.

Årsaken til den økende overvåkning i arbeidslivet er sannsynligvis at det har kommet til ny teknologi (bl.a. GPS, dørsensorer, automatiske kameraer) som gjør slik overvåkning mulig og rimelig, og at forståelsen av de uheldige konsekvensene ved å ta i bruk slik teknologi ligger etter teknologiutviklingen.

5. Datasikkerhet

Digitaliseringen fører gjennomgående til økende kompleksitet, usikkerhet og sårbarhet. Store ansamlinger av persondata kan utsettes for cyberangrep der de stjeles eller ødelegges, noen ganger med svært alvorlige konsekvenser.

Eksempler fra den siste tiden har dessverre vist at kompetansen til å sikre slike data er lavere enn den burde være, og at nødvendige (og av EUs personvernforordning pålagte) risikovurderinger – inkludert vurdering av personvernrisiko – ikke blir gjort.

Et velkjent eksempel på dette er beslutningen fra Helse Sør-Øst om å kjøpe inn eksterne tjenester til (*outsource*) drift av foretakets IT-infrastruktur. De persondata det her var snakk var lagret på datamaskiner som fysisk befant seg i Norge, men likevel valgte foretaket en teknisk løsning der IT-arbeidere i Bulgaria, India og Malaysia full tilgang til pasient-journalene til 2,8 millioner nordmenn over Internett.

Datasikkerhet er en stor utfordring, og det trengs et krafttak både for å ruste kompetansen på dette området, både hos næringsaktørene, offentlig sektor og tilsynsmyndighetene. Dette vil sannsynligvis kreve en omprioritering av ressurser.

Det har blitt mer og mer vanlig at virksomheter ikke eier sin egen IT-infrastruktur, men velger det på fagspråket kalles (IaaS – *Infrastructure as a Service*). Det innebærer at man abonnerer på den infrastrukturen virksomheten har behov fra en ekstern leverandør, for eksempel Amazon, Alphabet (Googles morselskap) eller Microsoft. Dette kalles gjerne for «skytjenester» fordi infrastrukturen det er snakk om ikke befinner seg et bestemt sted, men i det som gjerne kalles «nettskyen». Skytjenester er fleksible og skalerbare: Det å doble eller å halvere prosessor- eller lagringskapasiteten kan gjøres med noen få tastetrykk og tar bare noen minutter.

Skytjenester blir mye brukt i dag, både av private og offentlige virksomheter. Særlig Solberg-regjeringen gikk langt i å oppfordre offentlige virksomheter til å benytte seg av skytjenester.

I dag er markedet for skytjenester dominert av store kommersielle aktører, der de fleste er basert i USA. I USA hjemler «Patriot Act» at de hemmelige tjenestene kan kreve å få utlevert lagrede data på bakgrunn av en hemmelig rettsordre. Denne loven blir med rette oppfattet som svært problematisk i forhold til europeisk personvernlovgiving, siden den kan benyttes til å hente ut data om europeiske borgere dersom selskapet som lagrer dataene er underlagt amerikansk jurisdiksjon.

Til tross for dette har man i Norge *ikke* drøftet forhold knyttet til personvern, nasjonal sikkerhet og digital autonomi i de offentlige dokumentene som anbefaler bruk av kommersielle skytjenester. Datatilsynets hovedside om skytjenester[10] er fra 2018, og problematiserer ikke dette, ut over å minne om pliktene til å gjøre risikovurderinger og vurdere personvernkonsekvensene. I Tyskland later det til at man er seg mer bevisst disse problemene, og myndighetene der har valgt å etablere en statlig sky – *Die Bundescloud*[11] – slik at de offentlige virksomheter som ønsker å benytte skytjenester ikke er prisgitt kommersielle aktører underlagt amerikansk jurisdiksjon.

Avslutningsvis bør nevnes at den teknologiske utviklingen også kan komme til å gi oss teknologi som kan gi bedre vilkår for personvernet i nær framtid: Med 5G trådløse nett vil det bli rimeligere og enklere å etablere et privat, lukket og kryptert nett på et fysisk avgrenset område. Eksempler kan være sykehus, institusjoner og militære anlegg. Innenfor et slikt nett kan man så tilrettelegge for lokal databehandling. Dette betegnes gjerne som «edge computing». I et 5G-nett kan data lagres og behandles nær der brukerne sitter, i datamaskiner som er installert lokalt. «Edge computing» er det motsatte av en skytjeneste. I og med at persondata ikke vil bli eksponert for eksterne infrastruktur-leverandører underlagt andre staters lovgiving, vil både kompleksiteten og personvern-risikoen bli mindre.

6. Demokrati og data

Bruken av adferdsdata og adferdsprofiler til å mikromålrette politisk påvirkning, omtalt i avsnittet «Privatsfæren», utgjør en reell trussel mot demokratiet og fri meningsdannelse.

