



LÆRERVEJLEDNING

for danske folkeskolelærere til undervisning af
elever i dataforståelse og digitalt selvforsvar

Forfatter: Pernille Tranberg
I samarbejde med: Center for Undervisning, CFU
Sponsoreret af: LB Forsikring

September 2019

KOLOFON

Forfatter: Pernille Tranberg
I samarbejde med: Center for Undervisning, CFU
ved Lonnie Sørensen
Korrekturlæser: Annette Bjørg Koeller
Fotos: Unsplash.com
Digital version på Dataforståelse.dk

September 2019

Sponsoreret af: LB Forsikring



LB Forsikring

Børn skal forstå data



Når vi i dag benytter sociale medier, hjemmesider og apps, afgiver vi alle data i større eller mindre grad. Det giver os mange muligheder, men det giver også adgang til vores privatliv og øger risikoen for udnyttelse til kommercielle eller kriminelle formål. Derfor skal langt flere være bevidste om, hvordan deres data bruges og udnyttes.

Dataforståelse og dataetik handler om de måder, vi håndterer den voksende mængde data, vores samfund bygger på. Data trækker flere og flere tråde gennem vores hverdag, og det fordrer refleksion om, hvordan data indsamles, bruges og lagres. Samtidig kan privatliv og datakontrol også for mange børn - og voksne - virke fjern og ligegyldig. De har langt hen ad vejen accepteret, at prisen for at bruge internettet er, at man skal afgive private oplysninger. Derfor kommer digital myndiggørelse og dataetik fremover også til at handle om, hvordan man bedst muligt beskytter og kontrollerer sine data.

Børn skal lære at forstå, hvad data er, og - når det gælder persondata - hvordan data kan bruges på godt og på ondt, til fordel og ulempe for dem selv og samfundet. Og hvordan de kan sikre sig, at persondata forbliver så privat som muligt og på et sikkert sted.

De skal lære at være offentlige mennesker og se såvel de positive som negative sider af onlinelivet - herunder at kunne fremstille realistiske og afmålte kommunikationer om sig selv til relevante målgrupper og vurdere bagvedliggende agendaer og adfærdsstyrende mekanismer i online-tjenester.

Over det næste år vil en alliance bestående af Center for Undervisningsmidler og LB Forsikring, som blandt andet består af Lærerstandens Brandforsikring, samt dataetisk ekspert Pernille Tranberg sørge for, at 1200 lærere landet over bliver klogere på, hvordan man underviser børn i dataforståelse.

Til dette formål har vi udviklet en 3-timers workshop for lærere/pædagoger i grundskolen med tilhørende læringsressourcer, der efterfølgende kan bringes i spil i arbejdet med elever fra 5. - 10. klasse.

Læringsressourcerne består først og fremmest af denne gennemarbejdede lærermanual med baggrundsviden, øvelser og tilhørende videoer. Derudover dias fra workshoppen, så man efterfølgende kan sammensætte og justere i indhold til brug for netop de elever, man arbejder med.

Alle ressourcer ligger på www.dataforståelse.dk

God arbejdslyst.

Center for Undervisning, LB Forsikring og Pernille Tranberg

INDHOLDSFORTEGNELSE

KAPITEL 1. SAMFUNDS- OG FORRETNINGSMODELLER

Samfundsmodeller baseret på data

- Datadiktatur

- Datamonopoler (Øvelse 1.0 Infrastruktur)

- Datademokrati

Forretningsmodeller baseret på data

- Gratis (Øvelse 1.1. Gratis vs penge)

- Datakøbmænd

Gode måder at bruge data på

- Ikke-persondata

- Aggregerede, anonymiserede data

Risikable/uetiske måder at bruge data på

- Personalisering (Video: Posten vil gøre som Facebook og Google. Øvelse 1.2. Algoritme dilemma)

- Prisdifferentiering

- Profilering og prediktion (Øvelse 1.3. Apply Magic Sauce)

- Diskrimination

- Mikrotarifisering

- Automatiserede afgørelser (Øvelse 1.4. Automatiserede afgørelser dilemma)

KAPITEL 2. PRIVAT VS OFFENTLIG

Privatlivsindstillinger er social kontrol-indstillinger

- (Øvelse 2.0 Tjek dine Facebook indstillinger)

- Manipulerende adfærdsdesign

- At være offentlig (Øvelse 2.1. Video med diskussioner)

- At være privat

- Deling (Øvelse 2.2. Fakenamgenerator.com)

KAPITEL 3. DIGITALE FODSPOR

- (Video: Hvis din app var en bagerjomfru)

- Cookies (Øvelse 3.0 - tracking cookies) (Øvelse 3.1 Analysér et website for cookies)

- Device fingerprinting

- Blokér for tracking (Video: Sådan virker og installeres en adblocker. Øvelse 3.2 Installer en adblocker på computer eller mobil)

- Søgning og browsere (Øvelse 3.3 Installer en privat søgemaskine)

KAPITEL 4. DATASIKKERHED

- Åbne wi-fi er også for hackere

- Phishing

- Passwords

- Sådan sætter du dine mobil-indstillinger

- (Video: Lytter nogen med via din telefons mikrofon?)

- (Øvelse 4.0 Hvad har dine apps adgang til?) (Øvelse 4.1 Hvem har adgang til din lokation)

- Dæk kameraet

- Styr din IP-adresse/lokation med en VPN (Video: Sådan installerer du VPN) (4.2. Øvelse: Installer og brug en VPN)

KAPITEL 5. DATAETIK, DATARETTIGHEDER & NY TECH

Hvad er dataetik (definition og principper)

Hvordan ved man, om en tjeneste er dataetisk?

Øvelse 5.0 Kahoot

Dataetiske eksempler (LEGO, Edulab, AULA, Apple, Clue)

Google Education

Datarettigheder

Når skaden er sket

Ny teknologi

ØVELSER 🏊

KAPITEL 1. SAMFUNDS- OG FORRETNINGSMODELLER

Samfundsmodeller baseret på data

Datadiktatur¹



I en række år har Kina testet et nyt system, der rulles ud for alle kinesere i løbet af 2020. Det er et system, som nok de færreste europæere ville ønske sig. Et skræmmescenarie for, hvad overvågning kan føre til, et worst case scenarie, når det udføres af staten og bruges til at mikrokontrollere befolkningen med.

En kineser bliver født med et antal point, som kan gå op og ned afhængig af, hvordan personen opfører sig - efter regeringens definition af god/dårlig opførsel. Går en kineser over for rødt lys, opfanges det af kameraer med indbygget ansigtsgenkendelse, så personen trækkes i point. Glemmer han/hun det månedlige afdrag på lånet, straffes man også. Gør man noget godt for naboer eller andet, som regeringen dømmer positivt, får man flere point. Antallet af point er afgørende for, om man kan få et visum til en udlandsrejse, hvor ens børn må gå i skole, eller om man må tage hurtigtoget eller bumletoget. Der er allerede millioner af 'diskrediterede' kinesere - en ny underklasse.

