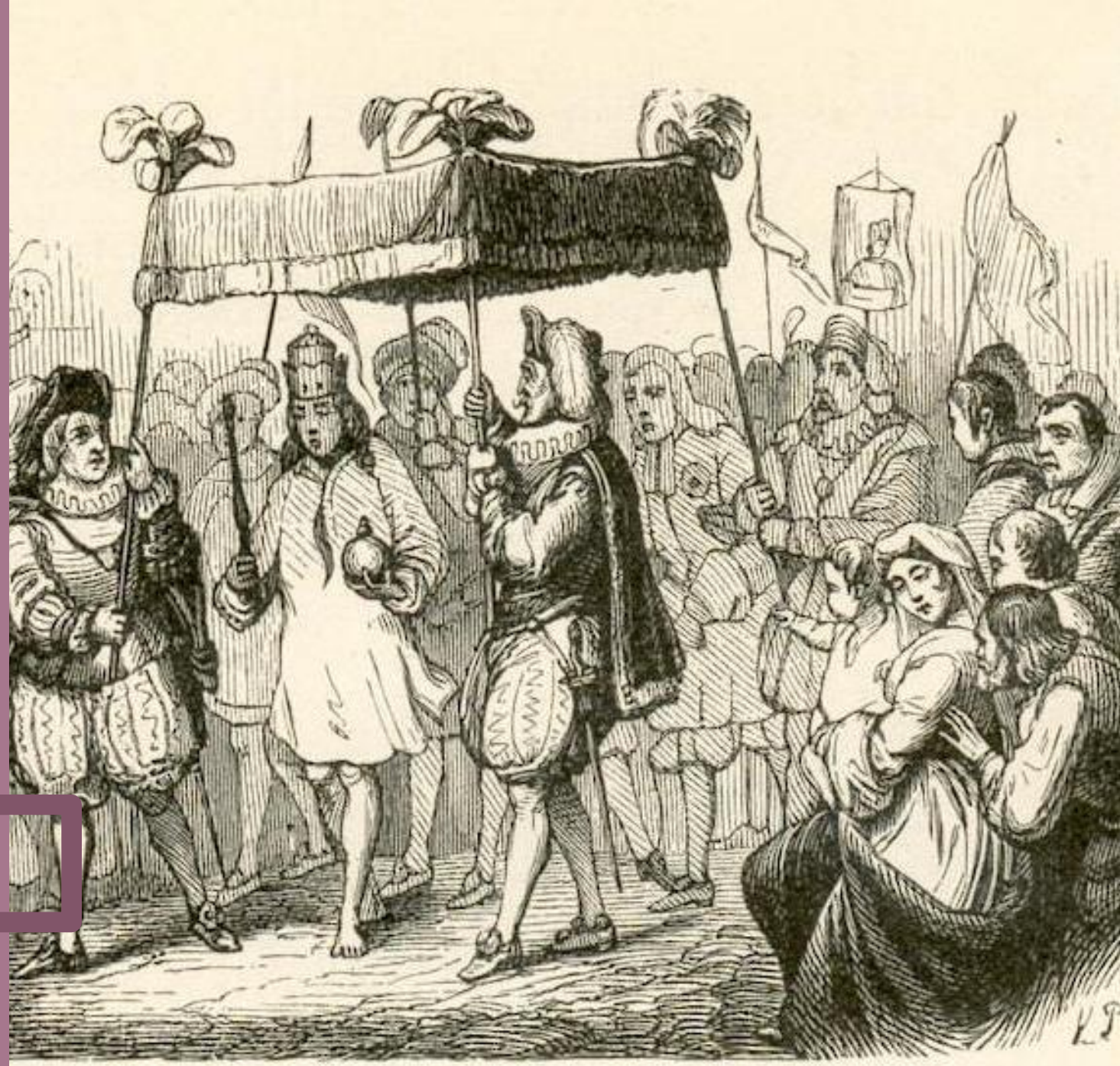
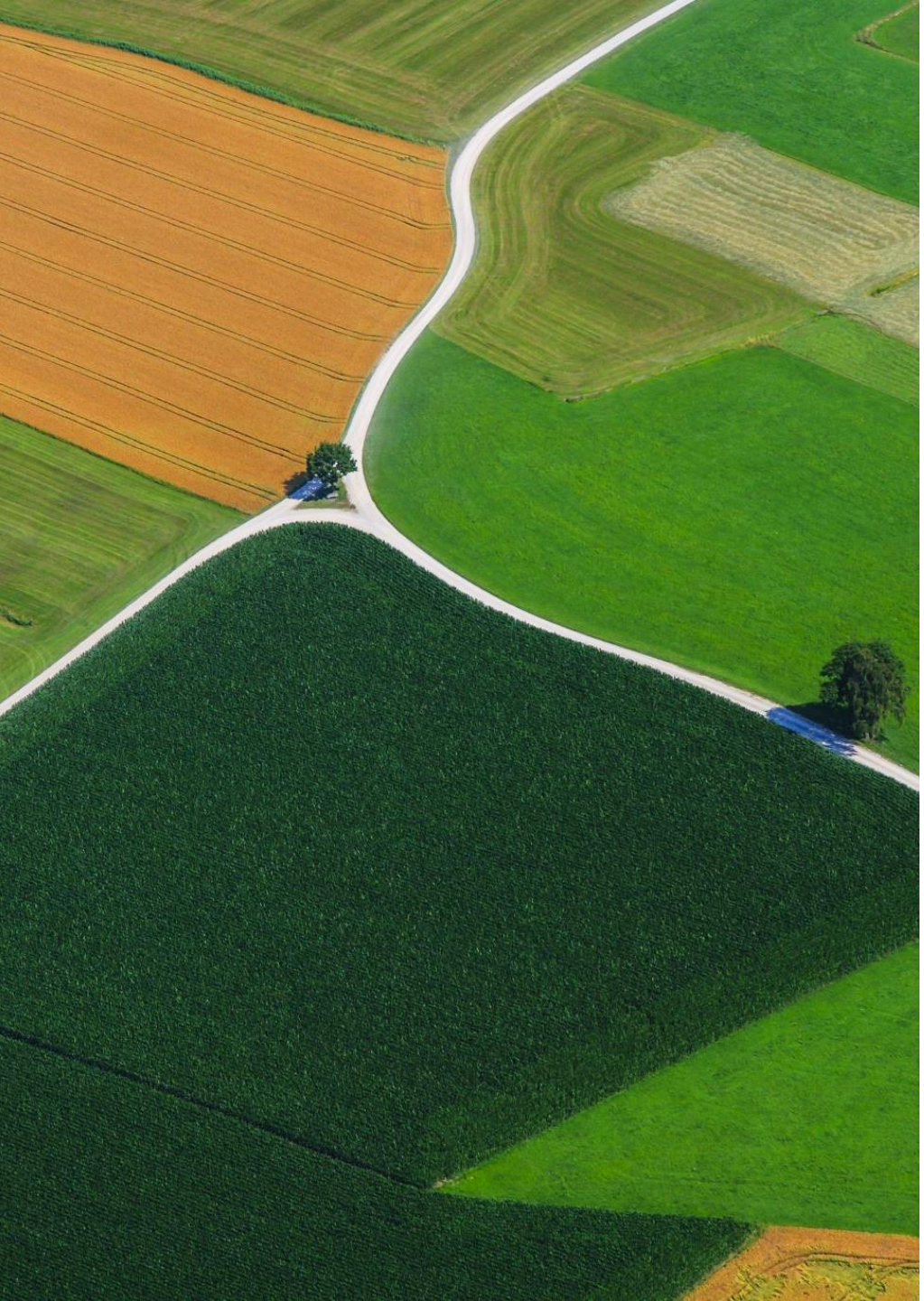
Hvorfor overholder MitID ikke dataminimeringskravet i GDPRs artikel 25, stk. 1?

