Justitsministeriet
Databeskyttelseskontoret
Slotsholmsgade 10
1216 København K.
jm@jm.dk og mir@jm.dk

10. oktober 2020

Høringssvar: National evaluering af databeskyttelsesreglerne

Danmark er stadig et af verdens bedst fungerende samfund, men det er på trods af vores forældede tilgang til digitalisering og navnlig at Danmark fra starten undlod at implementere GDPR for at tækkes en forældet centralistisk magt- og systemstruktur, der gør langt mere skade end gavn.

Der er ingen tvivl om at digitaliseringen er kommet for at blive og digitale data er selve grundlaget for forskning, services, forebyggelse af kriminalitet, konkurrenceevne og individuel livskvalitet.

Det væsentlige er at fokusere på at fejlene er strukturelle og til en vis grad stammer fra mainframens tidsalder, men at det kan skabe fejlopfattelsen af at GDPR skaber begrænsninger lokalt, som reelt skyldes en forældet arkitektur og datastrukturer centralt.

Man kan opsummere budskabet simpelt – GDPR er kompleks, hvor den forsøger at begrænse skaderne af sekundær brug af persondata, hvor der ikke blev tænkt på sikkerhed. GDPR er ubureaukratisk, når man har styr på sikkerheden og har designet med udgangspunkt i Privacy/Security by Design.

Fejlen er at der uden grund flyder stadigt flere persondata overalt i den offentlige sektor, hvor der principielt ingen persondata burde være. Dataflow er grundlæggende forkert designet, så det underminerer både sikkerheden, samfundseffektiviteten og borgerrettigheder på en måde, der skaber stadigt større ubalancer, som prioriterer særinteresser på bekostning af de primære samfundshensyn og specielt ligheden.

Dette gælder ikke kun gamle systemer såsom SKAT og og EPJ, men helt nye såsom National Genom Center, Telemedicin, MitID og AULA, der alle - på trods af bedre vidende - blev designet forkert fra starten. Og intet tyder på at man er begyndt at rette op, når man ser på f.eks. AML, Personlig Medicin og tiltag omkring kunstig intelligens.

En overfladisk analyse kunne pege på at f.eks. SmitteStop er det første forsøg på at rette op med Privacy by Design, men det er kun på overfladen, fordi samme er låst til NemID, mobil-platformenes overvågning og dækker funktionelt kun et meget lille del af problemstillingen, fordi man blev afpresset til det af Google/Apple..

Dette høringssvar har 2 ambitiøse mål:

1) At demonstrere høringens agenda om yderligere underminering for at fremme en allerede stærkt fejlslagen digitaliseringsstrategi er selve problemet for både samfundsøkonomien, sikkerheden og retssikkerheden.

2) At påvise, hvordan GDPR leverer svaret på hvordan statsadministrationen igen varetager sine hovedopgaver og bringer Danmark tilbage på sporet på alle 3 områder.

Formuleringerne er skarpe for at fremme forståelsen for pointerne, men skal ikke misforstås som havende et ideologisk (hverken økonomisk ideologisk eller f.eks. libertariansk anti-statslig) eller anti-teknologisk ærinde.

Budskabet er et grundlæggende behov for et opgør med en forældet tilgang til digitalisering, som har stået larmende klart i mindst 10 år uden nogen reelt er begyndt at tage ansvar. Allerede i 2010 kom Rapporten om "Nye Digitale Sikkerhedsmodeller"[1] med fokus på nødvendigheden af at systemskifte med fokus på Privacy og Security by Design. Baggrunden er den genereelle forskningsmæssige erkendelse at man ganske enkelt ikke kan beskytte persondata i centrale databaser – at vi er nødt til at skifte tankegang til at sikre data forebyggende

Rapporten dokumenterede med konkrete cases baseret på workshops med offentlige embedsfolk at it-systemer IKKE har brug for persondata for at fungere ligesom sikkerheden IKKE styrkes af overvågning og opsamling af persondata – faktisk kan de fungere meget bedre UDEN persondata.