Rigtig mange kinesere er online via mobiltelefoner - de er sprunget det led over, hvor vi andre først gik online via computere. Samtidig bruger de fleste nogle få meget brugte apps som WeChat (en udvidet version af Facebook Messenger), hvor man kan foretage sig alt fra at betale regninger, bestille og betale taxa eller pizza, chatte, videochatte etc. Og den kinesiske regering

¹ Mere læsestof:

<https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html>

<https://www.scmp.com/tech/apps-social/article/3003191/life-one-chinas-13-mi...>

<https://www.sixthtone.com/news/1003759/camera-above-the-classroom>

<https://dataethics.eu/how-china-will-beat-the-us-on-ai/>

<https://www.scmp.com/news/china/society/article/2143899/forget-facebook-lea...>

siges at kræve adgang til alle - også kommercielle tjenester - for at monitorere dem. Kina kan derfor med vestlige briller kaldes et datadiktatur.

Indtil nu har vi ikke hørt om de store demonstrationer imod systemet i Kina. Måske fordi de færreste forstår implikationerne af statsovervågning, og fordi mange kinesere faktisk har tillid til, at deres regering vil dem det bedste. Måske også fordi mange går mere op i, at de er blevet bedre stillet økonomisk end i deres politiske rettigheder. Og måske synes nogle, at det er meget bedre end før, for nu kan de altid gå hen på deres version af borgerservice, se deres point og forstå, hvad de overvåges for, og hvordan de straffes/belønnes.

Datamonopoler²



USA - og især Silicon Valley - har skabt nogle globale succeser - kaldet unicorns - i Google (søgning), Amazon (e-handel og cloud), Facebook og dertilhørende Instagram (sociale medier) samt Facebooks WhatsApp (chatapp). De er så store, at de ofte slipper af sted med ikke at betale lige så meget i skat som mange andre virksomheder. Nogle har forhandlet sig til delvis skattefrihed mod at slå sig ned i området med løftet om at skabe arbejdspladser, eller de er bare svære at

ramme for en lille myndighed. Deres forretningsmodel er, at de ofte er 'gratis', og det handler om at få så mange brugere som overhovedet muligt, så man enten kan tage betaling for sin tjeneste fra nogle af brugerne eller kapitalisere på brugernes data. Disse virksomheder sælger ofte sig selv, som om de er sat i verden for at gøre verden bedre og mere retfærdig.

Indtil forrige årtusinde regulerede den amerikanske stat ofte tech-monopoler. I 1990'erne gik myndighederne fx efter Microsoft. Men i dette årtusinde har det været småt med monopol-regulering. Det kan skyldes, at de store tech-giganter hælder milliarder af kroner i politisk lobbyisme og dermed forhindrer det. Det kan også skyldes, at den amerikanske regering faktisk ser fordele i at skabe globale giganter, så de kan stå sig i konkurrencen mod kinesiske giganter som Tencent, Alibaba og Huawei.

I hvert fald er det primært Europa, der forsøger at regulere tech-giganterne via monopol-lovgivningen - i tæt samarbejde med datalovgivningen (GDPR) og forbrugerlovgivningen.

USA har det med at beskyjde alle andre for at være protektionistiske i deres lovgivning, fx har den europæiske datalov, GDPR (General Data Protection Regulation), fået skyld for det. Men når man betragter USA, så er det ofte dem, der er protektionistiske. Fx har staten gjort sig meget umage for at advare og forbyde kinesiske tech-giganter som Huawei.

USA's tech-giganter truer ofte europæiske virksomheders levebrød. Da Google fx købte den største spiller på markedet inden for webstatistik, Urchin, og lancerede Google Analytics 'gratis' i hele verden, ødelagde det forretningsgrundlaget for de mange små virksomheder.

² Mere læsestof:

<https://dataethics.eu/wp-content/uploads/DATAETIK-2-udgave-2.pdf> - s 131/kap 11

<https://www.yalelawjournal.org/note/amazons-antitrust-paradox>

<https://dataethics.eu/?s=antitrust>

<https://www.businessinsider.com/tech-company-mission-statements-2016-1?r=US&IR=T#googles-mission-statement-is-straightforward-and-hasnt-changed-since-1998-googles-mission-is-to-organize-the-worlds-information-and-make-it-universally-accessible-and-useful-3>

[https://dataethics.eu/bog/kapitel 11 om datamonopoler](https://dataethics.eu/bog/kapitel%2011%20om%20datamonopoler)

I dag er mange mindre danske virksomheder dybt bekymrede over, hvad Amazon kan finde på, når det gælder erobring af markedsandele i Danmark og resten af Europa.

ØVELSE 1.0 🧐 (infrastruktur)

Datademokrati³

Europa forsøger sig med noget, man kunne kalde et datademokrati. I et demokrati er det borgerne, der bestemmer samfundsudviklingen via demokratiske valg. I et datademokrati har borgerne indsigt i, overblik over, forståelse for og ikke mindst kontrol over egne data, ligesom de har over egne penge. Der er vi dog slet ikke endnu, men GDPR, the General Data Protection Regulation, der trådte i kraft maj 2018, giver faktisk individer retten til at styre egne data.

Individer har ret til at få indsigt i sine data, til at få rettet og slettet og til at få sine data leveret i et let tilgængeligt format (portabilitetsprincippet) - se mere i kapitel 5.



I et (data)demokrati er det dem med magten, der er gennemsigtige/transparente omkring, hvordan de forvalter deres magt, og borgerne har mulighed for aktindsigt. Individuelle borgere kan selv vælge, hvor gennemsigtige de vil være. Men med gratis-forretningsmodellen er mange individer blevet gennemsigtige via deres data og dermed sårbare over for diskrimination og manipulation såvel økonomisk som politisk.

Forestil dig, at du havde et sted med fuldt overblik over alle dine data på samme måde, som du har det med dine penge i banken. I denne 'personlige databank' sætter du *dine* privatlivsindstillinger; det kan fx være, du ønsker, at dit online supermarked ved, at du er vegetar, at din læge har adgang til alle dine sundhedsdata samt din kost, som du registrerer via en app, og at du ønsker at donere dine sundhedsdata til offentlig forskning. Den personlige databank, som du vælger og har tillid til, kan give dig rådgivning om, hvordan du bedst varetager dine datainteresser. Du bestemmer selv, hvor megen kontrol du vil have, og hvor meget vejledning og handling du ønsker fra 'bankens' side, som kan agere på dine vegne, ligesom nogle af os i dag beder banken investere for os på vores vegne.

Du kan sætte en udløbsdato for, hvornår en tjeneste ikke længere kan få adgang til dine data. Og du kan aktivere dine data til fordel for dig selv, fx bruge tjenester, der hjælper dig med at optimere din økonomi, dit energiforbrug, din transporttid, dit vitaminindtag etc.

I denne vision vil vores persondata ikke blive samlet ét sted. Det er alt for usikkert. Vi vil bare hver især have et dashboard, der giver os overblik og kontrol. Vores data vil således stadig være spredt ud over en masse forskellige servere, da det ikke er forventeligt, at offentlige Danmark vil slette persondata i deres databaser, for at individer kan sidde på dem ene og alene. Nej, de må af med en kopi af folks data, så individer i det mindste selv har et overblik og kan berige egne data med fx adfærdsdata fra mobilen og bruge den viden til fordel for sig selv.

