Cyber- og informations-sikkerhed, åbne data og etik

3 råd fra IDAs Digitaliseringsudvalg

April 2018

Indhold

Resume

Cyber- og informationssikkerhed, åbne data og etik – 3 råd fra IDAs Digitaliserings-udvalg

Nærværende anbefalinger fra IDAs Digitaliseringsudvalg har fokus på, hvordan Danmarks forbedringspotentiale indenfor cyber- og informationssikkerhed, åbne data og etik kan realiseres. Det er blevet til 3 overordnede råd, og de er som følger:

1. Gør cyber- og informationssikkerhed til et højprioriteret samfundsansvar
2. Realiser potentialet i åbne data via et ordentligt og klogt fodarbejde
3. Indse at etik er et ufravigeligt aspekt af digitaliseringen

De 3 råd henvender sig både til private virksomheder, offentlige myndigheder og landets politikere. Endvidere er de 3 råd operationaliseret i en række konkrete anbefalinger. Det er blevet til i alt 13 anbefalinger, og de fremgår af *boks 1*. De 13 anbefalinger er ikke en udtømmende liste. Udvalget har ud fra et teknisk og naturvidenskabeligt fundament udvalgt de områder, hvorpå de vurderer, at det vil skabe den største værdi og effekt at sætte ind på nuværende tidspunkt.

Boks 1: 13 konkrete anbefalinger fra IDA

Gør cyber- og informationssikkerhed til et højprioriteret samfundsansvar

1. Få fastlagt en definition af Danmarks kritiske infrastruktur
2. Lovgiv om softwareproducenternes produktkrav
3. Straf private virksomheder ved "uagtsom omgang med data"
4. Etabler en havarikommission for cyber- og informationssikkerhedshændelser
5. Styrk Datatilsynet markant – og det med tekniske kompetencer
6. Sikr uddannelse på cyber- og informationssikkerhedsområdet – og dét livslang
7. Forbedr mailsikkerheden
8. Afsøg muligheden for at udskifte CPR-numre med en bedre og mere sikker identifikation af borgere

Realiser potentialet i åbne data via et ordentligt og klogt fodarbejde

9. Etabler en klar governance for åbne data
10. Få styr på klare begrebsdefinitioner og kvalitets- og dokumentationskrav
11. Etabler et løbende evaluerings-setup
12. Udarbejd sektorielle beregninger for de økonomiske konsekvenser

Indse at etik er et ufravigeligt aspekt af digitaliseringen

13. Etabler et udvalg for Digital Etik og fokuser arbejdet med at få udboret og defineret konkrete indsatser

Det bemærkes, at anbefalingerne ikke er listet i en prioriteret rækkefølge. De er lige centrale og ofte forudsætninger for hinanden.

IDAs Digitaliseringsudvalg

Primo 2017 nedsatte IDA et Digitaliseringsudvalg. Udvalget består af 8 eksperter, som har fået til opgave at hjælpe med at formulere IDAs Digitaliseringspolitik. Det gør de i forskellige delleverancer og anbefalinger, hvoraf de i denne omgang har kastet sig over emnerne i nærværende rapport: *Cyber- og informationssikkerhed, åbne data og etik – 3 råd fra IDA.*

Udvalget har tidligere lanceret en rapport ved navn *Bedre it-projekter – 7 råd fra IDA.* Udvalget vil foruden nærværende rapport og den forrige komme med anbefalinger vedrørende ledelse i en digital tidsalder. På side 39 præsenteres udvalget og deres fremadrettede arbejde yderligere.

Kontakt
Spørgsmål til rapporten kan rettes til IDAs chefkonsulent Helena Juul Jensen. Mail: hjj@ida.dk og tlf.: 3318 4705

1. Gør cyber- og informationssikkerhed til et højprioriteret samfundsansvar

1.1 Cyber- og informationssikkerhed skal topprioriteres

Danmark er det mest digitaliserede land i EU[1], hvilket i sig selv gør os særligt sårbare, såfremt vi ikke tilsvarende er det mest it-sikre land. Og det er vi desværre ikke. Ifølge FNs Global Cybersecurity Index 2017 lander Danmark blot på en 34. plads ud af 193 lande, når det angår cyber- og informationssikkerhed[2]. Det er stærkt problematisk og meget bekymrende. Tiltroen og tilliden til digitaliseringen er i stor fare, hvis ikke vi kan give borgere/forbrugere vished for, at cyber- og informationssikkerheden i Danmark er i den absolutte top. Uden den tillid og den tiltro realiseres potentialet i teknologi og digitalisering aldrig.

IDAs Digitaliseringsudvalg anbefaler, at cyber- og informationssikkerhed, herunder viden, kompetencer, beredskab, lovgivning osv., topprioriteres fremover hos både vores folkevalgte, de offentlige myndigheder og de private virksomheder.

1.2 Udfordringer

Ingen er længere uvidende om, at cyber- og informationssikkerhedshændelser indtræffer, og at de fører til økonomiske tab, tab af omdømme, usikkerhed og meget mere. Alle ved også, at ansvaret i forhold til at håndtere disse risici ligger hos ledelserne i private virksomheder og offentlige myndigheder samt hos vores politikere. Incitamentsstrukturerne ser også ud til at være på plads i vores samfund for, at ledelsen af offentlige og private virksomheder faktisk anspores til at gøre noget effektivt i forhold til disse risici, idet aktionærerne i private virksomheder faktisk lider tab[3], og at skandale-effekten i offentlige myndigheder er frygtet og kan have store konsekvenser for ledelsen – både for den administrative og den politiske[4].

Men hvis alt dette er på plads og i orden, hvorfor ser vi så den ene ulykkelige cyber- og informationssikkerhedshændelse efter den anden? Påstanden fra IDAs Digitaliseringsudvalg er, at man generelt i det danske samfund betragter cyber- og informationssikkerhedshændelser som fænomener, man ikke kunne forudsige eller træffe gode modforanstaltninger imod; med andre ord ”som lyn fra en klar himmel”. Fænomener, der er ærgerlige og tragiske, men ikke noget som en ledelse skal fyres for ikke at have set komme. IDAs Digitaliseringsudvalg mener, at det er den opfattelse, som vi bør prøve at korrigere.

Naturkatastrofer kan ikke forudsiges, men en ansvarlig ledelse vil alligevel kunne bygge omfangsdræn, diger, lynafledere mv. for at modvirke tab i den forbindelse. På samme måde findes der gode, fagligt funderede tiltag, som ansvarlige ledere kan bringe i anvendelse for at imødegå cyber- og informationssikkerhedsproblemer.

[1] Kilde: Digital Economy and Society Index (DESI) 2017
[2] Kilde: FN-agenturet ITU (2017): “Globnal Cybersecurity Index 2017”, side 57
[3] Kilde: Fx Børsen (2017): ”Mærsk: Så meget kostede hackerangreb”, den 16. august 2017
[4] Kilde: Fx Version2 (2017): ”To ministre fyret efter svensk it-skandale”, den 27. juli 2017

Hvis en oversvømmelse rammer, spørger alle i samfundet: *"Hvorfor har man ikke bygget diger og dræn?"* Hvis en it-katastrofe rammer, skal alle i samfundet på tilsvarende vis gøres klar over, at ansvarlige ledelser havde midler til rådighed, som de svigtede at bringe i anvendelse.

Og det er pointen her: Imødegåelsen af mange typer cyber- og informationssikkerhedsproblemer befinder sig ikke længere i en mørk middelalder, hvor det er overladt til anti-virus producenter. Det er en ingeniørmæssig disciplin med metodikker og værktøjer, som man kan og skal bringe i anvendelse helt parallelt til diger og jordskælvssikring. Ellers har man som ledelse svigtet en vigtig del af sin opgave.

Konsekvenserne som følge af manglende cyber- og informationssikkerhed er store. Mærsk blev fx i sommer ramt af et omfattende hackerangreb, der ifølge Mærsk selv har kostet koncernen op mod to milliarder kroner[5]. I foråret var det Forsvarsministeriet, der var udsat for ulovlig indtrængen af hackere[6]. I denne måned kom det frem, at et tudsegammelt it-system hos DR havde blotlagt en håndfuld musikeres cpr-numre[7]. Og i juli vakte skødesløs håndtering af personfølsomme oplysninger i og et muligt læk af følsomme data fra Sverige transportministerium[8] stor politisk tumult og resulterede i, at to ministre trak sig fra deres ministerposter[9]. Ifølge Datatilsynet kunne situationen i Sverige ligeså vel have været sket i Danmark[10].

Og ovenstående er kun eksempler på konsekvenser ved manglende ordentlig cyber- og informationssikkerhed. Cyber- og informationssikkerhedshændelser sker hele tiden, og vejen for de cyberkriminelle er mere eller mindre belagt med guld. Profitten er stor, investeringen er lille og det samme er risikoen for at blive snuppet. Såfremt vi ikke tager dette emne afgørende alvorligt kan det få endnu større konsekvenser end dem, vi hidtil har set. Ifølge CSOs Cyber Security Business Report 2017 estimeres skadesomkostningerne i 2021 ved cyberkriminalitet globalt set til at være 6 billioner USD. Det er en fordobling i forhold til 2016[11]. Til sammenligning estimerer Gartner, at udgifterne til produkter og services inden for cyber- og informationssikkerhed globalt set vil stige med 7 pct. i 2017 og ramme et niveau på godt 86 milliarder USD[12].

Mere eller mindre hele den danske infrastruktur, herunder forsyning, er digital, hvilket betyder, at hvis ikke cyber- og informationssikkerheden konsekvent er på sit absolutte maksimale, kan ubundne gæster lukke Danmark på ubestemt tid, hvis de skulle have lyst til det. Dertil kommer fx også potentielle graverende konsekvenser for vores demokratiske institutioner, hvilket blandt andet det amerikanske valg med hacking af 21 staters valgsystemer

[5] Kilde: Børsen (2017): "Mærsk: Så meget kostede hackerangreb", den 16. august 2017
[6] Kilde: Finans (2017): "Rusland har hacket ansatte i det danske forsvar i 2015 og 2016", den 23. april 2017
[7] Kilde: Version2 (2017): "Musikeres cpr-numre blotlagt af tudsegammelt it-system hos DR", den 4. september 2017
[8] Note: Skandalen er dog i IDAs Digitaliseringsudvalgs vurdering ikke alene forårsaget af digitaliseringen. Digitaliseringen har dog gjort omfanget af skaden større; og det har været lettere at fejle, idet ministeriets medarbejdere ikke havde en indbygget *rygmarvsreaktion* i forhold til digitale data, hvilken de nok ville have haft, hvis der havde været tale om fysiske aktstykker.
[9] Kilde: Information (2017), "Ministerrokade skal redde den svenske regering", den 28. juli 2017
[10] Kilde: Information (2017): "Datatilsynet: It-læk i Sverige kan også have fundet sted i Danmark", den 4. august 2017
[11] Kilde: CSO (2017): "Cyber Security Business Report 2017"
[12] Kilde: Gartner (2017): "Gartner Says World Wide Information Security Spending Will Grow 7 Percent to Reach $86.4 Billion I 2017", den 16. august 2017

var udsat for[13]. Hele det danske samfund baserer sig på den digitale infrastruktur, hvorfor det er afgørende, at vi ligeledes har en cyber- og informations-sikkerhed, som rangeres som nummer 1 i verden og ikke som nummer 34. Tilsvarende er tiltroen og tilliden til digitaliseringen i fare, hvis ikke vi kan give fx borgerne/forbrugerne vished for, at cyber- og informationssikkerheden er i den absolutte top. Uden den tillid og den tiltro realiseres potentialet i teknologi og digitalisering aldrig.

I IDAs Digitaliseringsudvalg har vi ingen interesse i at pege fingre, fordi vi er som fællesskab for tekniske og naturvidenskabelige kompetencer meget bevidste om, at var denne cyber- og informationssikkerheds-nød så nem at knække, så havde man nok allerede gjort det. Af samme årsag melder vi os under fanerne og er mere end klar til at træde i arbejdstøjet på denne dagsorden. Vi ønsker ud fra et teknisk og naturvidenskabeligt udgangspunkt at komme med konkrete bud på, hvad vi kan gøre for at gøre livet mest surt og vanskeligt for de cyberkriminelle. Vi ønsker med andre ord at tage et ansvar.

1.3 Anbefalinger

I det følgende stiller IDAs Digitaliseringsudvalg med konkrete bud på, hvad vi i Danmark kan og bør gøre i forhold til at forbedre vores cyber- og informationssikkerhed. Anbefalingerne spænder vidt, og veksler i mellem det meget konkrete til det lidt mere overordnede. De skal ikke betragtes som en udtømmende liste, men som et bud på, hvad der ud fra et teknisk og naturvidenskabeligt udgangspunkt er de væsentligste områder at sætte ind overfor på nuværende tidspunkt.

1.3.1 Få fastlagt en definition af Danmarks kritiske infrastruktur

Uden en klar definition af, hvad det er, vi skal sikre os bedre imod, bliver det vanskeligt at sikre os klogt. Tilbage i 2013 blev der på finansloven for 2014 afsat 3 mio. kr. til forskere, som skulle bruge de afsatte midler på at definere Danmarks kritiske infrastruktur[14]. En rigtig god ide, idet det uden denne definition bliver svært at arbejde målrettet og systematisk mod at beskytte det danske samfund mod cyber- og informationssikkerhedshændelser. Hvis det ikke er klart, hvad vi gerne vil beskytte, kan vi heller ikke forvente, at vi kan beskytte os selv ordentligt.

Uden at vide, hvor lang tid det måtte tage 1) at bruge 3 mio. kr. og 2) definere hvad der forstås med Danmarks kritiske infrastruktur, kan følgende ikke desto mindre sluttes: En definition af Danmarks Digitale infrastruktur ikke var tilstrækkelig på plads i udgangen af 2014 til, at den kunne komme med i Danmarks Nationale Strategi for Cyber- og Informationssikkerhed, som udkom i december 2014[15]. Derfor fik vi en strategi uden klar ide om, hvad det egentlig er, vi gerne vil sikre os strategisk imod.