Dette er netop essensen i GDPRs fokus på at styrke det gældende normative grundprincip om data minimering (f.eks. artikel 25 og 5.1.C), som allerede blev fastslået med det oprindelige direktiv fra 1995. Hertil kommer koblingen til eIDAS artikel 5 omkring Pseudonyme Signaturer, som implementerer princippet om "Legal Identifikation uden Digital Identifikation". En Trustworthy Identitet er meget mere end en pseudonym signatur, men implementeret og brugt rigtigt kan man næsten 100% eliminere modsætningerne mellem f.eks. borgerrettigheder og sikkerhed på den ene side og fællesskabets interesser i forskning, kriminalitetsbekæmpelse og eksport på den anden side.

En væsentlig del af budskabet er, at det haster at ændre retning, fordi det vil tage tid. Vi kan og skal ikke lave en tabula raza i troen på at en Big Bang ændring pludselig kan ændre årtiers fejldigitalisering. Hvis noget, så har Sundhedsplatformen understreget konsekvenser af manglende planlægning og forberedelse.

Vi slæber en teknologigæld med os, som kun gradvist kan omlægges i takt med investeringerne. Og denne teknologigæld er ikke kun er negativ – kontinuitet i services og generationers strukturerede opsamling af data er særdeles værdifulde for specielt forskningen. Det skal vi ikke bare kaste i havet, fordi tiderne og krav til den fremadrettede digitalisering har ændret sig. Det vil tage tid at rydde op i årtiers fejldigitalisering og det skal ske både intelligent og styret.

Ny tænkning kræver nye måder at evaluere på

Hovedproblemet er at evalueringen af nye digitaliseringstiltag foregår alt for primitivt og oftest direkte misvisende baseret på argumenter som plukker ud af en mere kompleks sammenhæng.

At skabe løsninger som tage højde for de mere komplekse krav uden at gå på kompromis med de primære hensyn kræver en grundlæggende ændring af gældende praksis. Det starter med at ændre evaluringskriterierne, så man f.eks. fokuserer på de følgende 5 grundspørgsmål:

1. Giver det borgeren beslutningskrav rum til at maksimere værdien for borgeren af medgåede ressourcer, dvs. så systemerne tilpasser sig borgernes behov i stedet for omvendt?

2. Giver det borgeren reel kontrol over egne data og herunder mulighed for at dele data til nye formål uden at afgive kontrollen?

1 https://digitaliser.dk/resource/781482/artefact/Nyedigitalesikkerhedsmodeller.pdf?artefact=true&PID=795677

3. Kan systemet forny sig og tilpasse sig borgernes individuelle behov uden dyre og langsommelige udbudsprocesser?

4. Er systemet baseret på Security by Design, dvs. er det designet til at modstå sikkerhedsangreb og forebygge skalering selv hvis perimetersikkerheden brydes 100% og databaserne blotlægges til de værste misbrugsinteresser?

Ovenstående vil meget ofte afsløres af den afgørende lovpligtige DPIA analyse med de to væsentlige spørgsmål

5. Er systemet data minimeret til det punkt, hvor der slet ikke indgår identificerede persondata (Privacy/Security by Design)? Har borgerne adgang til ”data portabilitet” direkte ved kilden uden man-in-the-middle (a la Sundhed.dk eller Borger.dk)?

Ovenstående afspejler en borger-centrisk tilgang til digitalisering, som er næsten giver i fysiske samfundssystemer, men meget sjældent fundet i digitale systemer.

Hovedproblemet er en fejlslagen Digitaliseringsstrategi

Danmark taber hastigt terræn fra den relative top, som kan dateres til ca. 1990-2000.
Demokratiet og samfundsøkonomien svækkes af præcis de samme årsager som har ramt de fleste af verdens demokratier, men Danmark rammes langt hårdere, fordi vi er mere digitaliseret i mainframens tidsalder og har fornægtet at tilpasse os realiteterne i den digitale verden.

Hastværket med at digitalisere uigennemtænkt med statsmagtens tvang i ryggen har IGEN erstattet den historiske danske styrke baseret på rationel analyse og balancerede beslutninger for den lange bane med letkøbte selvdestruktive ideologier.

Vi så det senest i 2008, hvor finanssektorens blinde tillid til modeltænkningen omkring diversificering af risici skalerede til ekstreme risici i en boble, som uundgåeligt ville springe (en ideologisk analytisk fejl, man er i færd med at gentage med præcis den samme BNP-tankegang som skabte 2008, men det er en anden diskussion end den nærværende).