Mydata-bevægelsen (mydata.org) arbejder for at sikre individer kontrol over egne data. Især Frankrig er langt med at teste mulighederne; fx forsøger det lærer-ejede forsikringsselskab MAIF

³ Mere læsestof:

<https://www.theguardian.com/news/series/cambridge-analytica-files>

<https://dataethics.eu/wp-admin/post.php?post=7135&action=edit> (OPDATER DENNE)

<https://dataethics.eu/data-democracy-the-european-way/>

<https://dataethics.eu/data-ethics-is-paying-off-for-french-insurance-company/>

<https://medium.freecodecamp.org/an-introduction-to-solid-tim-berners-lees-new-re-decentralized-web-25d6b78c523b> Forretningsmodeller baseret på data

at give en testgruppe af deres kunder fuld kontrol over egne data. Også Japan er i gang med at teste ideen fra statslig side, og så står Tim Berners-Lee, opfinderen af WWW, i spidsen for at bygge en ny decentraliseret internet-infrastruktur, Solid.

Det er vigtigt at understrege, at individuel datakontrol også er en fordel for virksomheder, organisationer og regeringer. Ikke kun fordi det vil være med til at sikre den digitale tillid, som er altafgørende for, at digitaliseringen fungerer og forbedrer vores samfund og velfærd, men også fordi den bedste kilde til rige, relevante, opdaterede og ægte persondata er fra kilden selv: individet.

Og så arbejder Mydata-bevægelsen (mydata.org) også på at få skabt nye innovative tjenester, hvor individer selv kan aktivere deres data, lære af dem og blive klogere, sundere eller rigere.

Forretningsmodeller baseret på data

Gratis⁴

Når noget er gratis, er du produktet. Medmindre virksomheden tjener penge på noget andet relateret til produktet og kun giver lidt eller en mindre version af produktet væk gratis for at skabe opmærksomhed, så kan man godt regne med, at 'gratis' produkter betaler man for med sine egne, sine kunders eller sine borgers persondata.

Google er nogle af de bedste eksempler, men også Netflix, Spotify og Amazon er eksempler på, at noget næsten er for billigt til at være sandt. Det er, fordi du (også) betaler med dine data. Og det gør du med bind for øjnene, for du ved ikke, hvor meget dine data er værd. Hvad er din fødselsdato værd? Din musiksmag? Hvad er din politiske holdning værd? Eller din seksuelle orientering?

'Gratis' handler også om at blive så stor som mulig. Først og fremmest med så mange brugere som muligt, så virksomheden kan indtage det globale marked og få endnu flere brugere. Og så enten gå på børsen eller lave en 'exit', dvs. blive solgt og skumme fløden på det. Da den danske Endomondo-app (hvor du kan tracke dine gå-, løbe- og cykelruter) blev solgt til en amerikansk virksomhed, blev den ikke solgt så dyrt, blot fordi der var tale om banebrydende ny teknologi, men mindst lige så meget fordi der var tale om salg af millioner af brugere - altså masser af persondata. Så set med de øjne solgte Endomondo i tusindvis af danske persondata til en amerikansk virksomhed.

Den amerikanske model er en 'winner-takes-it-all' model eller 'survival-of-the-fittest'. Der bliver ikke taget så mange hensyn til de svageste i samfundet som i et dansk velfærdssamfund. Det er din egen skyld, dit eget ansvar - sådan sat lidt på spidsen. Og så er det primært private kæmpevirksomheder - ikke staten - der sidder på det nye 'guld' eller 'olie', som vores persondata også kaldes.

Mange tech start-ups i Silicon Valley arbejder efter følgende mål:

Det skal være 'gratis' og finansieres af høst og brug af masser af persondata.

Så mange brugere som muligt - det bedste er at opnå en monopollignende tilstand.

Det skal gøre brugerne afhængige. De kan ikke få nok. Brugere køber mere og mere.

Gratis-forretningsmodellen bliver også kaldt noget andet mindre positivt: 'surveillance capitalism' - 'overvågningskapitalisme'.

⁴ Mere læsestof: <https://www.theguardian.com/books/2019/feb/02/age-of-surveillance-capitalism-shoshana-zuboff-review>

ØVELSE 1.1 😊 (Betal med data eller penge)

Datakøbmænd⁵

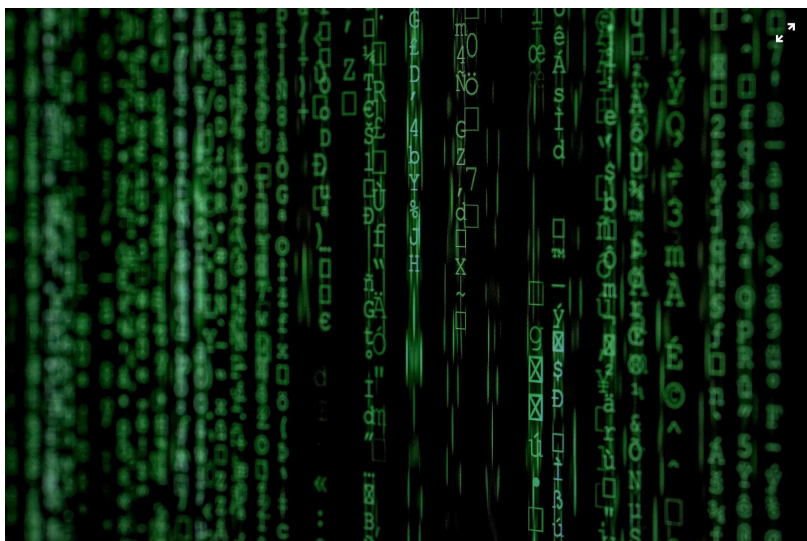
Google og Facebook sælger ikke dine data. De sælger adgang til dig og mig på baggrund af al den data, de har indsamlet og analyseret om dig og mig. Det ville være rigtig dumt af dem at sælge al den data, for så får de ikke så meget ud af den. Ved at sælge adgang til mennesker kan de jo sælge samme viden om dig og mig igen og igen og igen.

Datakøbmænd, data brokers, sælger derimod persondata. Det er en hel industri, der er opstået i takt med, at persondata er blevet mere og mere værd. Især i USA har myndighederne (FTC) kortlagt denne gråzone-industri, hvor der rask væk handles med lister over kræftramte og diabetikere eller forældre, der har mistet et barn i en trafikulykke.

Men også i Europa hersker datakøbmænd. Fx er det rapporteret, at i Tyskland sidder datakøbmanden Arvato AX Direct på 600 forskellige data point over 70 mio. brugere.

Gode måder at bruge data på⁶

Ikke-persondata



Når Vestas bruger vinddata til at planlægge, hvor vindmøller skal placeres for at kunne producere optimalt, er det helt uproblematisk, da vinddata ikke har noget med dig og mig at gøre. Når UPS bruger produktdata til at beregne risikoen for, hvornår en reservedel bryder sammen, er det helt uproblematisk, fordi de data heller ikke har noget at gøre med identificerbare personer. Alle andre data end persondata kan indsamles, analyseres og bruges til at forudsige ting og sager helt uden privatlivsmæssige

problemer. Faktisk ligger der et kæmpe vækstpotentiale i netop ikke-personlige data i forhold til at optimere produktion og logistik mv, ifølge konsulentvirksomheden McKinsey.