«Cambridge Analytica»-skandalen i USA i 2018, der en tredjepart via Facebook fikk tak i adferdsprofilene til 87 millioner Facebook-brukere, og benyttet disse til personrettet politisk markedsføring til fordel for Donald Trump, viser at slike adferdsprofiler har potensiale til å bli misbrukt. Ved at markedsføringen skjedde individuelt og ikke var en del av den offentlige politiske diskurs, kunne Cambridge Analytica «skreddersy» budskapet til den enkeltes individuelle adferdsprofil. Antirasister ble fortalt at Trump også var antirasist – rasister fikk se det motsatte budskapet.

---

[10] https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/skytjenester/

[11] https://www.itzbund.de/DE/itloesungen/egovernment/bundescloud/bundescloud.html

Den danske teologen og grundtvigianeren Hal Koch hevdet i boken «Hvad er demokrati» (1945) at den åpne, offentlige dialogen er selve kjernen i demokratiet. De persontilpassede politiske monologer som foregår i lukkede ekkokammer, og som for enkelte helt har *erstattet* den dialogen som Koch viser til og vil, slik jeg vurderer det, ødelegge demokratiet dersom de får bre om seg.

Basert på bl.a. materialet lekket av tidligere omtalte Frances Haugen, vet vi at såkalte «sosiale medier» i motsetning til redaktørstyrte medier *ikke* ser det som sin oppgave å opplyse samfunnsdebatten. I stedet ønsker de å skape engasjement og aktivitet, uavhengig av om engasjementet og aktiviteten er basert på opplyst informasjon eller desinformasjon. I de dokumenter som ble lekket av Frances Haugen framgikk det at Facebook-kanaler som «Stop the steal» og «QAnon». Slike lukkede kanaler på Facebook og andre sosiale platt-former var essensielle for å spre konspirasjonsteorien om valgsvindel i presidentvalget i 2020, og instrumentelle for mobiliseringen til den voldelige stormingen av kongressen som skjedde den 6. januar 2021.

Kilden til stordata som foredles til adferdsprofiler er primært sporingsverktøy som en rekke selskaper stiller til rådighet for ukritiske nettstedeiere som betaler for tilgangen til disse verktøyene med sine brukeres persondata, jf. avsnittet «Privatsfæren». Det er to selskap som har en så stor andel av markedet for sporingsverktøy at de i praksis utgjør et duopol. Ifølge W3Tech er dette er Alphabet, som med Google Analytics har markedsandel på 86 %, og Meta, som med Facebook Pixel har en markedsandel på 17 %. Inntjeningen i begge selskapene stammer i hovedsak fra mikromålrettet reklame. De er begge svært lønnsomme. Årsaken er at sporingsverktøyene gir dem tilgang til stordata som lar dem utvinne en astronomisk mengde adferdsprofiler som sannsynligvis omfatter hele den delen av menneskeheten som har tilgang til Internett. Dette gjør det svært vanskelig for andre kommersielle aktører som selger annonser å konkurrere med dem. Redaktørstyrte medier har forretningsmodell der inntektene dels kommer fra brukerbetaling, og dels kommer fra reklame. Selv om disse nå også har lært seg å samle inn adferdsdata for å selge mer personrettet reklame, har de et langt spinklere datagrunnlag, og kan derfor ikke produsere like presise og omfattende adferdsprofiler som Alphabet og Meta. Resultatet er at redaktørstyrte medier blir mindre konkurransedyktige, og at en stadig større del av annonsemarkedet tilflyter duopolet. Slik jeg ser det er det et demokratisk problem at redaktørstyrte medier, som ser det som sitt samfunnsoppdrag å opplyse den offentlige debatten får sin konkurransekraft svekket.

Jeg mener derfor at man bør overveie å innføre et forbud mot mikromålretting, både av reklame og av redaksjonelt innhold). Det vil både gi bedre konkurransevilkår for redaktørstyrte medier, undergrave forretningsmodeller som er tuftet på massiv innhøsting og bearbeiding av persondata, og styrke demokratiet.

7. Kunstig intelligens og statens voldsmonopol

Kunstig intelligens er i ferd med å bli tatt i bruk av de institusjoner som utøver statens voldsmonopol, dvs. politiet, rettsvesenet og militæret.

I politiet har det primært handlet om såkalt forutseende politi[12] (engelsk: *predictive policing*) der maskinlæring og ulike statistiske metoder, som regel i kombinasjon med det som generelt refereres til som «stordata», benyttes i samband med rettshåndhevelse for å identifisere sannsynlige mål for politiintervensjon. Prediktivt politiarbeid inkluderer metoder for å forutsi lokalisering av forbrytelser, metoder for å forutsi lovbryteres identitet og metoder for å forutsi offerets identitet[13].