Der pågår på nuværende tidspunkt et tværministerielt arbejde med at udarbejde en ny national strategi for cyber- og informationssikkerhed, som skal gælde fra 2018-2020[16]. IDAs Digitaliseringsudvalg kan kun på det kraftigste opfordre til, at de forskellige interessenter i arbejdet bruger grundige kræfter på at lægge sig fast på en definition af Danmarks kritiske

[13] Kilde: Information (2017): "USA: Russiske hackere angreb 21 stater op til valget", den 21. juni 2017.
[14] Kilde: Version2 (2013): "Forskning for 3 millioner kroner skal definere Danmarks "kritiske infrastruktur", den 3. december 2013
[15] Kilde: "National strategi for cyber- og informationssikkerhed", december 2014. Via www.fmn.dk
[16] Kilde: Finansministeriet (2017): "Regeringen styrker indsatsen mod cybertrusler", den 26. august 2017 via www.fm.dk

infrastruktur, inden de kaster sig over de konkrete strategiske indsatser. IDA bidrager meget gerne i kvalificerende drøftelser heraf. Udvalget har i den forbindelse desuden følgende bud på, hvad Danmarks kritiske infrastruktur bør indeholde:

1. Teknisk infrastruktur, herunder vand, varme, transport, tele mv. Det har *direkte* konsekvenser for vores samfund, hvis denne infrastruktur udsættes for cyberkriminalitet. Ansvaret herfor er delt imellem regeringen/de offentlige institutioner samt de respektive forsyningsvirksomheder.
2. Offentlige data, herunder påvirkning af valg samt sløring/ændring af information brugt i det offentlige. Ansvaret for denne infrastruktur er regeringens/de offentlige institutioners.
3. Virksomhedsdata. Danmarks konkurrenceevnen svækkes ved fx industrispionage. Ansvaret for denne infrastruktur er virksomhedernes, men de bør støttes af offentligt finansieret rådgivning og offentlige kontrolinstanser.
4. Borgernes data, herunder fx læk af data brugt i forskning, hvis ikke der er anonymiseret ordentligt. Disse vurderes ligeledes at være de offentlige institutioners ansvar, idet borgerne har ikke de nødvendige kompetencer/viden nok til at beskytte sig selv, hvis systemet er svagt.

****
IDAs Digitaliseringsudvalg anbefaler, at man på nationalt niveau får fastlagt, hvad der for Danmark defineres som kritisk infrastruktur, og herunder får udarbejdet en handlingsplan for at nå det nødvendige niveau for sikkerhed
****

1.3.2 Lovgiv om softwareproducenternes produktansvar

Med EU's Databeskyttelsesforordning er der kommet fokus på ansvar og sågar på bøder til private virksomheder og offentlige myndigheder[17], hvis ikke de lever op til deres ansvar over for den enkelte borgers rettigheder i forhold til persondata. Ligeledes stilles der med Databeskyttelsesforordningen krav til privacy by design/privacy by default[18]. Begge dele betragter IDAs Digitaliseringsudvalg som glædelige skridt i den rigtige retning i forhold til at sikre borgerne samt understøtte den fortsatte tillid til digitaliseringen.

Udvalget vurderer dog, at tiden i forlængelse af ovenstående er inde til at slå et slag for den næste naturlige udvikling: *Softwareproducenters produktansvar*. Hvis en producent af fødevarer, biler, byggematerialer etc. sjusker således, at brugernes liv bringes i fare, forventer vi, at disse producenter stilles til ansvar, tilbagekalder produkter, udbedrer problemet og betaler erstatninger. Hvorfor accepterer vi, at det tilsvarende ikke gælder for softwareproducenter? Produktansvaret gælder naturligvis ikke kun borgernes liv, men også deres privatliv, adgang til hemmelige og retfærdige valg uden fusk og påvirkning fra hackere mv., samt firmaernes ret til at kunne køre en stabil forretning uden driftstop og kompromittering af forretningshemmeligheder.

[17] Note: I Justitsministeriets høring over udkast til forslag til databeskyttelsesloven side 20 fra juni 2017 fremgår det, at en afklaring om, hvorvidt offentlige myndigheder også skal straffes med bøder, fortsat udestår. Den 25. oktober 2017 blev databeskyttelsesloven fremsat i Folketinget, og her lagde regeringen op til, at offentlige myndigheder kan sanktioneres med bødestraf på til 4 pct. af en myndigheds driftsbevilling – dog med et loft på 16 mio. kroner. Se Børsen (2017) "Regeringen vil straffe offentligt sjusk med bøder op til 16 mio. kr.", den 25. oktober 2017.

[18] Kilde: EU's Databeskyttelsesforordning, artikel 25.

Der var engang, hvor meget af det software, vi brugte i samfundet, faktisk var omfattet af forskellige former for producentansvar; typisk fordi det var resultatet af store kontrakter[19], der rummede en masse forpligtelser for leverandørerne. Tænk fx bare tilbage på et ERP-system[20] eller et system til den offentlige administration.

Men meget af det software, som vi betjener os af i dag, er udviklet med kort time-to-market, SCRUM og med stay-in-beta og det er måske endda indlejret i produkter, som igen indgår i samlede løsninger på en uklar måde. Tænk som eksempel på et moderne gasfyr, hvor der er en lang og uigennemsigtig leverandørkæde ned til det stykke indlejrede software fra en asiatisk leverandør, som kører i en af de adskillige mikroprocessorer i apparatet, og som måske en dag indeholder en stump kode, der får huset til at eksplodere. Der burde kunne stilles krav om, at firmware i visse kritiske apparater skulle kunne opdateres, selvom det vil øge prisen på dette apparat en smule.

****

IDAs Digitaliseringsudvalg anbefaler, at der etableres lovgivning om produktansvar på dette område.

****

IDAs Digitaliseringsudvalg mener i forlængelse heraf, at man bør afsøge mulighederne for at kunne indføre/lovgive i forhold til en form for "entreprenør-ansvar", hvor leverandører tager mere eller mindre **hele** ansvaret for det samlede system/produkt. Med andre ord bliver det derfra leverandørens ansvar internt at gå videre og kæmpe mod sine underleverandører, og herunder sikre sig at de forskellige kodestumper, som underleverandørerne leverer, ikke har eller får utilsigtede konsekvenser. Skulle det ske, at de enkelte stykker embedded software ikke er af ordentlig kvalitet, er det hovedleverandørens ansvar over for kunden.

I forhold til ovenstående gør IDAs Digitaliseringsudvalg dog opmærksom på, at kan være hensigtsmæssigt at skelne mellem standardsystemer og specialudviklede systemer, herunder integrationer. For standardsystemer kan og bør vi stille krav til producenterne, idet det udelukkende bør betragtes som deres ansvar, hvad der bringes på markedet.

Men for specialudviklede systemer er det kunden, der stiller kravene (gode såvel som dårlige krav) og i øvrigt også kunden, der står for en stor del af afprøvningen. I sådanne tilfælde kan det ikke nødvendigvis være rimeligt at give producenten det fulde ansvar. Herunder henset til, at vi jo netop gerne skulle bevæge os væk fra, at virksomhedernes og myndighedernes ledelser tror, at de ikke er ansvarlige for it-projekterne og deres resultater.

[19] Note: I de store kontrakter, som nævnes på forrige side, er der ikke i dag et producentansvar, når først kunden har gennemført overtagelsesprøve og godkendt systemet. Producentansvar vil typisk være at finde i en **vedligeholdelseskontrakt**, hvor leverandøren mod betaling udbedrer de fejl, der eventuelt måtte vise sig senere.

[20] Note: Et ERP-system (Enterprise Ressource Planning) er et system, som integrerer alle virksomhedens forretningskritiske data og giver mulighed for at lave datamining og andet.

IDAs Digitaliseringsudvalg bemærker endvidere, at der ikke alene bør være tale om lovkrav til nye produkter og systemer. Mange cyber- og informationssikkerhedsangreb rammer eksisterende systemer/driftsinstallationer, hvorfor mulighederne for at stille krav til blandt andet opgradering af eksisterende driftssystemer ligeledes bør afsøges.

1.3.3 Straf private virksomheder ved "uagtsom omgang med data"

IDAs Digitaliseringsudvalg kunne uden problemer hurtigt stille med adskillige eksempler på personlige oplevelser med private virksomheder, der beder borgere, kunder, mv. om at sende et scan af pas, sundhedskort, årsopgørelser eller lignende til fx bank, fagforening, biludlejningsfirma via en ganske almindelig ukrypteret mail[21]. Dette er særdeles uhensigtsmæssigt, hvorfor udvalget vil slå et slag for, at private virksomheder bør kunne straffes for at tilskynde til "uagtsom omgang med data".

Det kan og bør ikke (kun) være den enkelte kundes ansvar, idet denne ofte vil være i en svag(ere) position i forhold til modparten/den private virksomhed. Kunder bør garanteres sikre løsninger (fx krypteret mail eller NemID-beskyttet upload), og de bør ligeledes kunne blive vejledt til brug af selvsamme sikre løsninger[22].

Ifølge Datatilsynet bør *"brug og håndtering af personoplysninger foregå betryggende og med et passende niveau af sikkerhed og privatlivsbeskyttelse"*, men opfordring til at oplyse private oplysninger i en ukrypteret mail betragtes af IDAs Digitaliseringsudvalg ikke som værende i overensstemmelse med ovenstående, idet der ingen sikkerhed eller privatlivsbeskyttelse er.

I den fortsat gældende persondatalovs §41, stk. 3 står der blandt andet, at den dataansvarlige (altså ikke kunden eller borgeren) skal træffe de nødvendige foranstaltninger mod, at oplysninger kommer til uvedkommendes kendskab. Der er altså allerede i loven lagt op til, at data skal beskyttes. Men manglende viden eller manglende incitament hos virksomheder og kunder fører ofte til, at dette ikke overholdes[23].

I dag er det kunden og ikke virksomheden, der løber en risiko, hvis personlige data lækkes. Samtidig er kunden som nævnt ovenfor ofte den svage part i forhold til virksomheden, hvilket kan gøre det vanskeligt at sige fra. Det er i praksis straffrit (på nuværende tidspunkt) for virksomhederne at spare på sikkerheden på kundernes bekostning.

****
IDAs Digitaliseringsudvalg anbefaler, at der etableres en straf for private virksomheder, hvis de tilskynder til "uagtsom omgang med data".
****

1.3.4 Etabler en havarikommission for cyber- og informationssikkerhedshændelser

[21] Eksempel: https://www.version2.dk/artikel/feriekontos-kundeservice-opfordrer-at-tage-billeder-noeglekort-1079628

[22] Bemærkning: IDAs Digitaliseringsudvalg bemærker, at dette synspunkt læner sig op af Privacy by design, som er en del af EU's Dataskyttelsesforordning, men det er endnu ikke lov, hvorfor det er forventningen fra udvalget, at der formentlig vil være store muligheder for fortolkning i den kommende lov. Af samme årsag slår IDA et eksplicit slag herfor i nærværende anbefaling.

[23] Note: se fx Bruce Schneier for flere betragtninger herom https://www.schneier.com/blog/archives/2016/03/data_is_a_toxic.html

I forbindelse med diverse it-projekt-skandaler har der fra tid til anden været røster, der har advokeret for etableringen af en it-havarikommission. Argumentet er langt overvejende, at vi jo kan se, at det virker inden for blandt andet flysikkerhed, så hvorfor gør man ikke noget tilsvarende inden for it? IDAs Digitaliseringsudvalg kan godt se potentialet heri, men det forudsætter, at scope for en sådan kommission er det rigtige.

IDAs Digitaliseringsudvalg mener, at der bør etableres en havarikommission, som beskæftiger sig med cyber- og informationssikkerhedshændelser. Og ikke en kommission, der beskæftiger sig med it-projekter, der allerede er gået galt. I forhold til sidstnævnte er det væsentligt, at it-projekter ikke kan eller bør sidestilles med fx fly. Udvalget bemærker, at der er forskel på it-projekter og fly og flyulykker. Fly er et stykke teknologi, imens it-projekter (og herunder særligt offentlige it-projekter) i stor udstrækning er politik. Der kan være alle mulige gode og ikke gode forklaringer på, hvorfor it-projekter går galt – herunder såvel teknologiske årsager såvel som uhensigtsmæssigheder i processen. Af samme årsag kan vi ikke bare mere eller mindre 1:1 kopiere konceptet fra fx en fly-havarikommission over til it-projekter.

Betyder ovenstående, at vi ikke skal lære af fortidens fejl og erfaringer. Nej, slet ikke. Men det betyder, at en større analyse af it-projekter, som allerede er gået galt, og som fx blev besluttet og initieret for efterhånden mange år siden, kan være uhensigtsmæssig i forhold til effekt og læring. It-toget buldrer derud af, og derfor kan en god beslutning truffet på et tidspunkt i et it-projekt af x, y, z hensyn, senere i projektet være dårlig, fordi udviklingen inden for it og digitalisering har overhalet beslutningerne indenom.

****
IDAs Digitaliseringsudvalg anbefaler, at der etableres en havarikommission for cyber- og informationssikkerhedshændelser
****

Derfor mener IDAs Digitaliseringsudvalg, at vi skal fokusere på at etablere en havarikommission, som skal have fokus på cyber- og informationssikkerhedshændelser. Med fokus på cyber- og informationssikkerhedshændelser kan vi lave pendanten til fx fly-havarikommissionen eller til den maritime havarikommission. Formålet, i lighed med de to nævnte og allerede eksisterende havarikommissioner er, at man ved hver hændelse analyserer og på den baggrund tilretter/justerer regler og procedurer derefter.

IDAs Digitaliseringsudvalg er særligt inspireret af det arbejde, som Center for Cybersikkerhed har lavet i forbindelse med, at en aktør via forskellige former for cyberangreb har forsøgt at tiltvinge sig adgang til postkasser og maskiner under Forsvarets myndighedsområde og Udenrigsministeriet[24]. Se i øvrigt *boks 2* nedenfor, som er opsummeringen fra Center for Cybersikkerheds rapport. Udvalget mener, at havarikommissionen i forbindelse med cyber- og informationssikkerhedshændelser netop bør udføre denne slags arbejde, idet der er en enorm læring for både den enkelte udsatte organisation/virksomhed og for

[24] Kilde: Center for Cybersikkerhed (2017): "Undersøgelsesrapport – én aktør, mange angreb".

andre (endnu ikke udsatte) organisationer/virksomheder. Dertil kommer, at et sådant analysearbejde generere en gennemsigtighed, som er afgørende væsentlig for den videre tillid til digitaliseringen af Danmark.