Et endnu mere relevant eksempel er den måde, man har ladet kommercielle BigTech kræfter overtage kontrollen med individets og dermed både hele demokratiets og markedsøkonomiens meningsdannelse og adfærd. Den direkte årsag hertil er den demokratiske stats governancesvigt, fordi man har ignoreret den demokratiske stats hovedopgave - at sikre borgeren - til fordel for en klart fejlslagen agenda om overvågning og central styring.

Staten har kort sagt ignoreret ansvaret for at skabe bæredygtige digitale rammer for samfundsdannelsen.

Dette senest dokumenteret med af en stor fransk Adtech, som i deres kvartalsmæssige fondsbørsmeddelelse[2] arrogant kom til at afsløre omfanget af deres udnyttelse af statens svigt på den digitale sikkerhed. De meddelte at de - udenom alle de fejlslagne bureaukratiske forestillinger om ”Cookie-popups” etc. - uden videre kan identificere og detailprofilere 98% af alle borgere.

2 https:// criteo.investorroom.com/download/CRTO+ Q2+2020+Earnings+call+Script_FINAL_WEBVERSION.pdf

Vi taler kort sagt om næsten totalt anarki, hvor udenlandske virksomheder, stater og andre kriminelle kræfter uden videre kan vade ind over de danske landegrænser og begå systematiske overgreb på næsten alle danskere, hvad enten formålet er manipulation med det danske demokrati, simpel vinding eller cyberattacks.

Årsagen til, at dette kan foregå upåagtet, er at den danske statsadministration bruger præcis den samme tilgang indenfor de offentlige perimeter-mure som anarkiet i det bredere samfund. Endnu værre, så har den danske stat aktivt blokeret alle digitale forsvar i den private sektor ved at gennemtvinge identifikation og overvågning. Statsadministrationen ønsker overvågningsdata fra den private sektor samtidig med at de samme ideologiske kræfter i den private sektor ønsker og har opnået tilgang til at udnytte de omfattende offentlige profileringsdatabaser på specielt finans- og sundhedsområdet.

Denne ”Datahvidvask” er en særlig destruktiv form for Digital Feudalisme, hvor statsmagten udnyttes til tvangsovervågning og profilering af borgerne for at opsamle data, som derefter udnyttes til magt og profit på borgernes og samfundets bekostning.

BigData AI drukner babyen i badevandet.

BigData AI kan opfattes som dårlige akademikeres forestilling om at man kan erstatte kausal problem- og samfundsforståelse med simple statistiske korrelationer, hvis blot man har nok data og modellen er tilstrækkelig avanceret.

Det er ikke en ny form for ideologisk idioti, idet det er samme tankegang som lå bag Taylorismen, Kommunismens 5-årsplaner og totalitære staters overvågning af borgerne. Men med neurale netværk til at automatisere dataanalyse og nye digitale overvågningsmekanismer til at opsamle og sammenstille data til intime profiler af borgerne fylder man gammel fejlslagen ideologisk vin på nye digitale flasker.

Det er væsentligt ikke at forveksle dette med f.eks. CPR og registersamkøring i perioden 1960-1990, hvor der var et reelt valg mellem effektive samfundsprocesser og rettigheder. Her valgte Danmark valgte at løbe risikoen med CPR-systemet, som de fleste andre lande ikke gjorde. Med internettet blev dette en falsk modsætning, fordi borgerne f.eks. med pseudonyme signaturer kan være direkte part i al datadeling. CPR-tanken er kort sagt forældet og moden til opgradering.

Vi både kan og skal lære af historien (til f.eks. sundhedsforskning), men ikke med de dårlige metodevalg som skaber flere særdeles alvorlige og selvforstærkende negative spiraler på en gang.

1. Al BigData forudsætter overvågning (identifikation), dvs. det sekundære formål bliver misbrugt til et selvstændigt angreb på basale rettigheder og skader it-sikkerheden overalt.

2. Al BigData forudsætter registersamkøring, dvs. det sekundære formål bliver misbrugt til at skabe stadigt mere intime profiler af hver enkelt borger og destabliserende magtstrukturer.