Rettsvesenet i USA har tatt i bruk slik teknologi for å bistå dommere og juryer med å fatte avgjørelser[14]. Avgjørelsene i domstolene fattes fortsatt av mennesker, men kunstig intelligens produserer analyser som for eksempel kvantifiserer sannsynligheten for at den tiltalte er skyldig, eller (ved saker som handler om prøveløslatelse) kvantifiserer gjentagelsesrisiko, kan legges fram som en del av bevisbildet[15].

Science-fiction filmen «Minority report» fra 2002 problematiserer dette i en fiksjonalisert kontekst.

De verktøyene som benyttes i justissektoren i USA vil kun gi et resultat i form av et prosenttall. Det er ikke mulig å hente ut eller overprøve en *begrunnelse* for at tallet ble som de ble. Dette er en kjent svakhet ved bruk av stordata. Stordata benyttes når datamengden er for stor, for mangeartet og for ustrukturert til at dataene kan forstås med menneskelig forstand. Kritikere av bruk av stordata i politiarbeid og rettsvesenet har pekt på at det alltid benyttes historiske data til maskinlæring. Dersom det finnes skjevheter (engelsk: *bias*) i dette læringsmaterialet, vil slike skjevheter også prege resultatene som produseres. Med andre ord: Dersom historisk politipraksis eller rettspraksis inneholder signifikante elementer av rasisme, vil også den kunstige intelligensen produsere forslag til avgjørelser som er rasistisk motivert.

Det er primært i USA denne typen verktøy benyttes av politiet og rettsvesenet, men i NOU2016:3[16] tas det (med henvisning til et notat fra Teknologirådet[17]), til orde for å ta bruk slike verktøy i norsk politi, jf. (side 224):

> «Teknologirådet beskriver flere eksempler der slike metoder brukes allerede. For eksempel bruker politiet i flere land denne typen analyser til å styre sin tilstedeværelse i forskjellige områder til forskjellige tider, med redusert kriminalitet som resultat. Gevinsten er både bedre disponering av politiressursene og bedre kvalitet.»

---

[12] https://teknologiradet.no/wp-content/uploads/sites/105/2018/05/ForebyggendeAnalyse_endelig_WEB.pdf

[13] http://predictive-policing.roztr.com/

[14] https://www.technologyreview.com/2019/01/21/137783/algorithms-criminal-justice-ai/

[15] https://www.theatlantic.com/technology/archive/2018/01/equivant-compas-algorithm/550646/

[16] https://www.regjeringen.no/contentassets/64bcb23719654abea6bf47c56d89bad5/no/pdfs/nou201620160003000dddpdfs.pdf

[17] https://teknologiradet.no/wp-content/uploads/sites/105/2018/05/Rapport_Denne-gangen-er-det-personlig.-Det-digitale-skiftet-i-offentlig-sektor.pdf

Min vurdering er at dette er langt mer problematisk enn det Teknologirådet i dette sitatet gir uttrykk for. Fagfellevurdert forskning på slike verktøy og metoder gir ikke grunnlag for å hevde at de bidrar til målbar redusert kriminalitet. Og som påpekt av kritikere, kan bruken av historiske data til maskinlæring kan være problematisk, dersom slike data inneholder skjevheter.

Dersom analyseverktøy basert på kunstig intelligens skal benyttes til beslutningsstøtte i justissektoren, blir det samtidig viktig å kontrollere og forstå hvordan slike beslutningsstøtte-systemer blir brukt. Justisdepartementet bør sørge for at det utføres jevnlige tilsynskontroller av maskinlæringen og analysene som benyttes. Det er viktig for at man skal kunne forsikre seg om at man benytter slike verktøy riktig, opererer innenfor lovverket, og ivaretar personvernet i alle ledd. Et eksternt, uavhengig og teknisk kyndig tilsyn bør få tilgang til justissektorens analysesystemer for å vurdere hvorvidt materialet som benyttes til maskinlæring inneholder skjevheter, usikkerheter, subjektive vurderinger eller tilfeldige valg som kan bidra til å systematisere utilsiktede konsekvenser, som for eksempel diskriminering.

Forsvaret i flere land, blant annet USA, Russland, Storbritannia, Israel, Kina og Sør-Korea, utvikler autonom, dødelig våpenteknologi. Egenskapene ved slik våpenteknologi ble satt på spissen av den amerikanske general Michael Hayden, en tidligere direktør for CIA og NSA, som i 2014 på en konferanse uttalte[18]:

> "We kill people based on metadata."