Boks 2: Eksempel på hvordan en rapport fra en cyber- og informationssikkerhedshændelseshavarikommission kunne se ud

Opsummering fra Undersøgelsesrapporten "Én aktør, mange angreb" fra Center for Cybersikkerhed. April 2017

Denne rapport beskriver, hvordan en måttet, vedholdende og ressourcestærk udenlandsk aktør har spioneret mod Danmark. Rapporten gennemgår, hvordan aktøren via forskellige former for cyberangreb har forsøgt at tiltvinge sig adgang til postkasser og maskiner under Forsvarets myndighedsområde og i Udenrigsministeriet. Center for Cybersikkerhed (CFCS) har fundet tegn på, at aktøren har haft adgang til en række email-postkasser fra en ikke-klassificeret mail-service i Forsvaret og kopieret deres indhold. Der er ***ikke*** set tegn på, at maskiner eller data hos Udenrigsministeriet er blevet kompromitteret.

I 2015 og 2016 har CFCS observeret flere forsøg på at franarre email-longinoplysninger, dvs. brugernavn og kodeord, fra medarbejdere under Forsvarsministeriets myndighedsområde ved hjælp af vellignende kopier af mail-servicens loginside (webmail.mil.dk). Målpersonerne er blevet forsøgt lokket til at indtaste deres loginoplysninger på de falske sider. Det er meget sandsynligt, at flere mil.dk-postkasser efterfølgende er blevet kompromitteret, og at postkassernes indhold er kommet i aktørens hænder over flere omgange i 2015 og 2016.

CFCS har afdækket to sideløbende bølger af phishing-emails med ondsindende links rettet mod Forsvarsministeriets myndighedsområde og Udenrigsministeriet. CFCS vurderer, at hensigten har været at få adgang til og kontrol over modtagernes maskiner. Bølgerne har ramt i 2015 og involverer et større antal phishing-mails. Der er ikke tegn på, at aktøren har fået adgang til nogen maskiner som følge af phishing-angrebene.

CFCS vurderer dertil, at samme aktør har forsøgt at tiltvinge sig til adgang til mil.dk-postkasser og servere i Forsvaret via forceringsangreb i 2015 og 2016. Der er ikke tegn på, at forceringsforsøgene er lykkedes

Endelig har CFCS set rekognosceringsaktivitet mod mailsystemer hos forskellige danske myndigheder, inklusiv under Forsvarsministeriets myndighedsområde. Aktiviteten er tegn på, at aktøren har en interesse for de rekognoscerede systemerm og der er derfor en øget risiko for, at de kan blive mål for cyberangreb.

CFCS vurderer, at det er meget sandsynligt, at aktøren har APT28 (alias Fancy Bear, Sofacy, Pawn Storm, mfl.) har franarret loginoplysninger til det internetvendte mailsystem mil.dk fra medarbejdere i Forsvaret. CFCS vurderer det sandsynligt, at samme aktør står bag de øvrige beskrevne hændelser. CFCS vurderer videre, at der er tale om en vedvarende trussel mod Forsvarsministeriets myndighedsområde og Udenrigsministeriet.

Rapporten indeholder forslag til tiltag, der med udgangspunkt i erfaringerne fra hændelserne kan hjælpe myndigheder og virksomheder til at modvirke lignende angreb.

Ved etableringen af en havarikommission for cyber- og informationssikkerhedshændelser er det helt centralt, at tilrettelæggelsen heraf sker hensigtsmæssigt og velovervejet. IDAs Digitaliseringsudvalg mener blandt andet i den forbindelse, at kommissionen skal sikres tværfaglighed i sin kompetencesammensætning, herunder repræsentanter fra offentlig og privat sektor, fra forskningsverdenen og fra brancheorganisationer som fx Rådet for Digital Sikkerhed og/eller it-branchens sikkerhedsorganisationer så som Center for Cybersikkerhed og Datatilsynet.

Udvalget mener, at der bør være meldepligt for offentlige myndigheder og private virksomheder i forbindelse med en cyber- og informationssikkerhedshændelse til kommissionen. Forpligtelse til at melde it-sikkerhedshændelser ind til kommissionen er med til at signalere

cyber- og informationssikkerhedens væsentlighed. Denne meldepligt skal dog ikke forveksles med tvungen offentliggørelse. Udvalget mener fx ikke, at det nødvendigvis kommer andre/offentligheden ved, at x-firma har fået stjålet sine øvrige ikke-personfølsomme data (fx patenter, investeringsplaner, økonomiinformationer). I forbindelse hermed kunne man nærmere arbejde med en frivillig ordning, hvor virksomheder kan få adgang til kommissionens (fortrolige) råd og vejledning uden at blive hængt ud i pressen. Af samme årsag skal det hensigtsmæssige niveau for forpligtet meldepligt afklares. IDAs Digitaliseringsudvalg har blandt andet stærke holdninger til, at såfremt en cyber- og informationssikkerhedshændelse vedrører personfølsomme oplysninger, bør der være både meldepligt og tvungen offentliggørelse.

Endelig er det væsentligt at få afklaret, hvilket mandat samt hvilken organisering og forankring en havarikommission for cyber- og informationssikkerhedshændelser skal have. Udvalget mener, at det er væsentligt at skele til de to allerede nævnte havarikommissioner, Havarikommissionen og Den Maritime Havarikommission. Førstnævnte er forankret under Transport-, Bygnings og Boligministeriets Departement, imens sidstnævnte er en selvstændig enhed under Erhvervs- og Vækstministeriet.

IDAs Digitaliseringsudvalg anbefaler, at havarikommissionen for cyber- og informationssikkerhedshændelser etableres som selvstændig og uafhængig enhed med et klart mandat. Hensigtsmæssigheden af, hvor enheden organisatorisk skal placeres, skal imidlertid afklares. Et bud kunne være at organisere den i tilknytning til allerede eksisterende enheder; fx Center for Cybersikkerhed eller Datatilsynet. I forhold til sidstnævnte kunne argumentet dels være, at meldepligt til Datatilsynet ved sikkerhedshændelser relateret til personfølsomme oplysninger bliver lov i forbindelse med ikrafttrædelsen af Databeskyttelsesforordningen den 25. maj 2018. Og dels at Datatilsynet som følge af Databeskyttelsesforordningen får endnu flere opgaver tilføjet tilsynets opgaveportefølje (*jf. desuden 1.3.5 Styrk Datatilsynet markant – og det med tekniske kompetencer*). Et andet bud kunne være at placere enheden under Ministeriet for Offentlig Innovation, idet dette ministerium dels sidder som penneførerpå den kommende Nationale Strategi for Cyberkriminalitet og dels er ansvarlig for og har erfaring med tværoffentligt samarbejde (med særlig reference til arbejdet med og implementeringen af de fællesoffentlige digitaliseringsstrategier). Uanset organisatorisk placering er det afgørende element, at kommissionen ikke skal være en underordnet enhed med vagt mandat. Enheden skal have muskler, gennemslagskraft og uafhængighed, og det er helt centralt, at kommissionen kan sætte og holde sin egen dagsorden samt sine egne prioriteter.

1.3.5 Styrk Datatilsynet markant – og det med tekniske kompetencer

IDA identificerer med hhv. EU's databeskyttelsesforordning, som får virkning den 25. maj 2018, samt regeringens lovforslag til en databeskyttelseslov, at Datatilsynet pålægges adskillige nye opgaver. Alene databeskyttelsesforordningen oplister 22 forskellige opgaver[25] og dertil kommer tilsyneladende tillægsopgaver i regeringens lovforslag til en databeskyttelseslov[26]. Det er helt centralt for beskyttelsen af personoplysninger i Danmark og Europa, at Datatilsynet kan løfte de opgaver, som det pålægges i loven.

[25] Kilde. EU's Databeskyttelsesforordning, artikel 57.
[26] Kilde: Justitsministeriet (2017): "Udkast til forslag til databeskyttelsesloven" via www.høringsportalen.dk

Med regeringens finanslov for 2018 vil regeringen øge Datatilsynets budget med godt 50 pct. i forhold til 2017[27], men i IDA mener vi, at det langt fra er nok. Dels betyder EU's databeskyttelsesforordning flere og nogle helt nye konkrete opgaver. Dels har Datatilsynet en absolut afgørende rolle i forhold til at sikre, at danskerne fortsat har tillid til, at vi digitaliserer på en sikker såvel som på en effektiv måde.

Datatilsynet har udtalt, at de finder "noget" stort set hver gang, de laver et tilsyn[28] Sidste år (2016) havde tilsynet dog kun tid og mandskab til 51 tilsyn på et år[29]. Og de har desuden et for svagt mandat til at tvinge især offentlige instanser til at rette ind[30].

Vi har i Danmark valgt at tvangsdigitalisere, og det har på mange måder været en kæmpe løftestang for det digitale Danmark. Og vi har på nuværende tidspunkt både en kommende omfattende databeskyttelsesforordning samt en digitalisering, som "buldrer" derudaf, herunder øget omfang af data og øget anvendelse af data. Ingen af delene er nogen nyhed – ej heller noget, som man skal tage letsindigt på. Ikke desto mindre kan IDA konkludere, at Datatilsynet ikke er fulgt med denne udvikling, idet antallet af årsværk i Datatilsynet er faldet siden 2011 og har de sidste 4-5 ligget stabilt (lavt), jf. tabel 1.

Tabel 1. Antallet af årsværk i Datatilsynet (2011-2017)

År	Årsværk	Indeks 2011 = 100
2017	33,4	92
2016	32,3	88
2015	33,4	92
2014	33,7	92
2013	33,8	93
2012	31,6	87
2011	36,5	100

Kilde: Moderniseringsstyrelsens forhandlingsdatabase.
Note: 2011 er indeks 100.

Det, mener vi, er stærkt problematisk. Det er ikke at digitalisere ordentligt, klogt og sikkert. Til sammenligning kan nævnes, at i følge en opgørelse fra Politiken har fx Irland øget antallet af ansatte i tilsynsmyndigheden fra 30 til 100 siden 2014[31].

****

IDAs Digitaliseringsudvalg anbefaler, at Datatilsynet som følge af EU's databeskyttelsesforordning og databeskyttelsesloven styrkes (med minimum en fordobling af tilsynets egne medarbejdere) samt at tilsynets ressourcer løbende evalueres og oprustes i takt med, at digitaliseringen kun bliver mere og mere omsiggribende (for både offentlige og private).

IDAs Digitaliseringsudvalg anbefaler, at Datatilsynet oprustes med tekniske kompetencer, idet disse i dag er underrepræsenteret i tilsynets nuværende kompetencesammensætning.

[27] Kilde: Regeringen (2017): "Aftale om Finansloven for 2018" via www.fm.dk
[28] Kilde: Datatilsynet (2017): "Tilsynet med statslige myndigheder afslører brud på persondataloven" via www.datatilsynet.dk
[29] Kilde: Computerworld (2017): "Datatilsynet gennemførte blot 51 tilsyn i 2016 – laveste antal i 15 år", den 8. juni 2017
[30] Kilde: Version2 (2017). "Datatilsyn: Vi bliver sat skakmat, når myndigheder ignorerer vores kritik", den 9. august 2017
[31] Kilde: Politiken (2017): "Historisk lov om at beskytte dine data gennemføres af svagt tilsyn", den 12. juni 2017

****

Vi er i IDA klar over, at det har en pris at minimum fordoble Datatilsynet og løbende at evaluere og opruste tilsynet i takt med digitaliseringens udvikling. Men prisen i tabt tillid til digitaliseringen, prisen for at få eksponeret sine følsomme personoplysninger for uvedkommende og prisen for ineffektive virksomheder og myndigheder, der bruger masser af mandetimer på at løse de samme udfordringer, fordi de ikke kan få gode råd fra tilsynet, er langt større. Såfremt databeskyttelsesforordningen og databeskyttelsesloven skal implementeres og håndhæves ordentligt i Danmark, er et stærkt Datatilsyn et ufravigeligt krav.

Erhvervslivet, offentlige myndigheder og borgere har brug for et Datatilsyn, som ikke kun er tilsyn, men som også i høj grad kan informere konkret om reglernes anvendelse, når der er brug for det. Tilsynet skal have ressourcer til at udføre sine opgaver efter databeskyttelsesforordningen og databeskyttelsesloven på en måde, som er tilpasset det moderne samfunds forventninger. Blandt andet gennem besvarelse af konkrete spørgsmål både fra virksomheder, myndigheder og borgere, anvende moderne kommunikationsfaciliteter og mere generelt være tilstede i den offentlige debat.

Der spildes i dag enorme ressourcer på at vurdere de samme problemstillinger i forskellige organisationer. Det vil medvirke til betydelig effektivisering til gavn for dansk økonomi, hvis Datatilsynet får ressourcer til at vejlede virksomheder, institutioner m.v.

1.3.6 Sikr uddannelse på cyber- og informationssikkerhedsområdet – og dét livslang

At danskerne er meget aktive på nettet er afgørende vigtigt for, at vi som nation kan holde os fremme i feltet i forhold til den digitale udvikling. Derfor er det også grundlæggende nødvendigt, at vi ved, hvordan vi skal agere for at kunne være trygge og sikre.

Det er desværre stadig vanskeligere at undgå at få computere og netværk i hjemmet inficeret af virus, malware, ransomware eller lignende. Politiet råder til, at man ikke åbner mails fra ukendte afsendere og ukendte vedhæftninger. Derudover er det en god ide at opdatere programpakker og netværk med de seneste versioner. IDA udarbejdede i foråret 2017 en analyse ved navn *Privacy og Datasikkerhed*[32]. Et repræsentativt udsnit af danskerne deltog, og de blev i den forbindelse stillet otte spørgsmål omkring, hvilke sikkerhedsforanstaltninger de tager for at beskytte sig imod cyber- og informationssikkerhedshændelser privat. Svarene fremgår af *tabel 2.*

Tabel 2: Hvor ofte gør du følgende?