3. Koblingen til neutrale netværk skaber en selvforstærkende negativ spiral, hvor den indbyggede bias tvinger samfundsprocesser og mennesker til at tilpasse sig modellen og dermed skaber interesse-styret tvangsadfærd.

BigData skaber ”tvungne svingninger”

Problemet med BigData AI kan sammenlignes med ”tvungne svingninger”, som kan trække ellers stabiliserende samfundskræfter stadigt mere ud af balance. Vi ser denne fejl overalt, hvor dette indgår.

I SoMe bruges det til at filtrere verden ved at fodre borgerne med stadigt mere af det som de gør og frasorterer alt andet bortset fra det som kommercielle interesser ØNSKER skal forandres (reklamefinansieret), dvs. det skaber subjektive styrede opfattelser, som aktivt manipulerer mennesker og dermed hele den demokratiske process og markedsøkonomien.

Indenfor økonomi har BNP-modeller altid været dårlige til at beskrive virkeligheden, men de sidste årtier har man skabt særligt negative feedback-loops, hvor man med økonomiske tiltag (såsom f.eks. QE / Quantative Easing) forsøger på at tvinge samfundsøkonomien til at tilpasse sig de dårlige modellers indbyggede bias og politiske agendaer om BNP som økonomisk mål. Dette på trods af at BNP ikke kan sige meget rationelt om værdiskabelsen i samfundet for borgerne i hverken den offentlige (hvor man de faktor sætter Værdi=”Medgåede omkostninger”) eller private sektor (hvor man endnu værre arbejder med Værdi=”Profit” selvom fungerende konkurrence netop ville reducere profitten).

Denne forveksling af konjunkturpolitisk og strukturpolitik er formentlig en af de største krise-skabere i nyere tid, som i perioden fra ca. 1990 til i dag har betydet at man har skredet fra en krise til den næste, hvor den næste krise skabes af specielt QE-tiltag for at håndtere den forrige krise.

Problemet er at den samme makro-økonomiske agenda ny skrider ind i mikro-områdets detailstyring via intim overvågning på, ineffektiviserende tvangsforsimpling og egentlig adfærdskontrol i både social- (f.eks. misrøgt, social svindel), uddannelse- (f.eks. trivsel) og navnlig sundhedssektoren (f.eks. personlig medicin og National Genom Center) uden tanke for den indbyggede skævvridning og næsten deterministiske sammenbrud.

Nationalstatens forsøg på ”nudging”-baseret adfærdsstyring er vejen mod og ses klarest i den Kinesiske model med Social Kredit, hvor man aktiv straffer ikke bare borgeren selv, men alle borgerens venner, samarbejdsrelationer og familie, hvis borgerens adfærd ikke er som et-parti systemet ønsker.

I Danmark finder vi i varierende grad tilsvarende modeller også indenfor Justitsministeriet selv – selvfølgeligt alle skabt med positive formål som hovedmotiv, men uden at tage højde for de indbyggede negative eksternaliteter. Generelt vil midlernes destruktive effekter overstige problemerne – kuren er meget værre end sygdommen og man overvejer end ikke lovlige og samfundsgavnlige alternativer (se nedenfor og ”Nye Digitale Sikkerhedsmodeller”).

Det er i dag gået så vidt at man kan høre en dansk Justitsminister udtale fra Folketingets talerstol at ”Overvågning skaber frihed”, hvilket er en rendyrket usandhed. Det er rigtigt at bekæmpelse af kriminalitet er en del af enhver frihedsforståelse – men det er ikke sandt at overvågning er nødvendigt for at bekæmpe kriminalitet. Ikke mindst fordi det kommercielle og kriminelle misbrug af overvågning for længst har oversteget den kriminalitet, man stopper og kunne forebygge med bæredygtige midler. Det er kort sagt dårlig governance.

I ovenstående eksempler kan det være vanskeligt at skelne mellem modellernes bias, ideologiske (vrang)forestillinger og manglende teknisk viden om bæredygtige alternativer, men de bygger alle

på en stadigt mere ekstrem overvågning og magtkoncentration i direkte strid med GDPRs grundprincip om data minimering i henhold til state-of-the-art.