I både Vestas og UPS-eksemplerne bruges data til at bakke op om andre indtægtskilder, men der er også eksempler på virksomheder, der lever kun af data, der ikke er personhenførbare. Fx brugte start-up-virksomheden Food Genius menukort fra i titusindvis af restauranter og cafeer til at analysere, hvilke retter og råvarer der var efterspørgsel på, og solgte den viden videre til andre fødevarer- og restaurationsvirksomheder. Virksomheden blev solgt til US Foods i 2016.

⁵ Mere læsestof:

<https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>

<https://crackedlabs.org/en/corporate-surveillance>

⁶ Mere læsestof

<https://erhvervsstyrelsen.dk/sites/default/files/big-data-som-vaekstfaktor.pdf>

https://www.mckinsey.com/~media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Big%20data%20The%20next%20frontier%20for%20innovation/MGI_big_data_full_report.ashx

Aggregerede, anonymiserede data

Persondata kan bruges lovligt og etisk forsvarligt af såvel den offentlige som private sektor. Forskere bruger fx persondata fra Danmarks Statistik til at forske i sundhed og beskæftigelse. Dataene er pseudonymiserede, dvs. forskerne har ikke adgang til identificerbare data. Nøglen til disse har kun få udvalgte medarbejdere i Danmarks Statistik, som generelt har et godt omdømme i forhold til datasikkerhed.

Nødhjælpsorganisationer kan bruge anonymiserede data fra telefonmaster til at kortlægge flygtningestrømme og bedre vurdere, hvor de skal placere nødhjælps-centre/lejre. Private virksomheder kan også sælge persondata, så længe de er aggregerede og anonymiserede på den bedst mulige måde. Fx solgte den hollandske virksomhed TomTom, der laver GPS-systemer, GPS-data til politiet, så politiet kunne finde de bedste steder at sætte fartkontrol op. Mange kritiserede tiltaget, fordi det er svært at forstå forskellen på at sælge identificerbare data og mønstre baseret på rigtig manges anonymiserede data, og det var det sidste, der var tilfældet her.

Et lignende eksempel var Danske Bank, der på et tidspunkt fortalte i pressen, hvordan danskere på MobilePay opførte sig. Der var flere kritiske røster: "Kigger Danske Bank nu ned i mine data?" Nej, det var også mønstre, der var baseret på aggregerede anonymiserede data.

Den store hurdle her er, at man endnu ikke kan tjekke om det, virksomheder og organisationer siger, de gør, når de anonymiserer, også er det, de gør. Når en dansk virksomhed fx af Erhvervsstyrelsen får lov til at hente MAC-adresser ud af vores mobiltelefoner ved trafikovervågning, fordi den siger, at data bliver fuldt anonymiserede, har myndigheden ikke en chance for at tjekke, om det er sandt. Når Apple siger, at de kun har identificerbare data ude på vores mobile enheder og ikke inde på deres servere, hvor de anonymiserer data, så kan vi reelt ikke tjekke det. Dette er som oftest baseret på tillid.

Der kommer utvivlsomt krav i fremtiden om, at man skal bevise, at man anonymiserer tilstrækkeligt. Intet er 100% sikkert. Heller ikke anonymisering. Med tilstrækkeligt mange data kan man nogle gange re-identificere data og finde frem til personer. Men en 96% eller 98% sikkerhed er måske også nok. I hvert fald vil der komme krav om, at uafhængige eksperter kan få adgang til data-maskinrummet på tech-virksomheder og verificere og auditere, at det, de siger, de gør, det gør de også. På samme måde vil vi som forbrugere i fremtiden også få hjælp af mærkningsordninger, som peger på, hvilke produkter, vi kan stole på datasikkerhedsmæssigt; fuldkommen som vi i dag har troværdige mærker inden for økologi og fair trade.

Risikable/uetiske måder at bruge data på⁷



Personalisering



Posten vil gøre som Facebook og Google.

<https://www.youtube.com/watch?v=tw4DdF8dSjE>

Videoen, der viser en parodi på et Post Danmark, som har fået den gode ide at læse alle breve og sælge data, er ganske sigende. Den peger på den mest udbredte og basale måde at bruge persondata på i dag, nemlig at man kan personalisere/skræddersy tilbud til kunderne/brugerne på basis af mest mulig viden om dem.

Virksomheder, der ønsker at personalisere tilbud og indhold til sine kunder, indsamler data på flere måder. Både direkte, hvor kunderne selv giver dem data, og via tredjepart-cookies, der følger dig rundt på nettet og deler data om din adfærd, medmindre du blokerer for det (se mere kapitel 3). På mange måder kan det være godt, når man får gode tilbud. Fx hos Saxo, der fortæller dig om en ny bog, som du med stor sandsynlighed gerne vil købe, fordi du tidligere har købt noget i samme stil. Saxos personalisering er helt okay, fordi Saxo primært bruger de data, du selv har givet Saxo, og dermed føler deres kunder sig vidende om, hvad der ligger bag tilbuddet: "Nå ja, jeg købte jo også den og den tidligere." Hvis Saxo derimod gav dig et tilbud om en bog om kræft, uden at du selv havde vist Saxo den interesse, men at virksomheden havde fulgt dig rundt på nettet og forbi fx cancer.dk, som har tredjepart-cookies på hjemmesiden, så

⁷ Mere læsestof:

Siri-kommissionens rapport om AI og ethics: https://ida.dk/media/1583/ai_-_etik_-_sirikommissionen_rapport.pdf

<https://www.medieradet.dk/medieradet/digitaldannelse/persondata-hva-noget>

private traits are predictable, 2013: <https://www.pnas.org/content/110/15/5802.full>

<https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/>

https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-focus-big-data_en.pdf

<https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73>

<https://digitaluddannelse.org/> - bogen LIKES på dansk. Undervisningsmateriale til udskoling

ville du sandsynligvis føle, at det var *creepy*. Så personalisering af tilbud og indhold er kun okay for de fleste brugere, når det sker med data, som er givet direkte af kunden/brugeren.

ØVELSE 1.2. 🤖 (algoritme dilemma)

Prisdifferentiering

I 2017 søger jeg efter et hotelværelse i Tokyos centrale Shibuya-distrikt. Pris 11.000 DKR for ni nætter. Det er med en browser, hvor jeg blokerer for tredjepart-cookies (se kapitel 3), så hjemmesiden ikke kan se, om jeg har været inde flere gange eller søgt efter andre priser. Jeg sætter en VPN på (se kapitel 4), hvor man kan ændre sin lokation (dvs. IP-adresse), og ændrer den fra Danmark til Tyskland, hvor priserne generelt er lavere. Resultat: nøjagtig det samme hotelværelse for 9.000 kroner.

Mange websites differentierer priser efter, hvor du er. Medmindre du selv gør noget, så kan alle websites se din IP-adresse. I USA kalder man det 'price dynamics', mens EU-Kommissionen kalder det 'price discrimination'. Det er svært at sige, om det er ulovligt. Det er jo ikke ulovligt at prutte om priser. Det er sandsynligvis kun ulovligt, hvis du ændrer priser afhængig af køn, race mv.