	Aldrig	Sjældent	Af og til	Ofte	Altid	Ved ikke/ kender ikke	I alt
Klikker på links uden at vide hvor det linker til?	37 %	41 %	16 %	2 %	1 %	2 %	100 %
Åbner ukendte vedhæftede filer?	73 %	18 %	5 %	1 %	1 %	2 %	100 %
Opdaterer dine antivirusprogrammer på dine computere og andre enheder til nyeste version?	5 %	7 %	16 %	23 %	45 %	4 %	100 %

[32] Kilde: IDA Analyse (2017): "Privacy og Datasikkerhed"

Opdaterer din browser på dine computere og andre enheder til nyeste version?	3 %	7 %	18 %	25 %	41 %	6 %	100 %
Opdaterer dit styresystem på dine computere og andre enheder til nyeste version?	4 %	9 %	18 %	23 %	38 %	8 %	100 %
Bruger åbne netværk på fx cafeer, museer, offentlig transport eller andre lignende steder?	29 %	33 %	24 %	9 %	2 %	3 %	100 %
Bruger USB-nøgler til flere computere	33 %	29 %	22 %	8 %	2 %	5 %	100 %

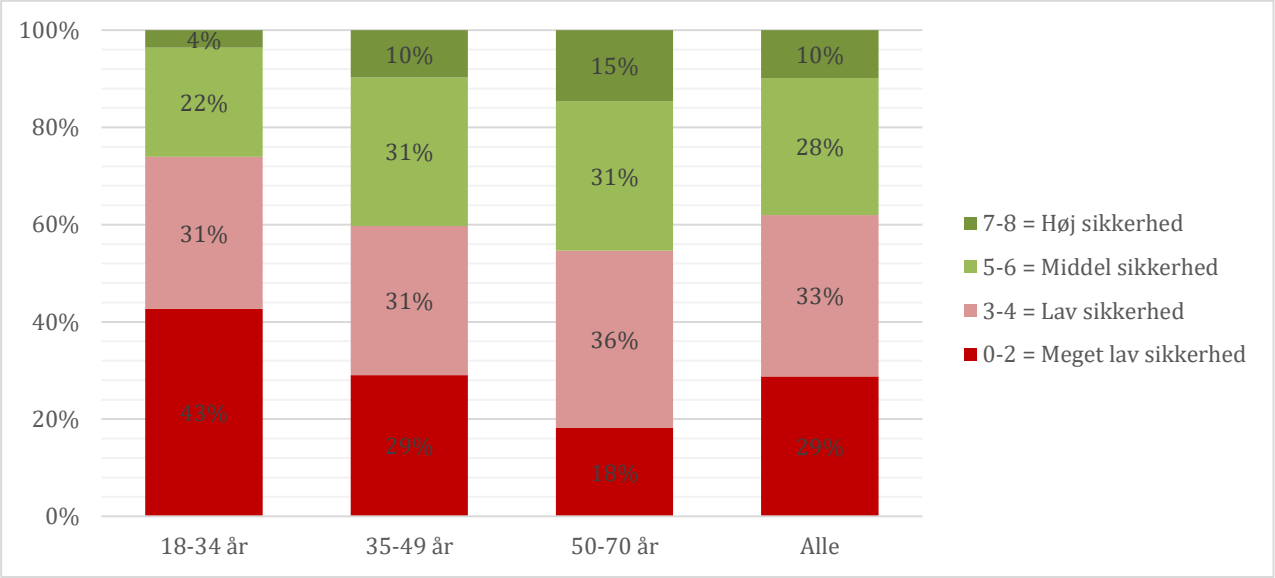
Kilde: IDA Analyse (2017): Privacy og Datasikkerhed

For at få en samlet vurdering af befolkningens sikkerhedsniveau blev det repræsentative udsnit af danskerne i analysen indplaceret på en sikkerhedsskala efter hvor mange af de otte sikkerhedsforanstaltninger, de følger. Højt sikkerhedsniveau er 8, mens lavest omvendt er 0, hvis man ikke opfylder nogen af de almindelige sikkerhedsanbefalinger overhovedet. De otte sikkerhedsanbefalinger:

1. Klik aldrig på links uden at vide, hvor det linker til
2. Åbn aldrig ukendte vedhæftede filer
3. Opdater altid antivirusprogrammer på computere og andre enheder til nyeste version
4. Opdater altid browser på computere og andre enheder til nyeste version
5. Opdater altid dit styresystem på computere og andre enheder til nyeste version
6. Brug aldrig åbne netværk på fx cafeer, museer, offentlig transport eller andre lignende steder
7. Brug aldrig USB-nøgler til flere computere
8. Brug altid kryptering af hjemmenetværk

Som det fremgår af *figur 1* har kun 10 pct. af befolkningen mellem 18-70 år et højt sikkerhedsniveau, når det kommer til beskyttelse af computer og netværk mod indtrængen udefra. Yderligere 28 pct. opfylder 5-6 af de otte anbefalinger, hvilket kan betegnes som et middel sikkerhedsniveau. I den anden ende af skalaen er der 29 pct., som kun opfylder 0-2 af anbefalingerne. Således er der, når det kommer til de grundlæggende sikkerhedsanbefalinger, god grund til at styrke danskernes viden om god it-sikkerhedsadfærd.

Figur 1: Sikkerhedsniveau for beskyttelse af computere og netværk



Kilde: IDA Analyse (2017): Privacy og Datasikkerhed

Når sikkerheden er lav øges risikoen for at blive inficeret og i værste fald miste værdifulde data, dokumenter eller billeder. Alligevel viser IDAs analyse, at der stadig er 14 pct., som lever med risikoen og ikke tager backup af vigtige filer og billeder. En anden trussel fra hackere er, at man risikerer, at fremmede overtager magten over computerens kamera, så andre kan følge med i, hvad der foregår i det rum, hvor computeren står. IDAs analyse viser, at det blot er 17 pct., som er så bekymrede over den trussel, at de dækker kameraet til med et klistermærke eller lignende, så eventuelle hackere ikke kan følge med i, hvad de foretager sig. Det svarer til, at 22 pct. af dem, der har en computer med kamera, har sat et klistermærke over kameraet[33].

Vi er alle forbrugere af it og dermed også af cyber- og informationssikkerhed. Og man skulle tro, at *digital natives* havde styr på teknologien, men det forholder sig desværre nærmest omvendt proportionalt med alderen og it-færdighederne, mener IDAs Digitaliseringsudvalg. Der er med andre ord en væsentlig forskel på at kunne begå sig digitalt og på at vide, hvad man laver og kende de tilhørende konsekvenser. Se *boks 3* for beskrivelse af den omvendte proportionalitet.

[33] Kilde: IDA Analyse (2017): "Privacy og datasikkerhed"

Boks 3: Det omvendt proportionale forhold mellem alder og it-færdigheder

Udtalelse fra Martin Bech, Head of operation and development for the Danish Research Network og medlem af IDAs Digitaliseringsudvalg. September 2017

"Min gamle mor (født før krigen) er uhyre påpasselig med sin it-anvendelse. Herunder med hvilke sites hun besøger, hvilke data hun afleverer, hvilke mails hun åbner, hvad hun giver samtykke til osv. Og det i en sådan grad, at det må siges at hæmme hendes udbytte af teknologien. På den anden side er der nok ikke den store fare for, at hun havner i et it-sikkerhedsproblem.

I den anden ende af skalaen er der mine børn, som har fuldt udbytte af alle de nye muligheder, men som tilsvarende lader SoMe-giganterne eje deres privatliv i en grad, som jeg ikke tror, de har styr på de fremtidige konsekvenser af. De er også jævnligt ude for, at deres computere og profiler bliver overtaget af fremmede kræfter i en sådan grad, at deres digitale platforme skal nedlægges og startes forfra."

En analyse[34] fra DANSK IT og DataEthics viser dog, at den yngre generation ikke er fuldstændig ligeglade med deres privatliv på nettet. Analysen viser, at de yngre generationer er villige til at skulle betale for bedre datasikkerhed og også mere villige end de ældre generationer. Således er 66 pct. af de 18-29 årige indstillet på, at hvis der fandtes en mærkningsordning, der viste, hvor datasikkert et produkt er, ville de i høj eller nogen grad at betale mere for øget datasikkerhed. Til sammenligning er blot 45 pct. af de 40-49-årige indstillet på at gøre det samme. Blot 2 pct. af de unge vil slet ikke betale mere for øget datasikkerhed, mens det samme gælder for 10 pct. af alle danskere.

Analysen viser dog også, at flertallet af danskerne har vanskeligt ved at gennemskue, hvordan virksomheder håndterer deres persondata. 75 pct. føler, at de "slet ikke" eller i "mindre grad" er i stand til at vurdere, om de persondata, en virksomhed indsamler fx via fx smart tv, mobiltelefon eller andet produkt, videregives til andre mod ens ønske. Dette understøtter pointen i *boks 3* om, at *"(de, red.) tilsvarende lader SoMe-giganterne eje deres privatliv i en grad, som jeg ikke tror, de har styr på de fremtidige konsekvenser af*".

Man kan sige, at begge parter, som skildres i *boks 3,* har brug for et højere uddannelsesniveau med hensyn til cyber- og informationssikkerhed. Det har mellemgruppen bestemt også, *jf. analysen fra DANSK IT og DataEthics*. Men grupperne har ikke brug for uddannelse på de samme punkter. IDAs Digitaliseringsudvalg mener, at vi som samfund bør og må tage denne opgave alvorligt.

Og det er desværre ikke alene borgerne, som mangler information og uddannelse. Virksomheder har ligeledes et væsentligt udviklingspotentiale. Således kunne som sagt IDAs Digitaliseringsudvalg samstemmigt finde adskillige eksempler på personlige oplevelser med virksomheder, der beder borgere, kunder, mv. om at sende et scan af pas, sundhedskort, årsopgørelser eller lignende til fx bank, fagforening, biludlejningsfirma via en ganske almindelig ukrypteret mail. Og vurderingen fra IDAs Digitaliseringsudvalg er, at ikke mange borgere/kunder tør (eller ved, at de bør) sige fra. *Jf. desuden afsnit 1.3.3 Straf "uagtsom omgang" med data.*

****

[34] Kilde: DANSK IT og DataEthics (2017): "Unge betaler gerne for bedre datasikkerhed", den 5. oktober 2017 via www.dit.dk

IDAs Digitaliseringsudvalg anbefaler, at uddannelse på cyber- og informationssikkerhedsområdet – og dét livslang – sikres.
****

Digitaliseringsudvalget er bevidst om, at der snart ikke er nogen ende på, hvad den danske folkeskole skal løse af samfundsudfordringer. Ikke desto mindre mener IDAs Digitaliseringsudvalg, at cyber- og informationssikkerhed er så centralt for den fortsatte tillid til digitaliseringen af Danmark og realiseringen af teknologiens potentiale, at cyber- og informationssikkerhed burde være en del af folkeskolens og det øvrige uddannelsessystems opgaveportefølje. Vores børn og unge pålægges at anvende og kommunikere via digitale enheder i børnehave, folkeskole, gymnasier og på de videregående uddannelser, og det kan vi altså ikke byde dem, hvis ikke vi også som samfund er indstillet på tage ansvar for, at de bliver tilstrækkeligt rustet til at begå sig ordentligt og sikkert digitalt. Med tvangsdigitaliseringen i Danmark *er* det en samfundsopgave og ikke en opgave, som vi alene kan overlade til familien og civilsamfundet.

Udvalget bemærker, at det selvfølgelig er glædeligt, at regeringen i finansloven for 2018 vil afsætte 100 mio. kr. over 4 år til en Strategi for Cyber- og Informationssikkerhed[35]. Det er IDAs anbefaling til regeringen, at disse 100 mio. kr. går til at forbedre cyber- og informationssikkerheden i praksis. Det vil sige, at der på både borger- samt ledelses- og medarbejderniveau i både offentlig og privat sektor sættes ind med mere viden og forbedrede kompetencer. Det er nødvendigt, at fx medarbejdere på alle niveauer skærper opmærksomheden og ved, hvad de skal gøre og ikke gøre. IDA advokerer således for, at der er tale om behov for både et kompetenceløft og på mange områder også for kulturændring. Det vil derfor være nødvendigt, at en stor del af de 100 mio. kr. øremærkes til at forbedre kompetencer og viden både i den offentlige og i den private sektor, jf. Digitaliseringsstyrelsen og Center for Cybersikkerhed i *"Cyberforsvar, der virker"* fra januar 2017.

1.3.7 Forbedr mailsikkerheden

På den tekniske front har vi med digitaliseringens udvikling gjort meget i forhold til firewalls, *intrusion detection*-systemer[36], adgangskontrol, segmentering og meget andet. IDAs Digitaliseringsudvalg vurderer dog, at tiden er kommet til at vende tilbage til begyndelsen: **e-mails**. E-mails er fortsat en af de væsentligste kilder til import af orme, vira, CEO-fraud etc. og etc.

IDAs Digitaliseringsudvalg vurderer, at udbredelsen af DMARC-teknologien[37] ser ud til at være et lovende skridt i den rigtige retning. Denne teknologi sikrer autencitet mellem mailservere. Det er vigtigt. Men den ultimative sikkerhed og sporbarhed kunne opnås, hvis krypteret og signeret mail kunne vinde større udbredelse.

[35] Kilde: Regeringen (2017): "Aftale om Finansloven for 2018" via fm.dk
[36] Note: Et intrusion detection system er et system, der beskytter din computer mod uønskede, ofte ondsindede, vira, bugs, orme og programmer, der kan være ødelæggende og som i nogle tilfælde anvendes til identitetstyveri alt afhængigt af med hvilket formål, computeren anvendes.
[37] Note: Domain-based Message Authentication, Reporting & Conformance bygger videre på SPF og DKIM og er en protokol, der fortæller modtagerens mailserver, hvordan den skal håndtere en mail, som ikke består en test af SPF eller DKIM. Instruktionerne ligger i DNS-opslaget for domænet, og domæneejeren kan vælge mellem tre politikker for håndtering af mails, der dumper testen. Mails kan enten modtages, men afsenderdomænets mailadministrator får en notifikation om, hvad der er gået galt, eller mailen kan sættes i karantæne eller den kan helt afvises. Kilde: www.dmarc.org

Et vigtigt skridt i den rigtige retning ville derfor være, at man supplerede e-boks (og dermed også Digital Post) med en mulighed for at modtage e-boks-dokumenterne som mail – selvfølgelig krypteret og signeret. Det ville være bedre for de modtagere, der allerede kan håndtere dette, og det ville give flere incitament til prøve kræfter med denne teknologi. Et mere vidtgående skridt kunne være, at der kom et lovkrav om, at det offentlige via Digital Post skal kunne sende og modtage krypterede og signerede mails. Hvis sikret mail bliver standarden i stedet for en sjælden undtagelse, vil det kunne blive enklere for brugerne at foretage de rigtige valg i deres mailboks.

****

IDAs Digitaliseringsudvalg anbefaler, at sikret (krypteret og signeret) mail bliver standarden frem for undtagelsen – og at muligheden for at stille lovkrav til de offentlige myndigheder herom afsøges.

****

1.3.8 Afsøg muligheden for at udskifte CPR-numre med en bedre og sikrere identifikation af borgere

Talrige datalæk har allerede punkteret den illusion, at CPR-numre er hemmelige. Det er et problem af flere årsager. For det første betyder det, at man ikke kan anvende kendskab til et CPR-nummer som sikker identifikation af en person. For det andet indeholder CPR-nummeret i sig selv personfølsomme data, såsom fødselsdato og køn.