Gentager for at fjerne enhver illusion om det modsatte – ovenstående siger IKKE at det f.eks. er et valg mellem at bekæmpe kriminalitet eller andre frihedsrettigheder, men at tilsyneladende modsatrettede legitime samfundshensyn (som defineret af Folketinget) oftest kan håndtere med et mere nuanceret design uden at gå på kompromis.

Et simpelt eksempel er såkaldt ”Negative Beviser” som generelt eksempel – f.eks. en jobansøger kan med et rigtigt formateret kryptografisk bevis fra Rigspolitiet dokumentere at tilhøre gruppen af ”Ikke dømt for noget, der ville forhindre xx” uden at måtte identificere sig (skabe persondata i cloud ansøgningssystemet og danne grundlag for diskrimination) eller fortælle politiet direkte eller indirekte hvad et sådan kryptografisk bevis skal bruges til.

Tilsvarende kan man altid erstatte f.eks. biometrisk overvågning eller ulovlig logning med modeller som ”plukker nålen ud af høstakken” i form af f.eks. betingede beviser, som kan åbnes af f.eks. en dommer i en vis periode.

Mere avancerede eksempler er SmallData eller Tillidsskabende Registerforskning, hvor man reelt anonymt uden at skabe eller være afhængig af allerede skabte persondata kan forske på tværs af datakilder, dvs. uden den intime og sikkerhedsdestruktive profiling, som i dag sker i f.eks. Danmarks Statistik, Forsker Service eller det utal af andre sammenhænge, hvor man sammenkøre persondata udover det direkte formål.

Fejldesign af operationelle systemer

Hovedproblemet er at man forsøger at løse reelle sikkerhedsproblemer med juridiske undskyldninger (om ”proportionalitet”, hensynet til ”fællesskabet” eller påstande om ”nødvendighed for at opnå xx hensyn”) uden at analyse de negative eksternaliteter eller overveje ofte pareto bedre alternativer.

Stort set samtlige offentlige pg samfundsmæssige it-projekter de sidste 15 år ville afspejle mindst et af nedenstående klare fejl med skade på samfundet til følge. I mange tilfælde skyldes det at it-systemet designes med afhængighed til andre it-systemer eller dårlige it-standarder med indbyggede fejl, dvs. så mere grundlæggende infrastrukturelle it-systemer skaber enten skaber masser af følgefejl og problemer andre steder eller også påføres disse kompenserende meromkostninger som kunne være undgået.

1. Den grundlæggende identitetsmodel er forældet

Som udgangspunkt bør man være bevidst om at selve CPR-systemet er forældet og ikke-interoperabelt til kravene og sikkerhedsbehov i en digital verden.

Når man gennemtvinger koblingen til CPR-nummer i en digital transaktion, så skaber man persondata i sammenhænge, hvor det næsten altid ville være legalt, sikkerhedsmæssigt og samfundsøkonomisk mere hensigtsmæssigt at skabe kontekstuelle nøgler, så man kan tilpasse sikkerhedsdesignet til formålet.

Pointen er ikke at man skal eliminere struktur til f.eks. forskning og genbrug af data. Men at dette ikke bør fastlåses i en ufleksibel identitets-forståelse, som ikke kan tilpasses eller sikres.

Denne grundlæggende fejl om løsning til en CPR-forståelse på laveste niveau skaber problemer overalt i både den offentlige sektor og civilsamfundet. Modellen bør opgraderes til en flerlags identitets-forståelse, hvor man som udgangspunkt altid arbejder med ikke-informationsbærende sessions- og transaktionsnøgler med udgangspunkt i under borgerens kontrol så vidt det er muligt.

I dag laver man ulovlig overvågning af alle og kaster borgerne identificeret for ulvene (både kommercielle, kriminelle og andre) med de helt umulige ePrivacy regler for ”cookie-popup”. Men det er indenfor for Danmarks magt og ansvar at ændre dette - i morgen kunne man digitalt klæde borgeren på til at eliminere overvågning og samtidig fokusere på sikkerheden mod kriminalitet med langt højere grad af nuancer.

