Rådet for Digital Sikkerhed .

9. december 2020

Rådet for Digital Sikkerheds positionspapir

Der findes stigende mængder af data om os, og mange af de ting vi bruger i dagligdagen (Internet of Things som smart watch, smart TV mv), indsamler data om os. Det stiller krav til behandlingen af data, så behandlingen sker med respekt for privatlivet – fx hvor data enten er anonyme eller ikke personhenførbare. Der findes teknologier som kan bidrage til ansvarlig brug af vores data til gavn for vækst hos danske virksomheder. Der er dog en række barrierer for ibrugtagning. Nærværende vejledning vil beskrive forskellige privatlivsfremmende teknologier (fordele og ulemper) samt give eksempler på anvendelsen af disse teknologier. Vejledningen kommer med anbefalinger til, hvornår det er relevant at bruge af privatlivsfremmende teknologier - fx i offentlige udbud.

Vejledning om privatlivsfremmende teknologier

Udkast

Rådet for Digital Sikkerhed
Vester Farimagsgade 37B, 1.th., 1606 København V
Telefon: +45 53 36 02 23 mail: info@digitalsikkerhed.dk web: www.digitalsikkerhed.dk

1. Baggrund og formål

I Danmark produceres enorme mængder af data. Der indbygges data, i ting vi anvender i hverdagen (Internet of Things – IoT), som så kobles på nettet. Det kan være sensorer i skraldespande, i vores bil eller ur. Teknologien kan på den måde bidrage med effektivitet og værdi fx i forhold til at optimere vores hverdag. Vores data indgår på denne måde i digitale forretningsmodeller, og de kan dermed blive en vare vi kan handle med.

Det stiller krav til håndtering af vores data og retten til privatliv. Retten til privatliv skal dog ikke sætte en stopper for forskning og innovation. Privatlivsfremmende teknologier kan hjælpe med at løse dette dilemma.

Denne vejledning vil beskrive forskellige privatlivsfremmende teknologier[1] (fordele og ulemper) samt give eksempler på anvendelsen af disse teknologier. Vejledningen beskriver teknologiernes funktionalitet på konceptuelt plan. Følgende teknologier gennemgås i vejledningen[2]:

- Zero-knowledge Proofs (ZKP)
- Multiparty Computation (MPC) & Fully Homomorphic Encryption (FHE)
- Differential Privacy (DP)
- Federated Learning (FL)

Formålet med vejledningen er at skabe kendskab til ovenstående teknologiske muligheder og tænke dem ind den digitale udvikling eller regulering af samme.

Vejledningens anbefalinger henvender sig til embedsmænd, som påvirker den nationale digitale dagsorden og vejledningen i sin helhed henvender sig til tekniske rådgivere, der stiller krav til udbud af offentlige it-løsninger (nationalt og kommunalt) og udviklere, som skal designe understøttelse af persondataretlige krav ind i forskellige løsninger.

Dokumentet er struktureret således, at vi gennemgår en række eksempler, hvor privatlivsfremmende teknologier kan skabe værdi. Eksempler er struktureret ud fra forskellige PETs, men disse teknologier præsenteres kun på konceptuelt niveau.

Vejledningens overordnede anbefalinger til embedsmændene fremgår af boksen herunder:

[1] PETs fra det engelske Privacy Enhancing Technologies

[2] Dette er ikke en udtømmende liste af PETs, men giver et indblik i de teknologiske muligheder.

Rådet for Digital Sikkerhed anbefaler, at:

- At både det offentlige og det private benytter privatlivsfremmende teknologier i større omfang – det gør en forskel som senest bevidnet ved debatten og konstruktionen af Smittestop-app'en.
- At myndigheder bidrager til at sikre det juridiske fundament for anvendelsen af disse teknologier og sprede viden om teknologierne
- At Datatilsynet hjælper med vejledning til, hvordan brugen af disse teknologier kan understøtte en lovlig behandling af personoplysninger
- At det offentlige påtager sig en rolle som lokomotiv i forbindelse med sådanne anvendelser fx i forbindelse med offentlige udbud.