I tiden, der er gået siden indførelsen af CPR-nummeret i 1960'erne, er det blevet almen viden blandt it-professionelle, at en identifikator ("nøgle") ikke bør indeholde nogen form for semantik. Hvem har ikke oplevet, at en leverandør ikke kunne finde en i kundekartoteket, fordi leverandøren anvender telefonnummeret som kundenummer, og at man er flyttet eller har opgivet fastnettelefonen?

Korte nøgler med semantisk indhold var praktisk, dengang bytene var dyre, og man skulle kunne huske nummeret og nedskrive det manuelt, men i en digitaliseret verden findes der alternativer. I dag bruger man ofte UUID'er[38] som nøgler i databaser, fx "b690329c-8f42-4381-b025-cbe687c53b0b"[39]. De kan synes upraktiske i daglig brug, men det er der råd for, mener IDAs Digitaliseringsudvalg.

Et yderligere problem ved CPR-nummeret er dets udbredelse. Enhver organisation eller virksomhed, som vil abonnere på adresseændringer, indberette til SKAT (herunder fx fradrag for gaver), udbetale penge via NemKonto, sende mail til borgerens e-boks og meget andet, har behov for at kende en borgers CPR-nummer. Da alle organisationer og virksomheder anvender samme nøgle til borgeren, bliver nøglen meget eksponeret for datalæk. Desuden muliggøres sammenstilling af data mellem organisationer.

Nogle af de organisationer og virksomheder, der i dag har behov for kendskab for borgerens CPR-nummer, var muligvis gerne dette kendskab foruden. Det medfører nemlig

[38] Note: UUID = Universally unique identifier
[39] Note: Genereret med www.guidgenerator.com/online-guid-generator.aspx

større krav til deres sikkerhed, blandt andet med henblik på overholdelse af databeskyttelsesforordningen. I mange tilfælde er der ikke behov for at registrere de personfølsomme data, som CPR-nummeret i sig selv indeholder.

IDAs Digitaliseringsudvalg mener, at en fremtidig løsning kunne være:

Hver borger tildeles en central borgerID i form af en UUID, som kun kendes af den centrale myndighed, der skal forvalte ordningen. Lad os kalde den BorgerID-forvaltningen, *jf. figur 2* for illustration. Skulle det forhåbentlig helt usandsynlige ske, at der sker læk herfra, kan BorgerID-forvaltningen vælge at generere nye UUID'er til erstatning for de lækkede.

Borgeren kan tilbydes en mere brugervenlig nøgle, som BorgerID-forvaltningen knytter til den centrale BorgerID. Det er kun borgeren, der skal kende og anvende denne brugervendte nøgle. Det kunne fx være det nuværende CPR-nummer. Borgeren skal også anvende denne brugervendte nøgle i forhold til sin NemID-løsning.

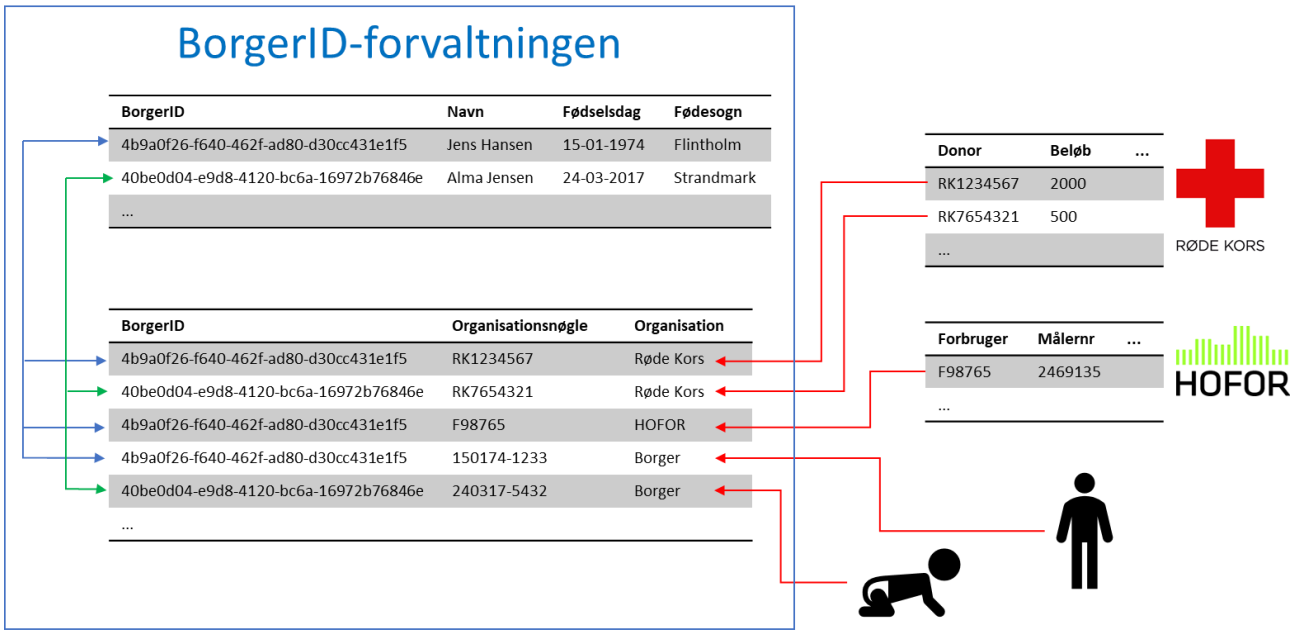
En borger kan – via en central komponent, som kan integreres på samme måde som NemID-komponenten i andre organisationers it-systemer – give tilladelse til, at en organisation får lov til at oprette en mapning mellem denne organisations personidentifikation (fx kundenummer) og borgerens borgerID. Denne mapning "bor" hos BorgerID-forvaltningen, og borgerens borgerID kommer derfor ikke til organisationens kendskab.

Borgeren kan på ethvert tidspunkt bestemme, at mapningen for en given organisation skal bortfalde, ligesom borgeren via databeskyttelsesforordningen har ret til at trække andre samtykker tilbage.

Organisationer og virksomheder, der skal indberette til SKAT, udbetale via NemKonto, sende sikker digital post mv. skal kunne anvende tjenester, stillet til rådighed af BorgerID-forvaltningen til omsætning mellem to organisationers personidentifikationer. Hvis HOFOR har en personidentifikation, og NemKonto en anden identifikation af samme borger, skal en central tjeneste hos BorgerID-forvaltningen kunne oversætte mellem de to organisationers personidentifikationer.

Denne centrale oversættelsestjeneste forudsætter nødvendige rettigheder og foretager logning af brugen. Misbrug kan derfor både forebygges og spores. Sammenstilling af data til forskningsbrug kan ligeledes ske via mapninger til den centrale borgerID, men uden at udlevere denne eller de oplysninger, som kan sammenknytte en given person med den pågældende borgerID.

Figur 2: Illustration over BorgerID-forvaltningen



****

IDAs Digitaliseringsudvalg anbefaler, at CPR-nummeret, som vi kender det i dag, udskiftes med en bedre og sikrere identifikation af borgere – eksempelvis med den her foreslåede løsning.

****

IDAs Digitaliseringsudvalg anerkender, at ovenstående løsning vil være en kolossal forandring, og herunder have store økonomiske omkostninger og konsekvenser for den eksisterende måde, man arbejder på i de offentlige myndigheder. IDA anbefaler det ikke desto mindre med åbne øjne for de netop nævnte implikationer, idet uhensigtsmæssighederne ved det eksisterende setup overgår økonomi samt den forandring, som en implementering heraf vil have på eksisterende arbejdsgange.

IDAs Digitaliseringsudvalg anerkender endvidere, at ovenstående bud på et alternativ til CPR-nummeret, kan have lange udsigter. Udvalget mener således, at man bør initiere ovenstående arbejde, og samtidig hermed lave forbedringstiltag i forhold til den nuværende situation.

IDAs Digitaliseringsudvalg mener, at man mere eller mindre her og nu bør forbyde anvendelsen af CPR-nummer som identifikation, idet nummeret jo ikke er hemmeligt længere. I praksis skal dette ske ved at vende bevisbyrden om, sådan at såfremt en forretning vil sende en regning/oprette en aftale med en kunde, er der **forretningens** ansvar at kunne bevise, at det er den rette kunde/borger – og CPR-nummer og adresse vil ikke være tilstrækkeligt. Dette vil være i modsætning til i dag, hvor ofre for identitetstyveri bliver nødt til at bruge hundreder af timer på at håndtere falske regninger osv. Denne her-og-nu-løsning vil ligeledes gøre identitetstyveri vanskeligere, hvis ID-kravet hæves fra ”at kunne sige et CPR-nummer eller at vise et fundet sygesikringsbevis” til fx ”billedlegitimation eller godkend aftale med brug af Nem-ID login”.

IDAs Digitaliseringsudvalg bemærker desuden, at udbudsmaterialet vedrørende den kommende NemID-løsning (MitID) ikke umiddelbart indeholder aspekter vedrørende nytænkning af den eksisterende cpr-løsning. CPR-nummeret nævnes i hvert fald ikke udbudsmaterialet[40]. IDAs Digitaliseringsudvalg opfordrer til, at det kommende arbejde med MitID benytter sig af muligheden for også at beskæftige sig med CPR-løsningen.

[40] Kilde: Digitaliseringsstyrelsen (2017): "MitID sent i udbud", den 20. december 2017 via www.digst.dk og Udbudsmaterialet via TED-databasen http://ted.europa.eu

2. Realiser potentialet i åbne data via et ordentligt og klogt fodarbejde

2.1 Udnyt og realiser potentialet i at lade de ikke-personhenførbare data flyde frit

Der virker til at være mere eller mindre bred konsensus om, at flere åbne data både nationalt og internationalt har et kæmpe potentiale for både det private, det offentlige og for borgerne/forbrugerne[41]. Tilsvarende vurderes der at være enighed om, at etableringen af frie datastrømme ikke just er den nemmeste opgave i verden at udføre[42], blandt andet fordi ikke-personlige data hurtigt kan blive personlige, hvis man blot har tilstrækkeligt mange af de ikke-personlige data til sin rådighed.

IDA betragter det som vigtigt, at der er mulighed for, at data kan flyde frit og sikkert i både Danmark og i mellem EU-landene. IDA gør opmærksom på, at det i denne forbindelse er afgørende nødvendigt, at der skelnes mellem personfølsomme og ikke-personhenførbare data. Ikke-personhenførbare data kan med fordel udveksles frit og effektivt for at skabe bedst mulige rammer for fx innovation, miljøovervågning og forskning, hvorfor IDAs Digitaliseringsudvalg mener, at der bør være en langt større tilgængelig til disse data. Og det gælder både offentligt og privat indsamlede data. Private virksomheder ligger inde med store mængder data, som ikke udnyttes og dermed ikke skaber den samfundsmæssige værdi, der kunne opnås, hvis data var tilgængelige. Det er vigtigt at arbejde for, at disse data bliver tilgængelige, ikke mindst for forskningsverdenen. Frit flow af personfølsomme oplysninger er omvendt afhængig af, at data anonymiseres og sikres tilstrækkeligt. I den forbindelse er det for udvalget en grundpræmis, at personfølsomme data er borgernes egne og at det således er borgerne, der ejer disse data.

2.2 Udfordringer

Der har igennem de seneste år været et stigende fokus på at gøre offentlige data tilgængelige for erhvervslivet, offentlige myndigheder og andre aktører. Myndigheder i stat, kommuner og regioner indsamler og producerer stadigt større mængder data, når de løser deres opgaver. De offentlige data i Danmark er internationalt set af høj kvalitet og rummer et stort erhvervsmæssigt produktivitets- og vækstpotentiale. Virksomheder kan bruge offentlige data til at optimere deres forretningsprocesser og til at udvikle nye produkter og tjenester, der skaber værdi for borgere, offentlige myndigheder og andre virksomheder.

Med Virk Data, Miljøportalen, Open Data DK, Grunddataprogrammet og den kommunale serviceplatform er store mængder offentlige data blevet gjort tilgængelige for andre end

[41] Kilde: Fx EU Kommissionen (2017): "EU Kommissionens forslag til en forordning om frie datastrømme", Monitor Deloitte (2017): "Analyse af efterspørgsel og markedstendenser indenfor offentlige data", Erhvervsstyrelsen (2017): " "Analyse af efterspørgsel og markedstendenser indenfor offentlige data (bemærkning til Monitor Deloittes analyse)" via https://data.virk.dk, McKinsey Global Institute (2013): "Open data unlocking innovation and performance with liquid information", Open Data DK.

[42] Kilde: EU Kommissionen (2017): "Free flow of non-personal data", Monitor Deloitte (2017): "Analyse af efterspørgsel og markedstendenser indenfor offentlige data", Den estiske regering (2017): "Estonian Vision Paper on the Frre Movement of Data – the Fifth Freedom of the European Union".

blot den enkelte myndighed selv. Det er positivt, men når det er sagt, så vurderes der fortsat at være mange offentlige data med potentiel kommerciel værdi, som ikke er tilgængelige for dansk erhvervsliv[43].

Og spørger man EU-Kommissionen er det ikke kun de offentlige instanser, som ligger inde med data, som kunne have kommerciel værdi for andre. Mange private virksomheder indsamler ligeledes data, som kunne generere vækst i helt andre brancher og sektorer, hvis de blev givet fri[44]. På visse områder er man allerede i gang med at lovgive sig til flere åbne data. Fx med et EU-direktiv, som træder i kraft ved årsskiftet 2017/2018, tvinges de danske banker til at åbne deres API og gøre data tilgængelig for andre virksomheder[45]. Dette ventes især at blive en fordel for fintech-iværksættere[46].

En forudsætning for, at det overhovedet giver mening at tale om at realisere et potentiale ved flere åbne data, er, at man som forbruger af selvsamme data kan være sikker på betydningen af data og kan stole på deres kvalitet. Se desuden *boks 4* for eksempel.

Åbne data bør være veldokumenterede, blandt andet med hensyn til data- og begrebsdefinitioner, datastruktur, syntaks, aktualitet, opdateringsstatus, nøjagtighed, dækningsgrad, dataproducent og eventuelle betingelser for brug, så forbrugerne kan vurdere, om data er velegnede til den påtænkte anvendelse.