Digitalt er det at prutte om priser noget mere ulige end analogt, da den digitale sælger ofte ved, hvor du har kigget på priser, hvad du er særligt interesseret i, dit køn, din lokation osv., afhængig af hvilke digitale fodspor du har afgivet.

Det er svært at vurdere, om der er prisdifferentiering på den måde i Danmark. Loyale aviskunder betaler fx mere end illoyale aviskunder, fordi de hvert år betaler fuld pris. Og man kan spørge sig selv, at hvis en sælger ved, at du altid køber den og den shampoo eller den og den sodavand, hvorfor så give dig rabat?

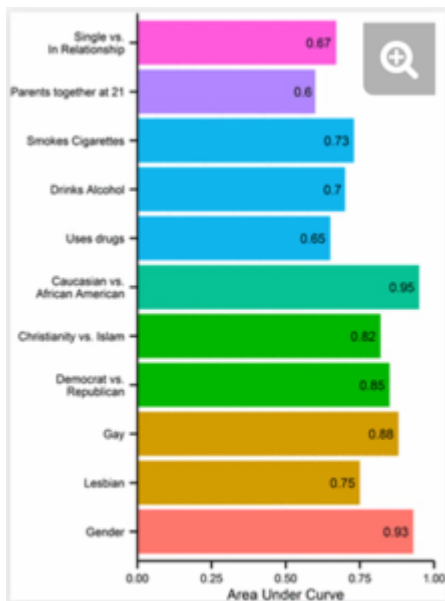
De fleste kunder ville nok blive stødt på manchetterne over, at deres supermarked ændrede priser på baggrund af detaljeret viden om deres adfærd, så det er nok ikke en udbredt praksis i Danmark.

Profilering og prediktion

At sende et enkelt like ud på Instagram eller et foto af sit barn på Facebook er i sig selv oftest ikke noget problem. Det er summen af dine likes, summen af din adfærd og dine andre data, der er interessant. Vi bliver alle profileret af især kommercielle virksomheder, der indsamler data i alle afskygninger om os. Hvor du befinder dig, hvad du liker og deler, hvad du køber eller oser forbi, hvilken browser du bruger, hvem du er i kontakt med, hvor du arbejder, hvad du downloader og så videre og så videre. Alle disse data bruges til at skabe profiler på os, så man bedst muligt kan 'servicere' os med relevante tilbud og indhold - se mere ovenfor om 'personalisering'.

En virksomhed må ikke bare profilere os uden vores samtykke, og ifølge GDPR har vi også ret til at sige nej tak til at blive profileret. Problemet er, at mange af os bare siger ja til lange handelsbetingelser (Terms of Conditions, TOC) for at få lov til at bruge fx Facebook, så de dermed har fået tilladelse til det hele. Ifølge GDPR er dette dog ikke lovligt, da man skal have specifikt samtykke for hvert formål, men der kører sager om den del.

Efter profilering kommer prediktion. Det vil sige, at man kan bruge data til at forudse din næste handling, køb, ønske eller livsbane. Dataprediktion kan bruges til at forudse og regne ud, hvilke



sygdomme du er disponeret for, om du ender på kontanthjælp, om dine børn bliver omsorgssvigtet, risikoen for at få en ulykke på skiferien og meget, meget mere. Dataprediktion kom for alvor på agendaen i 2013, da forskere fra University of California analyserede 58.000 Facebook-brugeres LIKES og fandt ud af, at selvom man ikke likede noget følsomt, men bare forskellige brands, kunne man med 67% sandsynlighed gætte, om du er single eller i parforhold, 73% sandsynlighed for om du er ryger, og 88% sandsynlighed for om du er homo- eller heteroseksuel.

Dette studie var også baggrunden for det arbejde, der blev lavet af konsulentvirksomheden Cambridge Analytica, der med hjælp fra Facebook kunne foretage politisk manipulation af vælgere i især USA og UK via Facebook-annoncering. Facebook-brugerne var blevet så gennemsigtige, at de blev manipulerbare. Men selvsamme sag var også med til at sparke gang i samtalen omkring

privacy og dataetik. For nylig kom Netflix-dokumentaren The Great Hack om denne sag, som Facebook har sluppet billigt for: en bøde på 5 mia. US-dollars for at bryde en aftale med de amerikanske myndigheder fra 2012 om at passe på brugernes data.

Mange danske embedsmænd er overbeviste om, at dataprediktion kan blive et gedigent værktøj, der kan spare forvaltningen penge og gøre servicen bedre for borgerne. Både Gladsaxe-sagen og sagen om prediktion af henholdsvis omsorgssvigtede børn og langtidsledighed viser, at det er meget følsomt at begynde at forudse skæbneforløb for det enkelte menneske:

Gladsaxe-sagen handler om, at kommunen ved hjælp af kunstig intelligens, samkørte data om børn og forældres adfærd og historik, ville udvikle et værktøj, der kunne opdage udsatte børn tidligere, end et menneske kan. Det lyder umiddelbart godt, hvis man kan opspore udsatte børn tidligere, men hvis det er på bekostning af masseovervågning af alle kommunens forældre og børn i Gladsaxe, så er det nok ikke proportionelt (dvs. lovligt). Kommunen ville bruge såkaldte risikoindikatorer, såsom børns udeblivelse fra tandplejen, fra sundhedsplejen, forældrenes psykiske lidelser, arbejdsløshed eller skilsmisse, til at forudse risikoen for omsorgssvigt. Arbejdet er dog indstillet, da der stilles juridiske og etiske spørgsmål ved modellen.

Sagen om brug af data til at forudse langtidsledighed, hvor ideen er at bruge data til at forudse, hvem der er i størst risiko for at blive langtidsledig, kører derimod for fuld skrue, da det danske Datatilsyn har givet Beskæftigelsesministeriet grønt lys. Men de juridiske og etiske spørgsmål omkring begge modeller er:

- er det ok at bruge data om børn til at forudse, om de bliver omsorgssvigtede eller ender på kontanthjælp? Og er det en hjælp til de børnefamilier at vide det, og er der ressourcer til at give dem tilstrækkelig hjælp? Eller burde vi ikke lade børn være børn og give dem en chance for at vokse op og bryde mønstre eller få en second chance?
- har beskæftigelsescentrene nogle helt specielle værktøjer til de arbejdsløse, der måtte være i høj risiko for langtidsledighed, eller bruges de samme værktøjer på alle, der bliver arbejdsløse?
- giver det mening - er det proportionelt - at overvåge alle forældre i Gladsaxe Kommune for at finde nogle ganske få omsorgssvigtede børn?
- er det en god ide at putte alle i kasser, som det sker, når man bruger data til at kategorisere 'muligt omsorgssvigtede', 'muligt langtidsledige' etc.