2. Hvor er det relevant at bruge privatlivsfremmende teknologier?

Der er mange eksempler på, hvor det vil være relevant at anvende privatlivsfremmende teknologier. Et af dem er *politiets "observationsliste"* over folk, som de gerne vil holde øje med. Politiet ønsker at undersøge, hvorvidt nogen på observationslisten også er på fx flyselskabernes passagerlister, men uden at give observationslisten til flyselskabet. Omvendt ønsker flyselskaberne at beskytte de rejsendes privatliv, og vil ikke udlevere hele passagerlisten til politiet.

Det kunne løses ved at begge giver deres lister til en betroet trediepart, som finder personerne, som er på begge lister, og giver politiet disse navne. Men med smart matematik kan dette udregnes uden en betroet trediepart.

Digitale kontanter: Et af problemerne ved betaling med Dankort, bankoverførsel og MobilePay er, at de efterlader et digitalt spor. Der findes digitale valutaer (fx såkaldte cryptocurrencies), hvor både betaler og modtager er anonyme, hvilket fx gør det sværere at opkræve den korrekte skat. Men der findes også digitale valutaer, som giver mulighed for, at betaler er anonym, mens modtager ikke er anonym. Med andre ord: hvis man ønsker at lave en digital e-krone så vil dette være en mulighed for at beskytte køberens privatliv, men stadig give mulighed for at beskatte sælgeren. Ved digitale penge behøver man altså ikke at vælge mellem 100% identificerbarhed eller 100% anonymitet, men kan man anvende PETs på en måde så både forretnings- og samfundsmæssige hensyn tilgodeses uden at underminere borgernes ret til privatliv.

3. Formålet med privatlivsfremmende teknologier

Privatlivsfremmende teknologier har til formål at beskytte individers data i forbindelse med forskellige anvendelser.

- En bruger kan få adgang til en tjeneste og gennemføre en transaktion uden at identificere sig

- To eller flere parter kan samarbejde om at finde en løsning på et fælles problem uden at kende hinanden og uden at kende de data, de hver især kommer med;
- Der kan ske et opslag hos en tjeneste, uden at tjenesten kan se, hvem der slår op, hvad der slås op efter, og at der overhovedet har været et opslag;
- Man kan bruge aggregerede data, der med sikkerhed ikke kan sige noget om de registrerede, som udgør datagrundlaget.

> Et aktuelt eksempel er tracking af smitte ifbm apps til sporing af Covid-19 smitte. En naiv løsning kunne være at registrere alle brugeres lokation (dvs. deres smartphones lokation) i en stor GPS-database. I stedet blev der faktisk valgt en privacy-by-design-tilgang, der sikrer app-brugernes privatliv i vidt omfang, og på en måde som er i overensstemmelse med GDPR, hvor data som udgangspunkt lagres lokalt og ved deling behandles anonymt.

PETs har længe været relevante, men i forbindelse med EUs databeskyttelsesforordning er det blevet ekstra vigtigt at forstå, hvordan man kan tilgodese både forretnings- og privatlivsperspektivet på en gang. Det er netop det PETs muliggør. Brugen af PETs er f.eks. særlig relevante ved tredjelandsoverførsler og udgør netop nogle af de supplerende foranstaltninger til standardkontrakterne, som EDPB har peget på i deres Recommendation 2020/1[3].

4. Privatlivsfremmende teknologier

Nedenfor præsenteres nogle forskellige privatlivsfremmende teknologier. For at en privatlivsfremmende løsning kan have samfundsmæssig relevans, må den som minimum leve op til følgende kriterier:

- Der findes formelle matematiske beviser for sikkerheden af de underliggende konstruktioner på linje med de garantier, som fx ligger bag NemID
- Der er en gryende kommerciel udbredelse af disse teknologier, som gør, at brugere kan forvente en tilstrækkelig produktmæssig modenhed.