Oplæg ved Stud.jur. Mona Heide Petersen

Ekspertbistand ved
Digitaliseringsekspert – og sikkerhed
Cand.merc.dat. Stephan Engberg

Eller: hvorfor har kejseren ikke noget tøj på?





Påstand:

- Den danske stat – de danske myndigheder m.fl. – krænker hver dag, året rundt, millioner af danskeres persondatarettigheder.
- Dette gør de, fordi MitID, den monopoliserede kritiske infrastruktur, som omkring 5.000.000 danskere bruger mange gange hver dag, i sit design forhindrer dataminimering som foreskrevet i GDPR-forordningen.
- GDPR-forordningen udspringer af EU's charter om grundlæggende rettigheder: det er således danskernes mest grundlæggende rettigheder der krænkes og misbruges af den danske stat. Hver dag. Året rundt. Siden 2021.

En kort introduktion til gældende persondataret i Danmark

EUs charter for grundlæggende rettigheder

Det Europæiske Råd besluttede i juni 1999 at udforme et charter om grundlæggende rettigheder, hvad angår bl.a. frihed, lighed, solidaritet, unionsborgerskab og retfærdighed.

I forbindelse med Lissabontraktatens ikrafttrædelse den 1. december 2009 blev charteret juridisk bindende via en henvisning til det i EU-traktaten TEU art. 6.

Unionen, der er sig sin åndelige og etiske arv bevidst, bygger på de udelelige og universelle værdier: menneskets værdighed, frihed, lighed og solidaritet; den bygger på demokrati- og retsstatsprincippet. Den sætter mennesket i centrum for sit virke med indførelsen af unionsborgerskabet og skabelsen af et område med frihed, sikkerhed og retfærdighed.

EUs charter (og EMRK) fortsat

- Den Europæiske Konvention til beskyttelse af menneskerettigheder og grundlæggende friheder blev vedtaget i 1950, men ekspansionen af EU's kompetencer til politikker med direkte indflydelse på de grundlæggende rettigheder, betyder, at EU's værdier skal være klart definerede. EU's charter om grundlæggende rettigheder trådte i kraft med Lissabontraktaten d. 1. december 2009. Den er bindende ved lov i hvert EU-medlemsland.

Hvad er GDPR?

- EU's generelle forordning om databeskyttelse (GDPR) blev vedtaget i 2016 og trådte i kraft i maj 2018.
- GDPR er en forordning, det vil sige, at det er bindende EU-retlig sekundærregulering.
- GDPR har både horisontal og direkte virkning i Danmark, derfor kan borgere i Danmark påberåbe sig GDPR over for staten og en anden borger.
- GDPR har til formål at regulere alle væsentlige spørgsmål om databeskyttelse og gøre dette på en måde, der medfører ensartethed i EU-medlemsstaternes persondataretlige regulering.

Hvad er GDPR II

- GDPR kan som følge af ovenstående karakteriseres som den centrale retskilde i dansk persondataret.

Forbindelsen mellem EU's charter og GDPR

Chartrets nærmere betydning for dansk persondataret fastslås i præambelbetragtning 4 i GDPR, efter hvilken GDPR skal overholde chartret.

Når chartret anvendes, skal det altid læses på baggrund af chartrets artikel 52, som fastsætter rækkevidden af chartrets rettigheder og principper og fortolkningen af dem.

EU-domstolen fastlægger med bindende virkning EU-rettens indhold, herunder ikke mindst regler og rettigheder som fastsat i GDPR og chartret.

Nødvendighedskriteriet – et EU-retligt princip

- Foranstaltningen skal være nødvendig i forhold til målet. Ved valgmuligheder skal man vælge den mindst bebyrdende foranstaltning for borgeren, jf. fx GDPR's artikel 25, stk. 1 state-of-the-art/det aktuelle tekniske niveau vedrørende design.
- I forbindelse med artikel 25 forpligter "det aktuelle tekniske niveau" dataansvarlige til at tage hensyn til **eksisterende teknologiske fremskridt, der er på markedet***
- Af artikel 25, stk. 1 følger, at den ansvarlige datacontroller altid har dokumentationsforpligtelsen i henhold til at overholde nødvendighedskriteriet og dataminimeringskravet.
- https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_da.pdf, p. 9

Hvad kan et pseudonym fx være:

Folketingsvalg, illustration:

- Man går anonymt ind i stemmeboksen
- Man identificeres (ved stemmebordet inden), men beviser kun data selektivt uden at blive identificerbar (selve stemmen). Stemmesedlen er et engangs-"pseudonym"
- Hvis regeringen kan identificere oppositionen, fortabes valgets formål som er at sikre fredeligt magtskifte, hvis flertallet skifter. Magten må ikke kunne forhindre magtskiftet ved at oppositionen kan forfølges.