At forudse mønstre baseret på ikke-persondata eller aggregerede anonymiserede persondata er meget mere problemfrit og kan uden tvivl skabe vækst i vores samfund frem for individuelle forudsigelser som i de to ovenstående eksempler. Dels er det for mange en krænkelse af privatlivets fred, mens andre kan ikke se formålet med det. Endnu andre kritiserer, at data langt fra er tilstrækkelige i antal eller gode nok til med en høj nok sandsynlighed at kunne forudse skæbner og hændelser. Og endelig lyder det fra mange, at ansatte i kommunerne godt selv kan udpege dem i risikozonen, men at vi alligevel ikke har ressourcer nok til at tage fat i dem.

Ø V E L S E 1.3. 🧙 (Applymagicsauce)

Diskrimination

Ud over prisdiskrimination (se under prisdifferentiering) er der mere indbagte risici for, at data og algoritmer kan diskriminere. Al databehandling foretages på historiske data, og vi mennesker har det med at diskriminere folk, der er i mindretal. Dommere har gennem tiden sendt mange flere sorte end hvide mennesker i fængsel i USA. Og når fængselsvæsenet i USA i dag bruger en algoritme til at forudse en mulig prøveløsladts sandsynlighed for at begå mord under prøveløsladelsen, så er der bias/diskriminations-risiko i de data.

Hvide mandlige topchefer har typisk promoveret hvide mandlige ansatte, så der er algoritmer baseret på de data, som diskriminerer alle andre end hvide mænd. Og resourcesvage har haft sværere ved at få kreditlån, så der ligger også en risiko for bias, hvis man bruger de data til at beregne vores kreditværdighed.

Hvis man profilerer og predikerer på baggrund af (historiske) data, er der altså stor risiko for, at man gentager denne diskriminering. Derfor er der i dag mange forskere og virksomheder, der forsøger at finde ud af, hvordan man kan rense historiske data for såkaldt bias for at undgå diskrimination.

Mikrotarifiering

Især i USA, men også i flere europæiske lande, ønsker forsikringsselskaber at indføre mikrotarifiering. Den oprindelige forsikringstanke var, at alle deltog på ens vilkår, og at heldige kunder dermed betalte for uheldige kunder. Over tid har forsikring udviklet sig, så den enkelte kundes risiko afspejles i prisen. Forsikring handler ikke kun om held og uheld - nogle grupper er mere udsatte end andre, fx i forhold til hvor de bor, eller om de står på ski på sorte løjper, og det afspejles i dag i prisen hos stort set samtlige selskaber. Med mikrotarifiering kan selskaberne gå helt ned på individuelt niveau og fastsætte præmier. Det sker allerede i dag ved installation af telematic-løsninger, som monitorerer, om du accelererer hurtigt og i det hele taget kører ordentligt, så selskaberne ved en ulykke kan vurdere, om du var medskyldig, fordi du kørte for stærkt. Samtidig er det en måde at forebygge, at fx unge bilister ikke kører for hurtigt og dermed påfører sig selv eller andre skade. Såfremt du har kørt for hurtigt, får du en højere selvrisiko, men du får til gengæld ofte en lavere præmie, hvis du kører med telematic-løsninger. Sådan en løsning er okay for at øge trafiksikkerheden - såfremt selskaberne ikke bruger dine data til andet end formålet og sletter dem efter brug.

Men ville det være okay, at de, der tegner sundhedsforsikringer, skal bære et armbånd om armen, så selskaberne kan få puls og skridt og sikre, at du bevæger dig nok, eller vurdere, om du er selvforskyldt i fedme?

Med mikrotarifiering står forsikringsselskaberne over for et kæmpe dilemma i forhold til det solidaritetsprincip, de har hyldet så længe. Mange unge, slanke, sunde og raske - og heldige -

har ofte ikke noget imod mikrotarifiering; men når de bliver 45+ og mærker aldringen, ja, så bliver de ofte solidariske. Derfor er dette emne et samfundsanliggende. Vi må som samfund beslutte, hvor langt vi vil gå med brugen af data.

Automatiserede afgørelser

Ø V E L S E 1.4. 😊 (automatiserede afgørelser)

Der er ingen tvivl om, at automatiserede afgørelser kan indføres på visse områder. Områder, hvor der er tale om klare regler og retskrav. Det kan være de mest banale byggeansøgninger, eller hvorvidt du har ret til en social ydelse. Men når der er tale om skøn, er der altid behov for at få et menneske indover.

Vi skal utvivlsomt diskutere, hvor langt vi vil gå i forhold til automatisering. For med den putter vi også os selv og alt det, vi laver, i kasser, og vi risikerer på lang sigt at tilpasse os de kasser og komme til at ligne hinanden for meget.

KAPITEL 2. PRIVAT VS OFFENTLIG⁹

Privatlivsindstillinger er social kontrol-indstillinger

I årevis har sociale medier som Facebook fortalt brugerne, at man kan være privat på platformen. Havde Facebook været ærlig, havde man kaldt det social kontrol-indstillinger fremfor privatlivsindstillinger. Til en vis grad kan man nemlig selv kontrollere, hvem man vil være venner med, hvem der kan se ens opslag, og man kan også skrive en-til-en beskeder til venner, både via Facebook, Instagram og WhatsApp. Men i alle de tre Facebook-ejede medier lytter Facebook med på en eller anden måde og til en vis grad også Facebooks kunder for at tjene penge på målrettede annoncer og indhold. Med WhatsApp er der tale om, at Facebook ikke kan læse med på indholdet af dine beskeder og samtaler, fordi de er krypterede. Det er også planen, at det skal ske for Facebook Messenger, siger Facebook, som i dag følger med i alt, hvad vi måtte lave på Messenger. Men selv med WhatsApp har Facebook rigtig fin adgang til data om os, da såkaldte metadata er guld værd: Det vil sige, hvem du er i kontakt med, hvor længe, hvor ofte og hvorfra - både telefonnumre og lokationer.

SnapChat bruger lidt samme taktik som Facebook. Folk - især børn - strømmede til SnapChat, da det blev lanceret, og mange troede, at alle beskeder forsvandt, så snart de var sendt. Det viste sig ikke at være sandt. Det er uvist, om de forsvinder i dag, men de fleste brugere forstår, at man altid kan tage et screenshot af en besked og dele den et andet sted, og så er den heller ikke forsvundet. Det positive her er, at mange unge faktisk tiltrækkes af et medie, hvor de tror, at deres indhold kun lever ganske kort tid.

Et andet område, hvor Facebook er offentlig-by-default - som standardindstilling - er din vennekreds. Du skal selv aktivt gå ind og skjule den, hvis du ikke vil have, at andre end Facebook kan se den. Men hvorfor skulle du dog det? Det er da meget fedt, at vennerne kan se, hvor mange venner du har? Det kan du overveje, fordi den viden kan bruges til mange ting. Hvis du er en person, der går imod strømmen og kritiserer andre (fx journalist, advokat, dommer, politiker, ekspert mv.) så kan din vennekreds bruges imod dig: "Nå, du er også ven med den og den, så er du inhabil." Hvis du søger et job som fængselsbetjent, ville jeg som interviewer også tjekke din vennekreds og sikre, at du ikke er venner eller venner med venner, der er venner med nogle bandemedlemmer. Og så har Facebook fået patent på en ide om at bruge vennekredsen til at udvikle et redskab, som kan vurdere, om du er værdig til at låne. Så det er om ikke at have for mange taber-venner.