En pseudonym signatur i eIDAS-forståelse indebærer i Danmark at man eksplicit kryptografisk eller på anden vis validerer strukturen i forhold til det danske CPR-grundregister på transaktionstidspunktet forhold til det specifikke formål.

En pseudonym signatur er forudsætningen for at vi kan sikre og effektivisere end-to-end uden at cloud-processerne dataadgange bliver legalt og sikkerhedsmæssigt personhenførbare.

Det betyder f.eks. at borgeren PÅ SAMME TID OG I SAMME TRANSAKTION skal kunne være trustworthy anonym i nettet overfor tredjepart og den kommecielle infrastruktur, specifikt valideret i en cloud-applikation til en bestemt transaktion og samtidig f.eks. en sagsbehandler såsom egen læge have merviden om den konkrete transaktion. f.eks. i forbindelse med en online konsultation.

I forhold til f.eks. infrastrukturen betyder sikring af borgerne, når de går på nettet, både et krav om reel anonymitet for at beskytte mod kommerciel (specielt beskyttelse mod BigTech) eller kriminel overvågning, samt en validering af en identitet i forhold til en generelt politisk besluttet ansvarlighedsmodel givet det kontekstuelle formål.

Du ønsker f.eks. ikke at ansvarlighedsmodellen indebærer ulovlige logning som KAN annullere anonymiteten i SmitteStop. Tilsvarende skal det være muligt at tilgå landets love, domsafgørelser og lovsforslag under behandling (Folketinget.dk) reelt anonymt, dvs. NOGLE digitale transaktioner skal upfront kunne holdes helt uden for et ansvarlighedskrav (formålsspecifikt godkendt anonymitet på applikationsniveau). Sådanne balancer er både mulige og nødvendige, men ikke med de strukturer og tilgange, man arbejder med i dag.

Man skal f.eks. kunne håndtere reelt anonyme digitale applikationsprocesser, hvor det er nødvendigt med en form for godkendelse (spørgeskemaer, søgning på politisk indhold etc.), specifikt tilpassede sikkerhedsmodeller (a la SmitteStop adgang til backend-databaser, som bør være reelt anonyme, men valideret i forhold til formålet) og arbejde med en generel default for udefinerede adgange til nettet, der afklares efterfølgende.

En sådan model ville samtidig hæve niveauet for CyberSecurity betragteligt på flere planer på samme tid. Forebyggende kryptografisk validering uden mulighed for overvågning ville gøre det næsten umuligt for cyberkriminelle at komme ind – og selv hvis de kom ind ville angreb ikke kunne skalere over i andre systemer. Samtidig ville f.eks. Center for CyberSecurity overvågning kunne detektere og aktivt gribe ind overfor virusangreb uden at opsamle person- eller virksomheders kundedata.

2. Sikkerhedsmæssige flaskehalse, som tvinger identifikation i infrastrukturen

Denne generelle forståelse er i dag ikke indbygget. Af samme årsag har Danmark gennem specielt de sidste 10-15 år opbygget en helt stribe af sikkerhedsmæssige flaskehalse i infrastrukturem

Her kan man i flæng nævne NemId, MitID, Borger.dk, Sundhed.dk, NemLogin og Digital Post, men også f.eks. Landspatientregisteret som et af de infrastrukturelle baggrundsystemer, hvor man aldrig har overvejet sikkerheden tilstrækkeligt.

Disse systemer skaber alvorlige sikkerhedsproblemer (f.eks. kriminelle har nemt ved at angribe NemId) og persondata uden grund (f.eks. gennemtvinger NemId mulighed for tredjeparts opsamling af persondata i digitale processer), fordi de arbejder identifikationsbaseret uden nuancer.

Samtidig blokerer de for trustworthy sikre alternativer a la de pseudonyme processer beskrevet ovenfor. F.eks. er det i dag ikke muligt at få sikker adgang til resultatet af en Covid-19 test uden at lække sensitive persondata overalt i processen. Den kunne være Trustworthy Anonym, dvs. låst til en bestemt borger med en pseudonym signatur via biometri etc. men uden at selve prøven og prøve resultatet kan henføres til CPR-nummer af andre end borgeren selv.