Link til EU-høring om GDPR

- Have you say: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14054-Report-on-the-General-Data-Protection-Regulation_en

Konsekvensanalyse

- GDPR's artikel 35, stk. 1, konsekvensanalyse (at undersøge konsekvenserne ved designet):

- "Hvis en type behandling, navnlig ved brug af nye teknologier og i medfør af sin karakter, omfang, sammenhæng og formål, sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, foretager den dataansvarlige forud for behandlingen en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger. En enkelt analyse kan omfatte flere lignende behandlingsaktiviteter, der indebærer lignende høje risici".

GDPRs artikel 23

”EU-ret eller medlemsstaternes nationale ret, som den dataansvarlige eller databehandleren er underlagt, kan ved lovgivningsmæssige foranstaltninger begrænse rækkevidden af de forpligtelser og rettigheder, der er omhandlet i artikel 12-22 og 34 samt artikel 5, for så vidt bestemmelserne heri svarer til rettighederne og forpligtelserne i artikel 12-22, når”[…]

Dette betyder modsætningsvist, at fx GDPR’s artikel 25, stk. 1 aldrig kan fraviges.

Ulovligheder….

- Jf. GDPR's (meget vigtige) artikel 23, stk. 1 betyder det i klartekst at: hvis man – de danske myndigheder - henviser til en (sektor)-lov eller en bekendtgørelse for at påstå hjemmel til at ignorere dataminimeringskravet og/eller nødvendighedstesten, så henviser man til en ulovlig lov. Og uden en forfatningsdomstol, kan vi ikke teste kvaliteten af vores love.

GDPRs artikel 25, stk. 1

- Under hensyntagen til det aktuelle tekniske niveau […]
- gennemfører den dataansvarlige både på tidspunktet for fastlæggelse af midlerne til behandling og på tidspunktet for selve behandlingen passende tekniske og organisatoriske foranstaltninger, såsom pseudonymisering, som er designet med henblik på effektiv implementering af databeskyttelsesprincipper, såsom dataminimering […]
- med henblik på integrering af de fornødne garantier i behandlingen for at opfylde kravene i denne forordning og beskytte de registreredes rettigheder

Grundlæggende forvaltningsretligt princip

”Desto hårdere en retsakt rammer private interesser, desto mere må forvaltningen – fx staten – sikre sig, at en retsfølge ikke går videre end nødvendigt for at opfylde det lovlige formål. Hvis der er tale om et indgreb i en fundamental rettighed […] skal det nøje overvejes, om mindre indgribende midler i tilstrækkelig grad vil kunne fremme formålet”.

Underimplementeres GDPR i Danmark, side 8

Forvaltningsretligt princip, fortsat

- "Behandlingen af personoplysninger vil i denne sammenhæng være at betragte som et indgreb i en privat interesse, der karakteriseres som en fundamental rettighed".

- Underimplementeres GDPR i Danmark, side 8

eIDAS-forordningen 2016

- eIDAS-forordningen (Forordningen om elektronisk identifikation og tillidstjenester) implementeres i Danmark i 2016.
- Den danner baggrunden for udviklingen af den nye National Standard for Identiteters Sikringsniveau (NSIS), som Digitaliseringsstyrelsen har i høring i denne periode.
- eIDAS skal som udgangspunkt sørge for, at
- "virksomheder, borgere og offentlige myndigheder hjælpes med at gennemføre sikre og gnidningsløse elektroniske interaktioner", "ansvarlighedsbevis".