ØVELSE 2.0 🤔 (privatlivsindstillinger på Facebook)

⁹ Mere læsestof

- <https://www.wsj.com/articles/how-13-became-the-internets-age-of-adulthood-11560850201> (du kan få denne gratis ved at søge på overskriften på Google.com)

- Børnetjenester: 2 ud af 14 tjenester rettet mod børn er dataetiske. <https://dataethics.eu/da/2-ud-af-14-boernetjenester-er-dataetiske/>

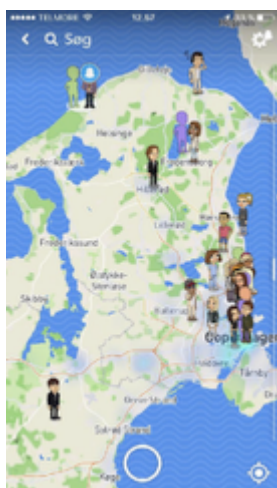
- Rasmus Rosenmeier om det er forbudt at dele nøgenfotos. <https://www.youtube.com/watch?v=LdMWc-tXxRg>

- <https://www.nytimes.com/2015/02/15/magazine/how-one-stupid-tweet-ruined-justine-saccos-life.html>

- Umbrella sagen <http://nyheder.tv2.dk/krimi/2019-01-11-hoejesteret-stadfaester-dom-i-umbrella-sag> og <http://nyheder.tv2.dk/krimi/2019-03-11-politiet-rejser-148-nye-sigtelser-i-umbrella-sag>

- Presseetiske retningslinjer: <https://journalistforbundet.dk/guide-til-de-presseetiske-regler>

Manipulerende adfærdsdesign



SnapChat er mester i 'nudging' eller med kritiske briller 'manipulerende adfærdsdesign'. I mange år har det været et must for virksomheder i Silicon Valley at gøre folk afhængige af deres produkter - eller i hvert fald blive så attraktive, at de er svære at forlade eller holde pause fra. Det kritiske opstår især, når der er mange børn på et medie. Og hos SnapChat er både Maps og Streaks manipulerende. Med Maps afgiver børnene deres lokation og bestemmer selv, hvem af deres venner der skal se, hvor de opholder sig. Det er lækkert lavet med små ikoner på et kort, hvor du kan zoomer helt ind på den konkrete adresse og se, at de tre veninder er samlet der i aften - uden dig. Hvad de færreste børn forstår er, at de samtidig giver deres lokation til SnapChat, der har brug for data til at sælge annoncer. Og SnapChat skriver som Facebook, Instagram, TikTok og alle de andre i deres betingelser, at man skal være 13 år for at bruge deres tjeneste. Det siger den amerikanske COPPA-lovgivning nemlig. At de fleste børn lyver sig ældre for at bruge tjenesten, er der ingen - bortset fra LEGO og EDULAB (se kapitel 5 om dataetik) - der gør noget ved.

At være offentlig

En god digital strategi er at tænke på sig selv i flere udgaver. Der er den offentlige dig. Den, som du gerne vil vise frem, når de søger på dit navn. Det er næsten som dit CV, når søgeresultatet kommer frem. Det kan være svært for børn at forstå, når de stadig kun har en privat identitet, men mange har en faglig færdighed, som de sagtens kan 'fremme' digitalt i deres eget navn. Men børn bør ikke bruge deres eget navn, før de forstår, hvad det vil sige at være et offentligt menneske. De risikerer at ødelægge det, dvs. man kan finde ting og sager om barnet, når man søger på dets navn, som barnet selv ikke ønsker skal være offentligt kendt, når det bliver større.

I 2013 skulle den 30-årige amerikanske Justine Sacco til Sydafrika på ferie. Da hun har stopover i Heathrow, tweeter hun en joke: "Going to Africa. Hope I don't get AIDS. Just kidding. I'm white!", springer på flyet og sover de 11 timer, det tager, hvor hun er offline. Da hun tænder sin telefon på landingsbanen, bliver hun overrumplet af beskeder. Hendes besked er gået viralt, og hun udsættes for en shitstorm af dimensioner. Den hvide racistiske bitch er landet, tweeter en bruger, der er taget ud i lufthavnen i Cape Town for at rapportere om hendes landing. I årene efter kan hun ikke få et nyt job (hun bliver fyret pga. beskeden) eller en kæreste, for når man googler hende, kom der en ting op på de første mange sider af svar: hvid, racistisk bitch.

Et tweet kan ødelægge ens liv. Det sker heldigvis for meget få, men det er vigtigt, at være obs på, at selvom man kun har 170 followers, som Sacco havde, så kan man godt gå viralt. Influencers og reality-stjerner, politikere og kunstnere er ofte offentlige mennesker. Mange af dem ville ønske, at de kunne være i fred engang imellem, for det kræver 'sin mand' og 'sin kvinde' at være offentlig.

Bagsiden af at være berømt blev helt tydelig, da realitystjernen og bloggeren Fie Laursen i sommeren 2019 lagde et selvmordsbrev på Instagram. Hun overlevede heldigvis - men hun er tydeligvis en sårbar og ulykkelig pige, som samtidig har over 300.000 followers og tilhører en gruppe af mennesker, som mange børn og unge ser op til og ønsker at blive!

Bagsiden af at være offentlig kan også ramme folk med handicap og sygdomme. Mange patientforeninger ønsker, at tabu skal forsvinde omkring en sygdom, og ønsker, at folk står frem

med deres sygdomme, men for mange almindelige mennesker kræver det styrke at stå frem med en sygdom. Også fordi der stadig er megen diskrimination på jobmarkedet i forhold til sygdomme.

Det er derfor en god ide at søge på sit eget navn engang imellem. Helst fra en andens computer, da du ellers risikerer bare at få personaliserede resultater efter dine egne præferencer og ikke kan se, hvad andre kan se om dig offentligt.

Ø V E L S E 2.1. 🧑🏻🗣️ (Privat vs offentlig video med diskussioner)

At være privat

Det er individuelt, hvad der er privat. Nogle homoseksuelle står frem til Gay Pride-parader, som bliver fotograferet, og fortæller dermed hele verden, at de er homoseksuelle. Andre er meget hemmelighedsfulde omkring det - måske fordi de bare ikke gider tale om det med andre eller rejser meget til Rusland eller Iran, hvor homoseksualitet er forbudt. Der er en lang række data, man bør overveje, om man vil være offentlig eller privat med. Viden, som mange tidligere er blevet diskrimineret, drillet, udelukket eller ekskluderet på grund af.

Det er

- Religion
- Helbred
- Race/hudfarve
- Hvem du stemmer på
- Seksuel orientering
- Alder
- Køn
- Økonomi

Her bør børn og voksne tænke og tale sammen om, hvorvidt de skal være offentlige med ovenstående. Også vores

- Lokation/IP-adresser
- Ansigter

Det er data, som er rigtig meget værd, fordi de kan afsløre utroligt mange intime detaljer om os, og derfor bør vi overveje at være sparsomme med at dele ud af dem.