For at forstå, hvorfor formelle beviser er nødvendige, skal man se på den lange række af løsninger uden beviser, som man har troet var sikre. Et udbredt problem er fx re-identifikation af databaser, hvor man har anonymiseret oplagt personhenførbare data ved at erstatte fx cpr-nr med et andet tilfældigt tal.

Artiklen Latanya Sweeny udgav[4]

> Et klassisk eksempel på, hvorfor det fejler, kom i 2002, da Latanya Sweeney udgav en artikel[1], hvori hun beskriver et re-identifikationsangreb på anonymiserede sundhedsdata for 135.000 borgere i staten Massachusetts (USA). Disse data var anonymiserede, men indeholdt korrekt køn, fødselsdato og postnummer. Selvom alle direkte personhenførbare oplysninger var anonymiserede, lykkedes det (let) Sweeney at finde guvernør William Welds journal. Angrebet var simpelt: Sweeney skaffede den (offentlige) liste over registrerede vælgere. I denne liste fandtes seks personer med samme fødselsdato som Weld, tre af dem var mænd og netop 1 havde samme postnummer som guvernøren

3 https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf, Se Annex 2

4 https://dataprivacylab.org/dataprivacy/projects/kanonymity/kanonymity.pdf

3.1 Zero-knowledge Proofs

Zero-knowledge proofs (ZK) er en teknologi, som gør det muligt at overbevise en modpart om forskellige udsagn uden at afsløre selve beviset, det vil sige bevise, at man ved "noget" uden at afsløre, hvad dette "noget" er.

> Et eksempel på dette er historien om "Find Holger" - konsulenten som tjener penge på at hjælpe folk med at løse "gåden" i de kendte Find-Holder-bøger[1]. Konsulentens problem er, at han for en sikkerheds skyld gerne vil betales forud, men hvordan kan kunderne så være sikre på, at han ikke snyder dem. Løsningen er, at konsulenten har et ark papir med et lille hul, hvorigennem man akkurat kan se Holger. Finten er, at arket er så stort (ifht bogen med Holger), at selvom konsulenten viser at Holger er der, så kan kunden ikke regne ud hvor, fordi arket med hullet er så stort, at kunden ikke kan se, hvor bogen er placeret under arket.
> Med andre ord: konsulenten kan bevise overfor kunden, at han kan finde Holger, men selv med denne vished har kunden ikke lært spor om, hvor Holger faktisk er.

Teknikken bag ZK er baseret på arbejde indenfor teoretisk datalogi, særligt kryptografi, som går tilbage til 1980'erne, hvor den først blev forsøgt kommercielt anvendt til elektroniske penge (uden større held).

I 0'erne kom både IBM og Microsoft med de første kommercielle prototyper[5] som bl.a. blev studeret i forskellige EU-projekter. Et eksempel er EU-projektet ABC4Trust, hvor der blev udviklet en løsning til en skole i Sverige, som gjorde det muligt for elever at "chatte" med fx skolens læge under delvist anonymitet. Delvist betyder her, at lægen har haft vished om, at der var tale om en elev på skolen, men ikke hvem[6].

Siden har ZK-teknikker opnået opmærksomhed i kølvandet på udbredelsen af kryptovalutaer og blockchain[7]teknologi. Fx bitcoin-klonen Zcash[8]. En anden privatlivsfremmende-fokuseret blockchain er Concordium, som udvikles i samarbejde med forskere fra Aarhus Universitet.

ZK er en kraftfuld teknik, som gør en lang række løsninger mulige, som umiddelbart virker kontra-intuitive, men teknikken er baseret på formelle matematiske beviser i samme omfang som fx de digitale signaturer som ligger bag NemID.