- Kilde: https://digital-strategy.ec.europa.eu/da/policies/eidas-regulation

Tidligere: Konflikt mellem eIDAS og GDPR

- eIDAS skal tilvejebringe et grundlag for aftaler, der kan tryktestes i en retssag. Det har den konsekvens, at fokus let bliver på at skabe personhenførbare data.
- GDPR: har til formål at beskytte og minimere skabte persondata og ultimativt at sikre, at der *slet ikke skabes persondata*.
- = Derfor har der været en kontradiktion, et modsætningsforhold, mellem de to forordningers kerneanliggende

Men så kom NemID-erhverv

- NemID-erhverv:
- Designet så en medarbejder kunne logge på med et pseudonym som en rolle: virksomheden er identificeret, men medarbejderen er unavngiven (x-medarbejder i rollen som yy fra det navngivne-firma)
- NemID-erhverv overholder eIDAS artikel 5, stk. 1: (Som siger at GDPR skal respekteres)
- NemID-erhverv overholder GDPR's artikel 25, stk. 1 (som statuerer dataminimering i standardindstillinger jf. state-of-the-art, dvs. teknisk mulige bedste stade)
- NemID bringer (næsten) harmonisering mellem eIDAS' artikel 5, stk. 1 (GDPR skal respekteres) med GDPR's artikel 25, stk. 1 (Dataminimering)
- eIDAS artikel 5, stk. 2: hvis der kan skabes pseudonyme data, så må brugen af disse ikke forhindres.

Opsamlende pointe

- GDPR kræver, at man skal dataminimere jf. state-of-the-art. Dette krav gælder også i eIDAS, da eIDAS (artikel 5, stk. 1) eksplicit er underlagt GDPR.
- I klartekst betyder dette, at modparten **skal** acceptere en pseudonym signatur. Modparten må ikke uden hjemmel kræve identifikation ud over pseudonymiteten*.
- Ovenstående krav kunne NemID-erhverv næsten imødekomme.
- *Se fx den nye eIDAS 2.0, hvor retten til pseudonymitet understreges.

MitID

MitID blev udrullet i Danmark i 2021. MitID er en SSO (en single-sign-on)-løsning i modsætning til fx NemID, som var en certifikatstyret signatur, som man som borger kunne kontrollere med papkortet

I MitID-designet er papkortet udgået: det var den eneste nøgle som borgeren "kontrollerede".

Man kan tilvælge et Chip-kort som fungerer som "password" med en nøgle som MitID ikke kender og/eller et kodedevice som skaber tids-afhængige koder, synkroniseret med en server.

Men denne løsning er ikke default. Den giver en smule mere sikkerhed ift., hvem der er logget ind, men det giver stadig ingen persondatabeskyttelse.

MitID datamaksimerer

MitID kan kun logge på en central server

MitID forhindrer dataminimering jf. GDPR's artikel 25, stk. 2 og GDPR's artikel 32, stk. 1a, da sessionen pr definition bliver identificeret

Der skabes uundgåeligt persondata, da der ikke er nogen mulighed for pseudonyme/trustworthy signaturer

SSO-teknologien fører til ulovlig logning (Man-in-the-middle-data-retention)

Hvis man ikke kan dataminimere, fordi MitID i sit tekniske design som udgangspunkt er programmeret til at datamaksimere, så forstøder hele MitID grundlæggende mod GDPR-artiklerne 25, stk. 1 og 2, og 32, stk. 1a

MitID (Edited)

Som tidligere nævnt følger det af nødvendighedsprincippet, at behandling af personoplysninger aldrig må omfatte mere end, hvad der er strengt nødvendigt til formålet

Artikel 5, stk. 1 i eIDAS siger, at GDPR skal respekteres

Artikel 25, stk. 1 og Artikel 32, stk. 1 i GDPR kan som nævnt ikke fraviges jf. GDPR artikel 23, stk. 1

Det vil i klartekst sige, at hvis staten kan lave tilstrækkeligt sikre løsninger, *så er staten også forpligtet til at gøre det.*

Fx à la den løsning der fandtes med NemID-erhverv

- Men han har jo ikke noget tøj på! (Edited)

- Fordi: MitID ikke overholder dataminimeringskravet jf. GDPR's artikel 25, stk. 1
- Fordi: MitID ikke overholder artikel 5, stk. 1 eller stk. 2 i eIDAS
- Fordi: den danske stat kunne have designet ligesom "best case eksemplet på et "trusted pseudonym«- signatur, NemID-Erhverv (og det skal den gøre, fordi den kan)
- Men det har den danske stat ikke gjort


PAUSE

Hvad betyder statsadministrationens ageren ift. befolkningens tillid?