Effekten er at den danske digitale infrastruktur er sikkerhedsmæssigt og legalt forældet på nederste niveau selv om man længe har vidst at dette ville skabe problemer. Nye Digitale Sikkerhedsmodeller fremhævede allerede i 2010 problemet med at man ikke kan sikre persondata i cloud. Alligevel har man skabt stukturer så ALLE digitale processer med borgerne skaber persondata overalt.

Det kan blive meget værre. F.eks. er man i færd med at ødelægge hele betalingsområdet med en næsten hysterisk tilgang til anti-money-laundering, hvor man ensidigt fokuserer på totalovervågning og BigData registersamkøring af betalingstranskationer frem for at tænke sikkerhed og marked. AML er et reelt problem og håndteret ekstremt bureaukratisk (som i 5-10 mia ekstra bureaukrati om året bureaukratisk), men hvis man skal løse problemerne uden at drukne babyen i badevandet, så skal man forebygge med pseudonyme signaturer på samme måde som telekommunikation ovenfor.

Hvis man vil vide mere om en konkret transaktion for at kunne afgøre om det er en legitim transaktion uden at ødelægge markedsdannelsen, så skal man isolere transaktionen fra andre transaktioner og lade borgeren overføre relevante beviser (GDPR artikel 20 ”Data Portabilitet”)[3].

3. Dårlige kommunikationsløsninger som skaber pesondata uden grund

Problemerne er ikke slut med ePrivacy og den direkte digitale infrastruktur. Ser man på de underliggende strukturer i det trådlåse rum og lokale rum vælter det med tilsvarende problemer.

5G er således designet uden forståelse for behovet for at sikre de digitale processer, fordi man i standarden har hardkodet de kommercielle krav om digital identifikation af trådløse devices, hvorved al trådlåse teleinfrastruktur indebærer overvågning dybt ind i private borgeres hjem, virksomhedernes interne processer og f.eks. statens interne processer. Kritikken af f.eks. Huawei burde gælde alle leverandører af 5G – ikke kun de kinesiske.

3 http://citizenkey.dk/doc/CitizenKey_AML_Automatisering_20191210.pdf

Men i dansk sammenhæng gælder det også f.eks. telemedicin og de reelt ulovlige digitale El-målere, som er under udrulning, hvor man på trods af bedre vidende end ikke har forsøgt at data minimere og sikre processerne. Her kan f.eks. henvises til det såkaldte ITS Notat[4] (som blev trukket tilbage i sidste sekund uden forklaring – formentlig grundet kommercielle interesser).

4. Udenlandske problemer som importeres uden kompenserende tiltag.

Det er klart at store dele af problemerne kan henføres til importerede problemer, specielt relateret til BigTech og dårlige infrastruktur-standarder. Såsom mobiltelefoner, app-stores, EMV-betalinger, 5G – som næsten alle kan henføres til US BigTech interesser, der virker aktivt markeds- og samfundsforvridende i deres systematiske opsamling af persondata. Som påvist, så kan Nationalstaten neutraliserer mange af disse problemer, men det kræver en del og meget bevidste tiltag.

5. Ensidig tilgang til sekundær databrug

De voldsomme sekundære interesser i persondata har i Danmark stort set eroderet alle borgerrettigheder til fordel for systematisk identifikation og registersamkøring. Dette kobles med letkøbte retoriske påstande om ”borgernes tillid” og at man ”passer på data”.

Problemet er at den manglende alternativforståelse gør det til en loose-loose model, hvor stadigt flere område møder konkret modstand. F.eks. når skolebørn begynder at lyve fordi Trivselsmålingerne er designet som overvågningsmodeller. Eller når praktiserende læger får problemer med relationen til patienterne (fortæller ikke lægen sandheden, lægen må undlade at notere eller f.eks. medicin såsom antabus etc. registeres under et andet navn), fordi deres journalsystemer indrapporteres.

Med pseudonyme signaturer og såkaldt ”anonyme akkreditiver” kunne man løse disse trade-ofs uden at gå på kompromis. Problemet er at dem, som skal træffe beslutningerne, ikke mærker konsekvenserne og dem, som mærker konsekvenserne, har typisk ingen indflydelse.