Til forskjell fra de analyseverktøyene som eksisterer for justissektoren er dette ikke bare beslutningsstøttesystemer. Dette er våpen som benytter maskinlæring og kunstig intelligens til å *treffe* beslutninger om å angripe et mål, som kan være en person, et kjøretøy, eller bygning. Målet blir så utslettet med dødelig kraft.

De samme problemene som tidligere er anført for automatiserte beslutningsstøtte systemer i justissektoren kan også anføres for autonom, dødelig våpenteknologi, men fordi de er autonome (altså uten at noe menneske er involvert) er konsekvensene av feilavgjørelser langt mer dramatiske.

Meg bekjent er det ikke aktuelt for det norske forsvaret å ta i bruk slike våpensystemer, men siden minst to av våre nære allierte (USA og Storbritannia) utvikler slike systemer, bør diskusjonen omkring settes på dagsorden i den norske offentlige debatten.

8. Sluttord

Det utvikles i dag teknologier som også vil kunne styrke personvernet dersom de brukes riktig, som for eksempel offentlige skytjenester og «edge computing» (omtalt over i avsnittet om datasikkerhet).

Det som kalles «personvernøkende teknologier (PET, engelsk: *Privacy Enhancing Technologies*) er et eget fagområde innenfor informatikk der det særlig arbeides med å

[18] https://www.theguardian.com/commentisfree/2016/feb/21/death-from-above-nia-csa-skynet-algorithm-drones-pakistan

skape metoder og praksiser som fremmer «innebygd personvern[19]» og «personvern som standardinnstilling[20]». Artikkel 25 i EUs personvernforordning krever at den behandlingsansvarlige gjennomfører «egnede tekniske og organisatoriske tiltak» for å oppnå dette, og åpner i Artikkel 42 for at det etableres en nasjonal sertifisering av slike krav overholdes. Et norsk personvernsertifikat vil utvilsomt styrke personvernet i landet, men slik forordningen er utformet, er kravene for vage til at det vil være hensiktsmessig. Kommisjonen bør overveie å anbefale regjeringen å utrede hvorvidt det skal etableres et norsk personvernsertifikat, hvem som skal kunne utstede det og i så fall hva de konkrete kravene til sertifisering skal være.

Det eksisterer i dag mange produkter som konkurrerer direkte med de produktene som har innsamling og foredling av persondata som forretningsmodell.

For eksempel gir «Matomo Analytics» nettstedeiere mye av den samme informasjon om de som besøker nettstedet deres som det tidligere omtalte «Google Analytics», men uten å eksportere de persondata som samles inn til en tredjepart for bearbeiding, uten å eksponere persondata, og med en reell mulighet for besøkende til å reservere seg mot sporing og profilering.

Det finnes også nettbaserte reklamevirksomheter som ikke baserer seg på overvåkning og som likevel klarer å tilby reklame som treffer annonsørens målgruppe presist.

Men disse alternativene har i dag lite kjent og har marginale markedsandeler og inntjeninger sammenlignet med de selskapene som benytter forretningsmodeller som bruker persondata som råmateriale. Ønsker man å redusere bruken av persondata til analyse og reklame må man for det første problematisere bruken av sporingsteknologier i offentlig og privat virksomhet, og oppfordre til at virksomhetene velger sporingsfrie alternativer der slike finnes. Dessuten bør man sikre de sporingsfrie konkurrentene bedre forretningsvilkår ved at innhøsting av persondata enten reguleres langt strengere enn det gjøres i dag, eller at dette gjøres ulovlig.

Det er dessuten ikke gitt at overvåkningskapitalisme er den *eneste* måten å utnytte den digitale kapasiteten og de nye teknologiene den har ledet til.

Man kan tenke seg at beregningskapasitet, sporingsdata og kunstig intelligens benyttes til å forbedre diagnosene i helsevesenet, oppdage og spore pandemier, og frigjøre arbeidskraft ved at autonome roboter overtar farlige eller slitsomme oppgaver. Det er nok av uløste oppgaver i samfunnet til at automatisering og robotisering neppe fører til mangel på arbeidsoppgaver. Men for å finansiere disse nye arbeidsplassene bør den verdiskapning som stammer fra automatisering og robotisering beskattes på samme måte som om denne verdiskapningen hadde stammet fra menneskelig arbeid.

Selvkjørende biler på nivå fem (dvs. uten ratt og pedaler) vil antagelig være sikrere enn kjøretøy ført av mennesker. Behovet for å eie et kjøretøy vil sannsynligvis bli redusert når

[19] https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf

[20] https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/

man kan påkalle det ved behov, noe som føre til behov for færre biler og vil være godt for miljøet.

Entreprenører bør derfor stimuleres til å finne profitable måter å utnytte digitale kapasitet på, både i form av personvernøkende teknologier, og grønn teknologi til gavn for miljøet.

Dette bør bli et eget satsingsområde for regjeringen.