Der findes eksempler på, at forskellige myndigheder registrerer stort set samme data blot på lidt forskellige måder. Eksempelvis klassificerer GeoDanmark vejnettet med et sæt vejkoder, mens vejmyndighederne anvender en lidt anden klassifikation. Dels er det unødvendigt dobbeltarbejde at klassificere flere gange, dels bliver det svært for forbrugerne af åbne data at finde rundt. IDAs Digitaliseringsudvalg opfordrer til, at man styrker tværsektoriel standardisering og genbrug af data.

Boks 4: Vigtigheden af at kunne stole på data

Uddrag fra interview med Finn Jordal, specialkonsulent i Styrelsen for Dataforsyning og Effektivisering, i Version2s artikel "Et succesfuldt offentligt it-projekt: Udvikler-engagement har været afgørende". 8. februar 2017

Ude fra set skulle man tro, at en adresse er en adresse. Men sådan er det langt fra. Eksempelvis kan H.C. Andersens Boulevard i København skrives på mange forskellige måder med forskellig placering af punktummer og mellemrum. Det er noget rod i en it-verden, fordi det skaber dubletter og behov for manuel sortering og datavask

Det gælder f.eks. hos webshops, hvor gentagelse af samme adresse i it-systemer skaber uorden i kundedatabaserne. Men fejlbehæftede adresser kan også have mere alvorlige følger: »Det kan have fatale konsekvenser, hvis en ambulance ikke kommer frem til det rette sted som følge af en misvisende adresseoplysninger,« fortæller Finn Jordal.

[43] Kilde: Erhvervsstyrelsen (2017): " "Analyse af efterspørgsel og markedstendenser indenfor offentlige data (bemærkning til Monitor Deloittes analyse)" via https://data.virk.dk
[44] Kilde: EU Kommissionen (2017): "EU Kommissionens forslag til en forordning om frie datastrømme"
[45] Kilde: EU Direktiv: "Payment service (PSD 2)" via www.ec.europa.eu
[46] Kilde: Computerworld (2017): "Nye regler tvinger bankerne til at åbne for API'er: It-firmaer kan få direkte adgang til dine bankdata", den 20. marts 2017.

Dertil kommer, at man som forbruger af de åbne data skal sikres, at man kan tilgå og få de *relevante* data og ikke kun data, som nogen synes, at man skal have lov til at se. I den forbindelse bliver en hensigtsmæssig governance helt afgørende for det endnu uudnyttede potentiale.

Endvidere skal data tilgængeligggøres på en sådan måde, at forbrugerne af de åbne data rent faktisk kan tilgå dem. EU har med INSPIRE direktivet forsøgt at tage hånd om denne udfordring ved at sætte forskellige krav til tilgængeligheden, herunder kræve at INSPIRE-data skal tilgængeliggøres i et bestemt format[47]. Noget har dog ikke virket efter hensigten, idet det ifølge IDAs Digitaliseringsudvalg er begrænset, hvor stor en efterspørgsel og anvendelse der har været af disse data. Ikke desto mindre mener udvalget dog, at tankerne i forbindelse med EU's INSPIRE direktiv er rigtige. Igen bliver det afgørende at have en klar governance, som dels har mandat til at stille krav til tilgængeliggørelsen af de åbne data og dels monitorerer udbud og efterspørgsel, sådan at forbrugerne af de åbne data rent faktisk får de data, som de kan realisere et potentiale ovenpå.

IDAs Digitaliseringsudvalg mener, at et sådant potentiale kunne realiseres ved at sammenstille data fra flere dataproducenter om det samme objekt for at tilgodese nye anvendelser. Forudsætningen er imidlertid, at de respektive dataproducenter identificerer objektet på samme måde, eller at der kan bygges bro mellem forskellige måder at identificere det samme objekt på.

Vejstrækninger er et eksempel på objekter, det er vanskeligt at sammenstille data for. Vejmyndighederne anvender et administrativt referencesystem bestående af vejnumre, vejdele og kilometrering / stationering (kan fx ses på kantpæle langs statsvejene). Adressemyndighederne anvender vejkoder, gadenavne og husnumre. GeoDanmark registrerer vejmidter med egne identifikationer. Vejdirektoratets anlægsområde anvender stationeringslinjer med tilhørende stationeringer. Vejdirektoratets trafikområde anvender indtil flere segmentmodeller. Adskillige GPS-leverandører har deres egne digitale vejnet, og det har Google Maps og Open Street Map også. Ingen af de nævnte referencesystemer er i øvrigt stabile over tid.

Der kan være gode grunde til, at man ønsker at opdele vejnettet i objekter på forskellige måder i forhold til forskellige anvendelser. Men det forhindrer, at man kan udveksle data med hinanden.

For nogle år siden besluttede Vejdirektoratet, det daværende Geodatastyrelsen (nu SDFE) og KL at etablere en landsdækkende, national vejreferencedatabase[48]. Tanken er, at der skal eksistere et – og kun et – sæt autoritative, stabile, nationale vejreferencelinjer, og at alle, der anvender egne referencesystemer, selv skal sørge for at etablere en mapning til de autoritative vejreferencer. Således vil data kunne udveksles og sammenstilles på trods af forskellige dataproducenters måder at opdele vejnettet på i objekter.

[47] Kilde: EU-direktiv: "INSPIRE Direktiv" via inspire.ec.europe.eu
[48] Kilde: Vejdirektoratet (2013): "Vejreference modellen – en national standard for stedfæstelse af vejdata" via www.vejdirektoratet.dk

Status på projektet er, at det centrale system til etablering og vedligehold af de nationale vejreferencelinjer er etableret i regi af SDFE, samt at Vejdirektoratet netop er gået i gang med at etablere en kobling mellem administrative referencer for statsvejene og de nationale vejreferencelinjer. Det vides ikke, hvornår øvrige interessenter følger efter.

Et projekt som dette er vanskeligt af mange grunde. Dels er det teknisk kompliceret, og dels er det vanskeligt at opstille en business case, som peger på en umiddelbar økonomisk gevinst. Der er tale om etablering af digital infrastruktur, som på den lange bane vil give nye muligheder og være værdiskabende. Men gevinsten høstes ikke nødvendigvis hos dem, der skal afholde omkostningerne. IDAs Digitaliseringsudvalg bemærker derfor, at det kræver et politisk commitment og fravær af suboptimering, hvis det skal lykkes at gennemføre sådanne projekter.

Det er en ***grundlæggende udfordring***, vurderer IDAs Digitaliseringsudvalg, at der er en antagelse om, at hvis vi bare lægger data ud, så kommer væksten mere eller mindre af sig selv. I udvalgets optik mangler vi på mange fronter at få fundamentet på plads. Herunder at få defineret forretningspotentialet, business casen og en fælles referencemodel på både et nationalt og et internationalt niveau. Myndighederne og virksomhederne kan bruge rigtig mange penge på at lægge data ud, men hvis udbuddet ikke rammer efterspørgslen, eller hvis ingen kan tilgå data, fordi formatet ikke kan anvendes af halvdelen af interessenterne, er vi lige vidt.

2.3 Anbefalinger

I det følgende stiller IDAs Digitaliseringsudvalg med konkrete bud på, hvad vi i Danmark kan og bør gøre i forhold til at forbedre tilgængeligheden og anvendelsen af åbne data. I lighed med anbefalingerne vedrørende cyber- og informationssikkerhed spænder nærværende anbefalinger vidt, og veksler i mellem det meget konkrete til det lidt mere overordnede. Anbefalingerne skal ikke betragtes som en udtømmende liste, men som et bud på, hvad der ud fra et teknisk og naturvidenskabeligt udgangspunkt er de væsentligste at sætte ind overfor på nuværende tidspunkt.

2.3.1 Etabler en klar governance for åbne data

I forbindelse med Den Fællesoffentlige Digitaliseringsstrategi 2016-2020 blev Partnerskabet "Åbne offentlige data" etableret. Partnerskabet består af hhv. Erhvervsstyrelsen, Kommunerne Landsforening, Danske Regioner og Opendata.dk, og har fået til opgave at bane vejen for erhvervslivets udnyttelse af offentlige åbne data[49].

Partnerskabet har som noget af det første kastet sig over at få analyseret, på hvilke områder danske virksomheder efterspørger, at flere offentlige data gøres tilgængelige for dem[50]. Med henblik på at etablere et grundlag for at identificere tendenser i Danmark, har man indledt analysen med at identificere omfang af og kvalitet i udstillingen af åbne offentlige data i andre lande (USA, Storbritannien og Norge), *jf. boks 5*[51]. Konklusionen herpå blev, at selvom alle tre lande objektivt set er langt med udstilling af data, er der en række

[49] Kilde: Initiativ 5.1 "Åbne offentlige data" i Den Fællesoffentlige Digitaliseringsstrategi 2016-2012 via digst.dk
[50] Kilde: Monitor Deloitte (2017) for Partnerskab "Åbne offentlige data": Analyse af efterspørgsel og markedstendenser inden for offentlige data
[51] Kilde: Monitor Deloitte (2017) for Partnerskab "Åbne offentlige data": Analyse af efterspørgsel og markedstendenser inden for offentlige data, side 10

udfordringer, der forhindrer deres virksomheder i at drage fuld nytte af de tilgængeliggjorte data. Og ifølge undersøgelsens inddragede internationale eksperter bunder disse i større eller mindre omfang i manglen på en koordineret og fælles myndighedsindsats[52].

IDAs Digitaliseringsudvalg er enig i denne analyse, og anbefaler på det kraftigste, at der først og fremmest etableres en klar og slagkraftig governance for åbne data, såfremt man vil realisere det potentiale, som der vurderes at være konsensus om. Og denne governance skal være foruden af være tværoffentlig (stat, kommune og region) også være tværsektoriel, hvis ambitionen fra EU's forslag til en forordning om frie datastrømme i EU[53] skal gøres til virkelighed.

Boks 5: Arbejdet med offentlige åbne data i hhv. USA, Storbritannien og Norge

Uddrag fra "Analyse af efterspørgsel og markedstendenser inden for offentlige data". Monitor Deloitte. 30. juni 2017

USA

I USA blev hele grundlaget for tilgængeliggørelse af de enorme mængder offentlige data dannet i 2009, da præsident Obama udsendte Open Government Directive, hvor det blandt andet blev påkrævet af alle myndigheder at udarbejde specifikke planer for udstilling af data. Her har Executive Office of the President of the United States drevet agendaen og fungeret som koordinerende myndighed. Et konkret eksempel på et initiativ herfra er projektet Project Open Data, hvor Executive Office har indsamlet koder, værktøjer og casestudier med henblik på at hjælpe de øvrige myndigheder i deres arbejde med at udstille data. Helt konkret er der tale om en hjemmeside, hvor alle myndigheder kan bidrage med bedste praksis-metoder og videndele på tværs af fagområder.

Storbritannien

I Storbritannien var det et lignende tiltag i 2012 fra den konservative regering under David Cameron, der satte gang i udstillingen af data. Ligesom i USA blev fagministerier pålagt at formulere strategier for at udstille data, og det overordnede ansvar blev forankret centralt hos Cabinet Office og Government Digital Service. Sidstnævnte har blandt andet ansvaret for data.gov.uk's drift. I forlængelse heraf er der oprettet en række initiativer, der har forsøgt at fremme en fælles og koordineret indsats på området. Her er det værd at nævne Data Leaders Network, der er en tværministeriel gruppe med 23 forskellige myndigheder repræsenteret nedsat i 2015 af Cabinet Office med det formål at skabe ensretning i de forskellige myndigheders arbejde med data og udstilling af data. Dertil kommer Data Steering Group, hvor forskellige interessenter fra det private erhvervsliv, interesseorganisationer, universiteter og myndigheder på det strategiske niveau fører tilsyn med myndighedernes efterlevelse af deres datastrategier og forsøger at fremme et tværministerielt samarbejde. Et sidste eksempel på et initiativ, der også er forankret i Cabinet Office, er Data Science Accelerator, der er et tværministerielt træningsprogram, hvor offentligt ansatte med udgangspunkt i data fra deres egen myndighed over en tre måneders periode lærer at arbejde mere dataorienteret.

Norge

I Norge begyndte processen med at tilgængeliggøre offentlige data formelt i 2011, hvor den daværende regering instruerede fagministerierne og deres respektive styrelser om at gøre deres data tilgængelige i et maskinlæsbart format. Ligesom det er tilfældet i USA og Storbritannien, koordineres indsatsen fra centralt hold af Kommunal- og moderniseringsdepartementet og Direktoratet for forvaltning og IKT.

Ifølge analysen er det i alle af de tre nævnte lande et politisk initiativ fra centralt hold, der har været den afgørende faktor for, at åbne offentlige data-agendaen er blevet drevet fremad, og at data er blevet udstillet. Dette er også anbefalingen fra IDAs Digitaliseringsudvalg til Danmarks politikere. Der skal sættes politiske muskler bag ambitionen om at realisere potentialet i de åbne data. Men når det er sagt, skal det offentlige ikke styre og

[52] Kilde: Monitor Deloitte (2017) for Partnerskab "Åbne offentlige data": Analyse af efterspørgsel og markedstendenser inden for offentlige data, side 25

[53] Kilde: EU Kommissionen (2017): "Proposal for a regulation of the European Parliament and of the counsil on a framework for the free flow of non-personal data in the European Union" via www.ec.europa.eu

kræve alene. De private udbydere af åbne data skal mere end bare inddrages fra tid til anden. Der skal etableres et reelt samarbejde og governance omkring de åbne data, sådan at aftagerne heraf kan regne med kvalitet, dokumentation (hvad data siger noget om, hvor præcise de er, hvor gamle de er, hvem der ejer dem, osv.), vedligehold, support, format, tilgængelighed mv.

Sidstnævnte anbefaling understøttes ligeledes i det omtalte partnerskabs analyse, idet det er en pointe i resultaterne fra de tre belyste lande, at myndighederne i deres arbejde med at tilgængeliggøre data ikke i tilstrækkeligt omfang har inddraget og kommunikeret med virksomhederne. Dette har skabt stor frustration i erhvervslivet, idet de ikke har oplevet, at myndighederne har villet imødekomme deres behov[54], hvilket ligeledes alt andet lige har givet anledning til en mindre anvendelse af de mulige åbne data.

Den etablerede governance skal også sikre, at man ikke via sammenhænge i data, som egentlig er ikke-personhenførbare kan ende op med at få noget personhenførbart.

****

IDAs Digitaliseringsudvalg anbefaler, at der etableres en klar national governance i forbindelse med udbredelse af åbne data.