Om Citizen First / CitizenKey:

CitizenKey[5] er baseret på næsten 20 års dedikeret forskning i en erstatning til PKI modellen baseret på blinded kryptografi (U-Prove). CitizenKey er designet til at løse et af den digitale samfundsmodels tungeste og mest komplekse problemer ved at implementer Trustworthy Identiteter og Trustworthy Data Deling i en stærkt distribueret peer-to-peer model uden man-in-the-middle strukturer. CitizenKey er baseret på Privacy / Security by Design og introduktion af et biometrisk borgerkort, som kan erstatte alle eksisterende kort og identitsmodeller samtidig med en gradvis opgradering, som opbygger nye formålsspecifikke identitet tilpasset de konkrete behov

CitizenKey vil blive stillet til rådighed for alle danskere på non-profit basis via en ny non-profit social-økonomisk forening ”Citizen First”, der finansieres af en lille andel af de store besparelser og samfundsbevinster. Citizen First skal være selvfinansierende og velgørende med fokus på finansiering af fri relateret forskning.

4 https://blog.privacytrust.eu/public/Reports/ITS_notat_v0_99.pdf

5 Gennemgang af CitizenKey https://www.youtube.com/watch?v=AVKaXs_I75Y
Slideset http://citizenkey.dk/doc/CitizenKey_AML_Automatisering_20191210.pdf
Opgradering til at håndtere Covid-19: http://citizenkey.dk/doc/Sundhedskort_med_indbygget_CitizenKey.pdf

Bilag – skema

Konkret beskrivelse af problemstillingen	Hvilken databeskyttelsesretlig regel knytter problemstillingen sig til?	Hvilke databeskyttelsesretlige overvejelser har man gjort sig som led i løsningen af problemstillingen?	Har problemstillingen været drøftet med en DPO? Hvad blev resultatet af drøftelsen?
Manglende Pseudonyme Signaturer umuliggør Privacy/Security by Design	eIDAS artikel 5 (Koblingen mellem Digitale Signaturer og GDPR)	Udarbejde af generel løsningsmodel – CitizenKey – som gør GDPR Compliance let samtidig med at det styrke datadelingen. Eksempel på et kritisk område er anonyme bio-prøver og anonym sundhedsforskning	Generel stærk opbakning i DPO-kredse, men de har ingen ressourcer eller kræfter. Sekundære interesser dikterer løsninger. F.eks. kunne det erstatte Ulovlig logning med win-win strukturer
Manglende data minimering National Genom Center	GDPR artikel 5.1.C og 25 Data Minimering i henhold til teknologiens aktuelle stade	Konkrete Privacy by Design løsningsmodeller præsenteret med konkrete fordele. F.eks. National Genom Center kan gennemføres reelt anonymt	Flere DPO'er rapporterer at det er næsten umuligt at få opmærksomhed på problemet grundet de stærke interesser i sekundær udnyttelse af persondata.
Manglende Data Portabilitet. 1. I Danmark kan borgerne kun få adgang til egne data via centrale overvågningsportaler (Sundhed.dk, Borger.dk) 2. Borgerne ikke få en struktureret kopi af egne data til Trustworthy genbrug	GDPR artikel 20	Udarbejde Citizen-Centric Once Only, som indebærer at borgeren kan dele data uden at afgive kontrollen. Mulighed for at bevise aspekter af identitet uden at identificere. Effektive synergier	Flere DPO'er har sagt det ville gøre deres arbejde meget lettere, hvis borgeren selv kan dele data.
BigData AI indebærer deterministisk overvågning og profilering af borgere i en selvforstærkende process Alternativet er SmallData	GDPR artikel 25	I stedet for den forældede CPR-baserede opsamling og registersamkøring med efterfølgende "pseudo-anonymisering, så kan man give borgeren værktøjer til SELV at sammenstille data og dele data anonymt til sekundært brug (data portabilitet). Ville skabe pareto bedre løsninger til forskning, markedsføring, AI m.m. uden at gå på kompromis.	DPO enig, men kan ikke få opbakning i organisationen, fordi det er nemmere at ignorere sikkerheden og bare sammenkøre. Ingen har og ingen vil tage ansvaret for overholdelse af lovgivningen. Konsekvenserne af skaderne ikke rammer dem som får de direkte fordele af tvang og registersamkøring.