- Hvad er konsekvenserne af, at MitID forhindrer beskyttelse af vores persondata?
- Dårlig cybersecurity
- Big tech opsamler en masse data om borgerne, herunder især om børn under 18
- Supercentraliseringsfokus skaber ineffektiv monopolisering: one size fits all: hindrer konkurrence, alternativer, skaber top-down mekanisme.

Afledte konsekvenser af misbruget af persondata (edited)

- Påstand: Den danske stat skalter og valter med borgernes personfølsomme data
- https://www.version2.dk/artikel/styrelse-gentager-ulovlig-praksis-sundhedskort-app-hoester-data-om-millioner-af-danskere-uden
- Dansk genom-center - https://sciencereport.dk/samfund/snart-kan-danskerne-ikke-fravaelge-at-dele-deres-gen-data-med-staten/
- SSI: https://www.dr.dk/nyheder/indland/blodproever-fra-danske-gravide-blev-floejet-til-usa-i-strid-med-reglerne-nu-vil
- Gladsaxe-modellen - https://www.version2.dk/artikel/gladsaxe-modellen-spoeger-nyt-ai-projekt-skal-forudsige-mistrivsel-hos-boern
- AI-model til forudsigelse af danskernes død - https://www.dtu.dk/english/newsarchive/2023/12/artificial-intelligence-can-predict-events-in-peoples-lives (Registersamkørsel)
- Udbetaling DK: https://justitia-int.org/wired-how-denmarks-welfare-state-became-a-surveillance-nightmare/ (Registersamkørsel)
- Markedsføring af salg af borgernes sundhedsdata til udlandet: https://investindk.com/insights/new-national-danish-research-health-data-gateway-assists-researchers-with-accessing-data

https://edps.europa.eu/data-protection/our-work/ipen/ipen-workshop-digital-identity_en, Stephan Engberg

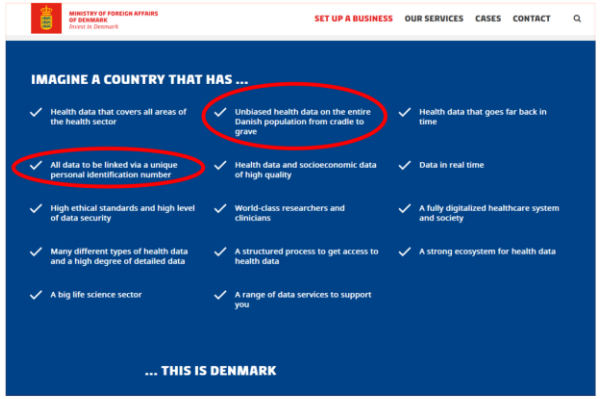
Our own institutions are killing democracy
The case of Denmark

Allways linkable Identified
100% Data Retention & BigData
MitID with serverside face recognition
Telco must force identification

Zero security
Mandatory central profiling
No attention to exponential damages

Secondary agenda drive collapse
Bureaucratic Command & Control
Surveillance Capitalism

.. Trustworthy PKI change that
Better solutions without eID Data Retention
Trustworthy Anonymity INSIDE eGov



5 minutters summer i små grupper, herefter opsamling i plenum

- 1) Hvad er I mest nervøse over i forhold til den ulovlige digitalisering?

- 2) Hvad kan vi som befolkning gøre: på individplan, på råd/forenings/organisationsplan

- 3) Politisk, strategisk ift. at genoprette den fejlslagne digitalisering

Men måske er der alligevel håb: Aligning MitID med EU-digital wallet

- Man kan godt have EU-digital Wallet ved siden af MitID
- Om to år skal EU-digital Wallet være integreret
- Er det de danske myndigheders chance for at rette op på deres ulovligheder?

Næste arrangement hos #Aktive Lyttere

- Catharina Engberg

- Oplæg om hvordan man sikrer børnene i den digitale verden
- Herunder:
- ZafeLoc
- Trustworthy anonym aldersverifikation
- EU-Digital Wallet/CitizenKey