[5] IdentityMixer og U-Prove

[6] https://abc4trust.eu/download/ABC4Trust-D6.1-Application-Description-School.pdf

[7] En blockchain er liste af elementer som er kædet sammen på en måde som garanterer at alle elementer forbliver uændrede. Typisk realiseres denne garanti vha et distribueret system

[8] https://z.cash/

3.2 Multi-Party Computation & FHE

Multi-Party Computation (MPC)[9] er en kryptografisk teknologi, som gør det muligt at regne på krypterede data.

> Et simpelt eksempel, kaldet Yao's millionærer, går ud på, at en flok rige mennesker gerne vil vide, hvem der er allerrigest – men ingen af dem vil oplyse deres faktiske rigdom til de andre. Ved hjælp af MPC er det faktisk muligt for dem hver især at kryptere deres rigdom, og så udregne netop hvem der er rigest. Matematisk kan det garanteres, at den funktion, der beregnes, ikke afgiver andre oplysninger en netop dette.

Ligesom ZK har MPC & FHE eksisteret teoretisk siden 80'erne, men blev betragtet som uanvendelig i praksis. Dette ændrede sig dog i 2008, da et større dansk forskningsprojekt i et samarbejde mellem kryptologer, økonomer og sukkerroedyrkere afviklede en MPC-baseret auktion. I denne såkaldte dobbeltauktion

> Meget tilsvarende mekanismer benyttes i en løsning fra den danske firma Partisia, som benyttes af japanske Tora til såkaldt off exchange trading af værdipapirer. Anvendelse af krypterede bud giver en meget effektiv beskyttelse imod såkaldt front running. På sigt åbner MPC muligheder for mange innovative løsninger, efterhånden som lovgivere og erhvervslivet får øjnene op for potentialet.
>
> Et eksempel på en anvendelse af MPC er Boston Women's Workforce Council (BWWC), som brugte MPC[1] til et studie i ligeløn i Boston området. De enkelte virksomheder der deltog i undersøgelsen skulle indberette løn aggregeret på køn og jobkategori. For at undgå at virksomheder ikke ville deltage, fordi de ville blive udstillet som evt. dårlige hvad ligeløn angår, blev der brugt MPC, så BWWC kun kunne se resultaterne på tværs af alle virksomhederne og ikke data om en enkelt virksomhed.
>
> Også i Danmark, som er førende indenfor MPC, er der løbende nye MPC-baserede tiltag. Et eksempel er HedaX-forskningsprojektet, som handler om at bruge sundhedsdata på tværs af datakilder, men samtidigt beskytte disse data. Fx arbejdes der på at kunne bruge data fra både Danmarks Statistik og Sundhedsdatastyrelsen, så socioøkonomiske forhold nemmere kan komme med ind i forskning i sundhedsdata, og så man samtidigt ikke går på kompromis med sikkerheden, fordi man ikke skal udveksle data for at kunne lave analyser.

handlede sukkerroedyrkerne EU-kontrollerede produktionsrettigheder, og det unikke ved auktionen var, at alle bud var krypterede; kun i forbindelse med handler, der skulle realiseres, blev budene dekrypteret.

3.3 Differential Privacy

En udbredt gammeldags (og dårlig[10]) teknik til at forsøge at beskytte private oplysninger i større databaser er enten at fjerne oplysninger som navn og cpr-nr, eller erstatte dem med pseudonymer (også kendt som tokenization). Problemet med denne tilgang er grundlæggende, at den er sårbar overfor re-identifikation, dvs. at de resterende oplysninger – evt. kombineret med andre offentligt tilgængelige data – muliggør præcis identifikation af de fleste individer i en sådan database; selvom det umiddelbart virker som om privatlivsbeskyttelse er sikret, så er det ofte ikke.

[9] https://en.wikipedia.org/wiki/Secure_multi-party_computation

[10] Jf. eksemplet fra Massachusetts i indledningen.