****

2.3.2 Få styr på klare begrebsdefinitioner og kvalitets- og dokumentationskrav

Ifølge IDAs Digitaliseringsudvalg bliver en af governancens fornemmeste og første centrale opgaver at få fodarbejdet i orden. Det betyder, dels at processer og samarbejde skal formaliseres og dels at få styr på klare begrebsdefinitioner og kvalitetskrav til data.

Det er afgørende, at der fra centralt hold defineres præcise definitioner af begreber samt klare krav til datakvaliteten og til dokumentationen; herunder for at reducere bias og for at realisere det fulde potentiale. Derudover er det nødvendigt med bred enighed om og opbakning til præcise krav og standarder for interoperabilitet mellem datasystemer for at sikre tilgængelighed og optimal anvendelse af data på tværs.

****

IDAs Digitaliseringsudvalg anbefaler en prioriteret indsats på nationalt niveau i forhold til at få styr på klare begrebsdefinitioner og kvalitets- og dokumentationskrav.

IDAs Digitaliseringsudvalg anbefaler ligeledes, at det skal være øverste led i ovennævnte governance, som har ansvar for at få styr på begrebsdefinitionerne og kvalitets og dokumentationskravene.

****

På trods af at initiativet bag åbne offentlige data har været centralt forankret i både Norge, USA og Storbritannien, har det reelle arbejde med at gøre data tilgængelig været forholdsvis silobaseret. Myndighederne har således haft et relativt snævert fokus på udstilling af

[54] Kilde: Monitor Deloitte (2017) for Partnerskab "Åbne offentlige data": Analyse af efterspørgsel og markedstendenser inden for offentlige data, side 26

egne data med udgangspunkt i egne retningslinjer og procedurer. Det skyldes først og fremmest, at der til trods for de forskellige fælleskoordinerende indsatser ikke reelt eksisterer et tværgående åbne offentlige data-mandat – kun individuelle mandater på ressortniveau. Med andre ord er der ikke noget reelt incitament for myndighederne til at arbejde sammen om udstillingen af data. Dertil kommer, at myndighederne – især i USA og Storbritannien – har prioriteret at udstille så mange data som muligt uden grundige og detaljerede overvejelser om, hvordan data bliver lagt ud[55]. Der har tilsyneladende været en (naiv) tro på, at udstillingen af data automatisk ville lede virksomhederne til at begynde at anvende åbne offentlige data.

2.3.3 Etabler et løbende evaluerings-setup

IDAs Digitaliseringsudvalg mener, at det er afgørende nødvendigt, at der etableres et evaluerings-setup med henblik på løbende at evaluere udbud og efterspørgsel. Herunder hvilke data, der er tilgængelige og hvilke der bliver brugt. Dette med henblik på at få kortlagt og nedbrudt eventuelle barrierer for at ikke-personhenførbare data kan flyde frit.

****

IDAs Digitaliseringsudvalg anbefaler, at den etablerede governance i forbindelse med udbredelsen af åbne data udvikler et evaluerings-setup, som løbende kan monitorere harmonien mellem udbud og efterspørgsel vedr. de åbne data.

IDAs Digitaliseringsudvalg anbefaler, at det er det øverste led i den etablerede governance, som får til ansvar at monitorere udbud og efterspørgsel mellem de åbne data.

****

2.3.4 Udarbejd sektorielle beregninger for de økonomiske konsekvenser

Endvidere er det væsentligt, at det videre arbejde med åbne data i Danmark og i EU indeholder beregninger af de økonomiske konsekvenser for såvel udbydere som for aftagere af de åbne data, idet blandt andet dataudbyderne alt andet lige vil have udgifter til 1) databearbejdning og udstilling, 2) sikring af datakvalitet og løbende vedligehold og 3) supportering og vejledning i forbindelse med andres anvendelse af og efterspørgsel efter data. Med andre ord er det ikke omkostningsfrit at gøre data tilgængelig for andre; særligt hvis det skal gøres ordentligt.

IDAs Digitaliseringsudvalg er med på, at en nøjagtig beregning af de økonomiske konsekvenser nok ikke er mulig ej heller gavnlig. Derfor mener IDAs Digitaliseringsudvalg, at man bør gå sektorielt til værks fx med udgangspunkt i Monitor Deloittes identificerede 4 dataområder i Danmark: vejrdata, energidata, transport-/mobilitetsdata og sundhedsdata[56].

****

[55] Kilde: Monitor Deloitte (2017) for Partnerskab "Åbne offentlige data": Analyse af efterspørgsel og markedstendenser inden for offentlige data
[56] Kilde: Monitor Deloitte (2017) for Partnerskab "Åbne offentlige data": Analyse af efterspørgsel og markedstendenser inden for offentlige data, side 55

IDAs Digitaliseringsudvalg anbefaler, at der udarbejdes sektorielle business cases for yderligere tilgængelighed og anvendelse af åbne data – herunder de økonomiske konsekvenser for både det offentlige og det private.
****

3. Indse at etik er et ufravigeligt aspekt af digitalisering

3.1 Etik i forbindelse med digitalisering bør have et selvstændigt fokus

Computere og software kommer i mange former – de kan være racister, de kan kønsdiskriminere og de kan koste menneskeliv. De er mekaniske og har ingen menneskelig forståelse, og derfor har vi på den korte bane brug for dels at tænke etik ind allerede i designfasen i al digitalisering og teknologi. Og dels at italesætte og forholde os til, at digitalisering og den teknologiske udvikling buldrer der ud af med en hastighed, som selv den årvågne kan have vanskeligt ved at følge med, hvorfor – hvis ikke vi tager de etiske dilemmaer *up front* – kan havne i situationer, hvor vi mennesker har mistet fodfæstet og overtaget over maskiner og algoritmer.

IDAs Digitaliseringsudvalg anbefaler, at Digital Etik får et selvstændigt fokus i et selvstændigt udvalgsarbejde. Etik bør ikke være en delpointe i forbindelse med digitalisering. Det bør være sit helt eget omdrejningspunkt.

3.2 Udfordringer

Dengang i 80'erne virkede filmene 'Tilbage til fremtiden' som det rene science fiction, men i en ikke så fjern fremtid vil vejene være fulde af selvkørende biler. Man har regnet ud, at det vil betyde færre trafikulykker og ligesom meget andet moderne teknologi frigiver de selvkørende biler en masse menneskelige ressourcer. Altså fordelene opvejer ulemperne. Men desværre vil der også være ulykker, og de kan potentielt være fatale. Og hvad gør man så? En sådan bil er forprogrammeret og fodret med viden og forskellige mulige scenarier og de mennesker, der har udviklet bilen, skal i langt højere grad end nu være tvunget til at tage stilling til konsekvenserne.

Her er et klassisk eksempel på et dilemma sat lidt på spidsen, en it-udvikler kan komme ud for. Hvem skal dø? Er det moren og datteren i fodgængerfeltet, der må lade livet? Eller skal det være det nygifte par inde i den selvkørende bil? Det er et af de mange spørgsmål, udviklerne af førerløse køretøjer i fremtiden skal være tvungne til at tage stilling til.

Det, vi forsøger at illustrere med eksemplet her, er, at det er vigtigt allerede tidligt i udviklingsfasen at afklare forskellige spørgsmål såsom, hvordan systemet vil reagere i forskellige situationer, og hvis man ikke har alle svarene på hånden, så er det uetisk og uansvarlig at påbegynde udviklingen.

For vi ser flere og flere etiske spørgsmål rejse sig i takt med, at it-løsninger som en naturlig del af hverdagen eksploderer. For eksempel som Microsofts Twitter-robot Tay, der blev racist på rekordtid. Meningen var, at Tay skulle lære af kontakten med andre Twitter-brugere – men Twitter-folket begyndte at fodre Tay med ondskab af forskellig art, herunder racistiske og sexistiske udsagn. Siden fundamentet for Tays eksistens hvilede på input fra

andre mennesker, endte chatbotten kort efter sin fødsel som fan af Donald Trump, holocaustbenægter og konspiratorisk fortaler for, at det var George W. Bush, der stod bag 9/11[57].

Det er heller ikke så længe siden, en robot forvekslede et billede af to sorte mennesker med aber[58].

Maskiner ejer ikke empati og besidder ej heller menneskelig forståelse, derfor er det yderst vigtigt, at vi fodrer dem med de rette informationer, og at der ligger en bred pallette af velfunderede etiske overvejelser bag. For 'machine learning'-algoritmer lærer helt uden kritisk sans af dybt indvundne race- og kønsfordomme, der er skjult i vores sprogbrugsmønstre, siger forskere[59]. Og også sådanne fejl skal der selvfølgelig rettes op på, inden de ser dagens lys – og det sker ved, at man allerede i designfasen indtænker etik som det naturligste i verden.

Vi møder i hverdagen flere og flere robotter, der servicerer og vurderer os, når vi skal bestille forsikringer, have behandlet låneansøgninger og i det hele taget løse opgaver for os onlinebrugere – og så behandler de i stigende omfang vores sundhedsdata og lægger dermed pres på personfølsomme oplysninger og privatliv.

Teknologien er her allerede og vi bruger den også i vidt omfang, men har vi reelt taget stilling til, om det er den retning, vi ønsker at gå i? Der er mere eller mindre konsensus om, at vi via teknologi og digitalisering kan gøre ting nemmere og effektivisere, men har vi derudover reelt indsigt i konsekvenserne? Tidligere ville man fx ikke acceptere/finde sig, at man skulle stille med alt, hvad man brugte sine penge på, inden man kunne få et lån. Men med digitalisering og robotter har bankerne i dag fået en bagdør hertil via big data. Og en ting er, at bankerne nu har al den viden tilgængelig. En anden er, at man som bankkunde kan få afslag på sin lånansøgning på grund af en eller anden algoritme. Og hvem klager man så til i den situation?

Endvidere har fx den sundhedsteknologiske udvikling haft en kæmpe positiv indflydelse på en lang række områder, men der er også etiske spørgsmål, som både nu og i fremtiden lurer under overfladen. Hvordan håndterer vi blandt andet, at det allerede nu er muligt at hacke en computer via DNA[60]? På sigt vil mere og mere digitalisering materialiserer sig i fysiske og levende ting, hvilket betyder, at det trusselsbillede i forhold til cyber- og informationssikkerhed samt de etiske overvejelser, som vi allerede kender og gør os i dag, kun bliver endnu mere komplekse og uigennemskuelige.

[57] Kilde: The Washington Post (2016): "Meet Tay, the creepy-realistic robot who talks just like a teen", den 23. marts 2016
[58] Kilde: c|net (2015): "Google apologizes for algoritm mistakenly calling black people "gorillas", den 1. juli 2015
[59] Kilde: , Patrick Allo, Mariarosaria TaddeoSandra Wachter, Luciano Floridi (2016): "The ethics of algoritms: Mapping the debate" I *Sage Journals* via www. journals.sagepub.com[60] Peter Ney, Karl Koscher, Lee Organick, Luis Ceze, Tadayoshi Kohno (2017): "Computer Security, Privacy, and DNA Sequencing: Compromising Computers with Synthesized DNA, Privacy Leaks, and More", *University of Washington*
[60] Peter Ney, Karl Koscher, Lee Organick, Luis Ceze, Tadayoshi Kohno (2017): "Computer Security, Privacy, and DNA Sequencing: Compromising Computers with Synthesized DNA, Privacy Leaks, and More", *University of Washington*

3.2.1 To hovedudfordringer

IDAs Digitaliseringsudvalg identificerer på baggrund af ovenstående særligt to hovedudfordringer.

I Danmark har vi en grundlæggende et højt niveau af tillid. Det har i mange henseender været et plus og har arbejdet til fordel for udviklingen af det danske samfund. I forbindelse med den stigende digitalisering kan vi dog risikere at sætte denne tillid over styr, hvis ikke vi tænker os overordentlig godt om.

Grundet vores grundlæggende tillid til samfundet og dettes aktører har vi også med stor tillid taget digitaliseringens og teknologiens muligheder til os. Og det både i blandt de offentlige myndigheder, de private virksomheder og ikke mindst borgerne/forbrugerne. Vi er det mest digitaliserede land i EU, og vi er stolte af det. Men betyder det, at vi er verdensmestre til at anvende teknologi klogt og sikkert? Nej, det gør det ikke. For samtidig med vores 1. plads indtager vi jo som nævnt også 34. pladsen ud af 193 lande i forhold til cyber- og informationssikkerhed. Det lugter lidt af, at vi tillidsfuldt har taget digitaliseringen til os, men måske vi har været for tillidsfulde og ikke brugt krudt på at sætte os ordentlig ind i konsekvenserne.

På nettet bliver man som bruger ofte bedt om at afgive en række personlige oplysninger. Det kan være som medlem af en kundeklub, når man opretter en profil på et socialt medie, når man foretager et køb eller er i kontakt en med en offentlig myndighed. Når den enkelte afgiver data, er der masser af faldgruber. For det første er det selvfølgelig vigtigt at sikre sig, at modtageren er den rigtige. For det andet bliver man ofte blive bedt om at afgive data, som ikke er nødvendige for at kunne gennemføre det køb, den tjeneste eller den tilmelding, som man ønsker. For det tredje kan det være svært at afgøre, hvordan de data, man afgiver, bliver opbevaret og behandlet. Der findes ikke noget samlet overblik over, hvor mange data, der videresælges til tredjepart i kommercielt øjemed, men antallet af personaliserede reklamer vidner om, at der videregives/sælges store mængder data. Endelig er der selvfølgelig også en risiko for, at data bliver solgt eller opsnappet/hacket og brugt til kriminelle aktiviteter.

På trods af at mange (69 pct.)[61] gerne vil gøre mere for at sikre deres anonymitet på nettet, er der ifølge IDAs analyse "Privacy og Databeskyttelse, *jf. tabel 3,* 34 pct., som sjældent eller aldrig læser betingelserne, når de tilmelder sig tjenester eller downloader apps. Yderligere 26 pct. gør det kun af og til. Man må konstatere, at der er en opgivende holdning til mulighederne for at beskytte sit privatliv på nettet. Det understøttes af, at 55 pct. af befolkningen svarer, at det er umuligt at færdes anonymt på nettet. En forklaring på, at så få sætter sig ind i betingelserne for de forskellige tjenester, kan være, at det ofte er meget lange, komplicerede tekster, som mange ikke orker at komme igennem. En anden forklaring kan være, at situationen er *take it or leave it*: Hvis man ønsker (eller er nødt til) at bruge en tjeneste/se noget indhold mv., er man nødt til at acceptere betingelser, selvom

[61] Kilde: IDA Analyse (2017): "Privacy og datasikkerhed"

man ikke er glad for det. Det er jo en form for ”pakkeløsning”, hvor man får dette indhold/denne service, hvis du betaler via dine personlige data. De fleste er dog nok ikke klar over eller bevidste om dette forhold, og heller ikke om prisen de (potentielt) betaler.