Differential privacy (DP) forbedrer dette drastisk ved at give konkrete matematiske/statistiske garantier for, hvor svært det er at udlede oplysninger om et enkelt individ ud fra data i en database. På samme måde som for ZK og MPC gives der således matematiske garantier for de egenskaber, teknologien har.

> Et eksempel på sådan en anvendelse findes hos den amerikanske virksomhed Apple, som har udviklet en løsning til at indsamle viden om brugen af deres smartphone[1]. Ideen er, at Apple kan lære fx hvilke hjemmesider der tærer mest på en telefon, uden at lære noget om den enkelte brugers opførsel.

På samme måde som i dette eksempel muliggør DP, at der kan opsamles aggregerede data om individer på en måde, hvor der kan gives matematiske garantier for graden af privatlivsbeskyttelse. Dette sikrer imod naive fejl, som typisk begås, når man benytter tokenization[11] og andre ad-hoc tilgange.

3.4. Federated Learning

Når man ønsker at benytte sig af kunstig intelligens og lave Machine Learning, er en af de ting, der er brug for, og oftest er mest udfordrende, adgang til data - mange data. Samtidigt er der et behov for at beskytte disse data, hvis det er persondata, eller de på en anden måde er følsomme data.

Machine Learning virker ved at træne en algoritme, ved at lade algoritmen se på en stor mængde data - fx data om personer ramt af en bestemt sygdom og personer uden denne sygdom. Algoritmen lærer så ud fra disse data; man siger den laver en model. Denne model kan derefter bruges til ud fra nye data at vurdere, om personen er i risiko for at have den specifikke sygdom eller ej. Samme teknik bruges til at tagge katte eller personer i billeder og til at lære selvkørende biler at forstå vejskilte.

Hvis de data, der skal bruges til træning, findes i forskellige organisationer eller systemer, vil man ofte samle dem et sted først og træne modellen på dem der. Dette kan ikke altid kan lade sig gøre, og det kan oplagt give udfordringer privatlivsmæssigt. I stedet for kan man træne delvise modeller med algoritmen på mindre mængder data og samle de delvise modeller efterfølgende. Det kaldes Federated Learning og kan både bruges på få større mængder data, hos få fx HR data fra en mængde virksomheder i stil med Boston casen nævnt i afsnit 3.2, eller mindre data fordelt på rigtigt mange kilder. Både Apple og Google bruger federated learning, hvor der trænes delvise modeller på brugernes telefoner, som kan samles til modeller til at foreslå det næste ord eller emoji, vi vil skrive i en sms.

5. Opsamling

I dette holdningspapir er gennemgået forskellige privatlivsfremmende teknologier. Rådet for Digital Sikkerhed anbefaler, at man til behandling af personoplysninger og øvrige følsomme data, i videst muligt omfang benytter privatlivsfremmende teknologier. Rådet anbefaler derfor, at man vælger teknologier med følgende fælles egenskaber, der gør sig gældende for de gennemgåede teknologier:

[11] Tokenization: en metode hvor følsomme data erstattes af "støj"; dette gøres deterministisk dvs. samme data giver samme "støj" eller token, således at man stadigt kan lave fx databasesøgninger.

- Der findes formelle matematiske beviser for sikkerheden af de underliggende konstruktioner på linje med de garantier, som fx ligger bag NemID
- Der er gryende kommerciel udbredelse af disse teknologier, som gør, at brugere kan forvente en tilstrækkelig produktmæssig modenhed.
- De beskrevne PETs vil enten
    - Give bedre sikkerhed i eksisterende løsninger, eller
    - Muliggøre anvendelser som før ikke var mulige af privatlivshensyn

Ovenstående liste er ikke udtømmende. Rådet vil komme med yderligere vejledning af, hvorledes krav til privatlivsfremmende teknologier skal stilles i udbud samt opgradering af eksisterende løsninger. Samlet har disse teknologier langt fra realiseret deres fulde potentiale til at sikre privatlivshensyn uden at gå på kompromis med samfunds- eller forretningsmæssig funktionalitet.