Tabel 3: Læser du betingelserne, når du tilmelder dig tjenester eller downloader apps?

	2015	2017
Aldrig	11 %	10 %
Sjældent	27 %	24 %
Af og til	29 %	26 %
Ofte	17 %	24 %
Altid	13 %	13 %
Ved ikke	1 %	2 %
I alt	100 %	100 %

Kilde: IDA Analyse (2017): Privacy og Datasikkerhed

Den fremherskende digitale forretningsmodel på nettet er, at forbrugerne betaler for indhold ved at blive eksponeret for reklamer. Jo mere personligt reklamerne kan målrettes, jo større effekt, og der er derfor store økonomiske interesser i at indsamle persondata. Reelt betaler forbrugerne – ofte intetanende – en uigennemsigtig pris med deres persondata, og i takt med, at det går op for dem, vokser deres skepsis og deres lyst til at slette deres data, ligesom de holder sig tilbage fra at afgive deres data eller afgiver forkerte data. I forhold til at afgive forkerte data bryder man således de betingelser, som man netop har accepteret. Desuden er vurderingen fra IDAs Digitaliseringsudvalg, at denne manøvre dog sjældent virker. Ens digitale identitet bliver kortlagt og koblet til ens person, selvom man visse steder angiver forkert navn, køn, adresse mv.

På trods af at mange opfatter en række data som meget private, er der alligevel mange, som er parate til at afgive personlige date for at kunne oprette en profil på et socialt medie. *Jf. tabel 4* er der er fx 68 pct., der er parate til at oplyse om køn og alder, mens 53 pct. har afgivet oplysninger om fx navn, adresse og telefonnummer. Der er også mere end hver tredje, der har delt placering med et socialt medie. Tilsyneladende er ønsket om at have profiler på de sociale medier nok til, at mange slækker på ønsket om at holde på private oplysninger.

Tabel 4: Har du afgivet forskellige typer af data på nettet for at oprette en profil på et socialt medie? Markér hvilke oplysninger, du har afgivet

	2015	2017
E-mail	77 %	73 %
Køn og alder	71 %	68 %
Basale data: (navn, adresse, telefonnummer)	57 %	53 %
Din placering (locations-oplysninger)	37 %	36 %
Adgang til foto	33 %	27 %
Kontaktdata til venner (fx dine facebookvenner eller din adresseliste fra dit mailprogram)	16 %	14 %
Oplysninger om forbrugsvaner	11 %	11 %
Holdninger (fx politisk eller religiøs holdning)	10 %	11 %
Oplysninger om medievaner	12 %	11 %
Seksuel orientering	-	7 %
Personnummer	6 %	6 %
Oplysninger om økonomi og indtægt	7 %	6 %

Andet	-	3 %
Helbredsoplysninger	2 %	2 %
Ingen af ovenstående	14 %	17 %

Kilde: IDA Analyse (2017): Privacy og Datasikkerhed

Direkte adspurgt svarer en del af befolkningen, *jf. tabel 5*, at forskellige forhold vil kunne få dem til at afgive personlige oplysninger, som de ellers ikke ville være parate til at afgive. Det drejer sig vigtigst af alt om en tillidsvækkende og tydelig privacypolitik fra virksomheden. En del vil dog også afgive oplysninger, hvis de til gengæld opnår tilbud, rabatter eller andre fordele.

Tabel 5: Hvilken betydning har følgende for, om du vil afgive data om dig selv om dine vaner, som du ellers ikke ville give?

	Ja, det kunne helt sikkert få mig til at afgive flere data end ellers	Ja, det kunne muligvis få mig til at afgive flere data end ellers	Nej det kunne ikke få mig til at afgive flere data end ellers	Ved ikke	I alt
Hvis jeg har tillid til at mine data vil være beskyttet	15 %	52 %	25 %	8 %	100 %
Virksomhedens privacy politik (med hensyn til datahåndtering)	7 %	44 %	38 %	11 %	100 %
Hvis det er en virksomhed jeg ofte handler med	7 %	48 %	38 %	8 %	100 %
Gratis produkter	5 %	27 %	61 %	7 %	100 %
Rabat på forsikringer	5 %	36 %	51 %	8 %	100 %
Hvis jeg har stor interesse i produkterne eller ydelserne der tilbydes	5 %	36 %	50 %	10 %	100 %
Rabat på en vare, fx rejse eller bil	4 %	35 %	54 %	7 %	100 %
Hvis jeg kan lide virksomhedens værdier	3 %	30 %	56 %	11 %	100 %
Hvis det betyder, at jeg kan få tilbud, der er skræddersyede til mig	3 %	28 %	59 %	10 %	100 %
Standarden af virksomhedens kundeservice	3 %	24 %	61 %	12 %	100 %
En konkurrence hvor du kan vinde fx en rejse eller en bil	2 %	19 %	72 %	7 %	100 %

Kilde: IDA Analyse (2017): Privacy og Datasikkerhed

Ifølge IDAs Digitaliseringsudvalg står vi først og fremmest med en ***demokratisk udfordring***. Vores tillid til mange af de store firmaer, herunder Google og Facebook, som vi gladeligt afgiver alskens data til for til gengæld at modtage ”gratis” sociale medier og søgefunktioner og mailtjeneste, er stor. Uden at den egentlig burde være det. Hovedreglen er, at der aldrig er noget, som er gratis. Hvis noget er gratis (dvs. det koster ikke nogle penge lige nu og her), så er man selv produktet.

Ikke desto mindre er medlemskab af fx Facebook og Google blevet så indlejret i vores samfund, at organiserede instanser som fx DR og Jyllandsposten, såfremt man vil deltage i debatten på deres hjemmesider, kræver medlemskab af enten Facebook og/eller Google. Både DR og Jyllandsposten kan vel klassificeres som værende en del af den 4. statsmagt, hvorfor det er problematisk, at det kræves, at man lige skal betale med sine egne data først til Facebook/Google, inden man som borger kan få lov til at deltage i den del af demokratiet. Det er en kedelig og bekymrende udvikling, som bør standses.

Vi skal ikke have tvunget medlemskab til den slags tjenester for at kunne deltage i dette og hint. Hvis man som borger selv vil involvere sig med fx Facebook og Google, skal det stå den enkelte frit for. Men man skal ikke pålægges det og tilmed risikere at komme til at stå uden for, hvis man holder på sin ret til sine egne data og ikke vil produktliggøres af fx Facebook og Google.

Dernæst er IDAs Digitaliseringsudvalg enige om, at vi står med en seriøs ***udfordring i forhold til digital etisk dannelse***. Dette har overvejende sammenhæng til *"1.3.6 Sikr uddannelse på it-sikkerhedsområdet – og dét livslang".* I IDA betragter vi digital etisk dannelse som bestående af særligt tre områder, hvor danskerne har et betydeligt forbedringspotentiale. De tre områder er danskernes i) kildekritiske forståelse og indsigt, ii) bevidsthed om og ansvar for, at de er producenter af indhold på diverse SoMe-platforme og iii) kundskaber i forhold til at indgå i dialog i debat på ligeledes diverse SoMe-platforme.

Fordi vi overvejende er så tillidsfulde, er vi ikke tilstrækkeligt på barrikaderne, og vi er derfor i højrisiko for at blive taget ved næsen. De helt unge mennesker tager mere eller mindre ufortrødent diverse digitale enheder og apps til sig uden at kende konsekvenserne. Forældregenerationen tager måske knap så mange devises og apps til sig, men de har ligeledes begrænset begreb om konsekvenserne, og lægger mere eller mindre bekymringsfrit alskens billeder på op Facebook, Instagram og Snapchat af deres afkom, uden 1) at få samtykke fra deres børn og 2) tænke over, at alle tre tjenester lagre og har ret til at videredistribuere til tredjepart, hvis de skulle have lyst[62]. Og endelig er der Martins mor, *jf. boks 3*, som er så overforsigtig (og analog), at hun på ingen måde får det fulde udbytte ud af teknologiens muligheder.

I lighed manglende livslang uddannelse i cyber- og informationssikkerhed mangler der i særdeleshed også information og viden hos forbrugerne/borgerne omkring digital etik. Dels både konsekvenserne af at anvende diverse digitale enheder og apps og dels hvordan man skal gebærde sig online. DR Ultra initierede via deres app og Facebook-side en dialog med deres brugere (børn i alderen 7-12 år) om god tone på de sociale medier, herunder understøttet af en række små film, hvor man ansigt til ansigt sagde nogle af de udsagn, som børn via de sociale medier havde sendt afsted til hinanden. DR Ultras erfaring var, at børnene tog denne dialog konstruktivt til sig og havde et kæmpe behov for at italesætte udfordringen. Da DR Ultra forsøgte at tage dialogen med de voksne via DRs Facebookside måtte de efter en rum tid lukke dialogen ned igen, idet tonen i blandt de voksne

[62] Kilde: Se samtykkeerklæringer fra fx Facebook, Instagram og Snapchat

simpelthen blev for grov og ukonstruktiv[63]. Hvordan kan vi forlange, at vores børn skal holde en god tone, når deres forældre og forventelige forbilleder ikke kan levere tilsvarende? Det lugter af, at vi står med en samfundsudfordring, som vi som samfund må finde en måde at tage hånd om. Og IDA er vi klar til at spille en central rolle i den forbindelse via oplysning og samarbejde med andre relevante aktører med henblik på at finde ud af, i hvilken arena denne digital etisk dannelse har de bedste udfoldelsesmuligheder.

3.3 Anbefalinger

Skulle dette afsnit omkring etik følge strukturen i de to forrige afsnit, der indeholder anbefalinger, skulle IDAs Digitaliseringsudvalg stille med anbefalinger til, hvad vi i Danmark kan og bør gøre i forhold til etik og digitalisering. Dette var også indledningsvist ambitionen hos IDAs Digitaliseringsudvalg, men i takt med at drøftelserne i udvalget skred frem, blev udvalget enig med sig selv om følgende.

De etiske overvejelser i forbindelse med digitalisering er så vidtgående, at konkrete indsatser og anbefalinger i den forbindelse ikke bør være en delmængde i et udvalgsarbejde omhandlende digitalisering. Etik og digitalisering bør være et selvstændigt arbejde og have et selvstændigt fokus. Så vigtig og central, mener IDAs Digitaliseringsudvalg, at denne tematik er.

Fx kunne det være værd at overveje, om ikke etik i teknologiverden burde have et større politisk fokus – måske i form at sit eget etiske organ. Etisk Råd i Danmark beskæftiger sig mestendels med etiske spørgsmål om bio- og genteknologi såsom organdonation, aktiv dødshjælp, fødsel og død og er forankret under Sundheds- og Ældreministeriet. Det nuværende etiske råd udsprang i kølvandet på en række reproduktive dilemmaer, som – grundet moderne teknologier – opstod i 80'erne. Her godt 30 år efter, at Etisk Råd så dagens lys, er det måske på tide, at teknologi får sit helt eget etiske råd, i og med teknologi sniger sig ind i alle afkroge af vores liv, hvor flere og flere etiske dilemmaer opstår, hvilke i sidste ende også kan blive fatale.

Til en start anbefaler IDAs Digitaliseringsudvalg dog, at der nedsættes et nyt udvalg, som over et års tid dybdegående kan beskæftige sig med denne problemstilling.

****

IDAs Digitaliseringsudvalg anbefaler, at der etableres et udvalg for Digital Etik. Udvalget skal dybdegående beskæftige sig med at komme med konkrete bud på indsatser og anbefalinger til de udfordringer, som IDAs Digitaliseringsudvalg ud fra et teknisk og naturvidenskabeligt udgangspunkt har identificeret i denne rapport.

****

[63] Kilde: Dorte Høeg Brask, Digital Redaktør Børn, DR Medier.

IDAs Digitaliseringsudvalg både bemærker og velkommer regeringens nyligt nedsatte ekspertgruppe om dataetik, hvor også IDAs formand sidder med[64]. IDAs Digitaliseringsudvalg mener, at ekspertgruppens arbejde med fordel kan spille sammen med – og eventuelt være et indledende tiltag i forhold til – nærværende anbefaling om etablering af et udvalg for Digital Etik, hvilket har til hensigt at favne den samlede udfordring vedrørende etik og teknologi.

[64] Kilde: Erhvervsministeriet (2018), "Regeringen nedsætter ekspertgruppe om dataetik" via www.evm.dk den 12.3.2018

IDAs Digitaliseringsudvalg

8 eksperter hjælper IDA med at formulere IDAs Digitaliseringspolitik
Primo 2017 nedsatte IDA IDAs Digitaliseringsudvalg. Udvalget består af 8 medlemmer, som alle med forskellige vinkler er eksperter på digitalisering og de muligheder og udfordringer, som i den forbindelse skal gribes og håndteres. Udvalget er alene nedsat i 2017. Udvalget har fået til opgave at hjælpe IDA med at formulere IDAs digitaliseringspolitik, hvorfor et samlet bud herpå derfor bliver udvalgets slutprodukt. IDAs digitaliseringspolitik ventes at være udarbejdet primo 2018.

Nærværende rapport er udvalgets anden runde af anbefalinger, som er blevet [indstillet til og tiltrådt af IDAs formand Thomas Damkjær Petersen]. Udvalget lancerede i november sin første runde anbefalinger i en rapport ved navn *Bedre it-projekter – 7 råd fra IDA.* I løbet af 2018 offentliggøres yderligere anbefalinger vedrørende ledelse i en digital tidsalder Logikken bag Digitaliseringsudvalgets selektion af emner er forsøgt forklaret i nedenstående figur:

Medlemmer af IDAs Digitaliseringsudvalg

Martin Bech
Head of operation and development for the Danish Research Network

Jan Madsen
Professor, DTU Compute

Lise Gerd Pedersen
Ejer og stifter af ARCHIT

Kåre Løvgren
3Shape A/S og formand for IDA IT

Jan Bøgh
Contract manager ved TDC og formand for IDA Tele

Ivan Lilleng
Udvalgsformand og medlem af IDAs Hovedbestyrelse

Karsten Hjort Reichstein
Director - Head of IT S&D, e-nettet a/s

Bjørn Borup
CIO, IDA