Selv i et andet navn end dit eget bør du ikke dele data, som du anser som privat. Disse data deler du kun analogt eller på medier, som vitterligt er private

Deling

Du kan vælge at dele alt det, du vil, om dig selv, naturen og alt andet, der ikke har med andre mennesker at gøre. Så snart du vil dele noget med andre mennesker, hvor man kan genkende dem, skal du bede om samtykke (få et ja eller et nej). Det er ulovligt at dele indhold af andre uden deres samtykke. Tænk bare på den såkaldte Umbrella-sag, hvor 1004 unge blev anklaget for at dele nøgenfilm af andre uden deres samtykke. Der er givet fængselsstraffe og store bøder for det til flere af dem.

Med en social medie-profil har du din egen platform, du er din egen journalist og har adgang til et potentielt kæmpe publikum, som kan blive uoverskueligt stort, hvis der kommer en viral effekt. De sociale medier har demokratiseret adgangen til at komme ud med information i offentligheden. Før i tiden var det redaktører på aviser, radio og tv, der bestemte, hvem der

kunne komme til orde. I dag kan alle komme til orde via sociale medier. Derfor bør alle lære de etiske journalistiske regler og presseetiske retningslinjer, der bl.a. handler om ikke at offentliggøre data om andre, uden at de har givet samtykke.



Se denne video: Hvis din app var en bagerjomfru <https://vimeo.com/114229294>

Ø V E L S E 2.2. 😊 (Fakenamegenerator.com)

KAPITEL 3. DIGITALE FODSPOR¹⁰

Alt hvad du laver online, sætter digitale fodspor. Når du bruger en søgemaskine, besøger websites, køber varer, sender e-mails og chat-beskeder, uploader, downloader, ser videoer, hører musik, quizzes og så videre og så videre.

Børn er i stigende grad bevidste om, hvad cookies og algoritmer er - naturligvis flere i 7. klasse end i 4. klasse. Børns Vilkår har udarbejdet nogle fine undersøgelser (https://bornsvilkar.dk/wp-content/uploads/2019/03/BV_Digital_Dannelse_Del_4_11.03.19.pdf side 20 og frem) af, hvad og hvor mange børn der forstår hvad der sker af dataindsamling, når de bruger digitale medier. Fx ved 53% af børnene i 7. klasse, hvad cookies er, og 13% ved, hvad algoritmer er. Så ud over at forklare hvad teknologien kan, er det især sammenhængen til og forståelsen for demokrati, privatliv og rettigheder, som en lærer bør fokusere på.

Da internettet for alvor begyndte at blive brugt af den brede befolkning i 1990'erne, baksede mange virksomheder med, hvordan pokker de kunne tjene penge på tjenester via internettet. De manglede forretningsmodeller. Det var Google, der opfandt 'gratis'-modellen (se kap 1, 'forretningsmodeller baseret på data'). Gratis betyder, at den enkelte bruger får det gratis, men at man betaler med noget andet, nemlig sine data. Den mest gængse måde at betale med sine data er via cookies, der opsamler viden omkring alt, hvad vi laver på nettet - medmindre vi altså blokerer for det.



Hvis din app var en bagerjomfru <https://vimeo.com/114229294>

Cookies

Cookies er den ældste og mest udbredte måde at indsamle data på. De er i dag en fundamental del af 'gratis'-infrastrukturen på nettet og lægger sig på din gadget/computer, hver gang du går ind på et website, for at huske næste gang du kommer, hvad du laver, og evt. dele den viden med andre, der er en del af den såkaldte ad tech-industri. Langt størstedelen af alle websites bruger cookies.

Der er gode cookies og dårlige cookies.

Gode cookies kaldes også 1. part-cookies eller nødvendige cookies og sidder på alle websites og bruges til statistik og til at huske, hvad du har puttet i indkøbskurven eller dit password. Disse cookies deler ikke data med andre om dig.

Dårlige cookies kaldes også 3. part-cookies, marketing-cookies eller tracking-cookies og bruges på langt størstedelen af alle websites. Fx indeholder 89% af alle europæiske statslige websites disse cookies, ifølge en rapport fra Cookiebot. Det betyder, at hvis du går ind på patientforeningen alzheimer.dk, så ligger der tracking-cookies der, og de sladrer til andre om, hvad du laver på sitet. Det betyder, at patientforeningen giver en lille brik til det store puslespil/profil om/af dig. Jo flere brikker en virksomhed kan samle om dig, des mere detaljeret

¹⁰ Mere læsestof:

Digitalt selvforsvar - værktøjer - <https://dataethics.eu/da/selvforsvar/>

<https://www.esafetylevel.eu/>

<https://www.klicksafe.de/>

Rapport fra Cookiebot: <https://www.cookiebot.com/en/>

<https://www.cookiebot.com/media/1136/cookiebot-report-2019-ad-tech-surveillance-2.pdf>

<https://webbkoll.dataskydd.net/>

en viden får den og kan bruge profilen af dig til at ramme dig mere målrettet med såvel indhold som tilbud og ikke mindst priser.

Ø V E L S E 3.0 🤔 Dilemma om tracking cookies

Ø V E L S E 3.1 🤔 Analyser et website for cookies

Device fingerprinting

Cookies har udviklet sig over årene og bliver bedre og bedre til at tracke. Begrebet bruges her meget bredt - også såkaldt device fingerprinting.

Device fingerprinting er noget nyere og tracker også

- hvilken device du er på
- din taste-hastighed
- din IP-adresse
- hvad du har installeret af browser-add-ons
- tidspunkt du er på
- opløsningen på din skærm
- m.fl.

Det bliver altså sværere og sværere for brugerne at beskytte sig mod denne overvågning. For når vi ser på brugerundersøgelser generelt, er der stor modstand mod overvågningen via data, og flere og flere begynder at finde måder, hvorpå man kan beskytte sig imod den.

Blokér for tracking

Adblocking er en af de mest almindelige måder at beskytte sig mod web-tracking, og et stigende antal - især unge - benytter sig af det. De fleste adblockers blokerer i dag både for cookies og reklamer. Her er en liste over de bedste:

- Brug browseren **Cliqz.com**, så bliver der ikke indsamlet og delt identificerbare data om dig via cookies.
- Hvis du insisterer på at bruge Googles browser Chrome, som er den mest udbredte i dag, så kan add-on (tilføjelsen) [uBlock Origin](#) anbefales.
- **Ghostery.com** ejes af Cliqz, men kan installeres som en adblocker i så godt som alle browsere. Når den er installeret, skal du selv trykke på det lille blå spørgelses-ikon og sikre, at du har trykket på 'block all'.
- [Disconnect](#) er rigtig god til din computer. Med den ser du stadig reklamerne (og støtter dermed fx nyhedssider, der lever af det), men den blokerer for marketing-cookies.
- De to apps **AdblockFast** og **AdblockPlus** er blandt de bedste til dine mobile enheder. Slås til og fra med et enkelt touch på skærmen.

Disse adblockers anbefales, selvom du siger *Cookies Nej Tak* på de små bannere, som kommer frem, næsten hver gang du går ind på et website. Det er pga. EU-lovgivningen; et website, der opererer i EU, skal informere dig om cookies, men lovgivningen har i flere år været under revision (pga. stærk lobbyisme fra ad tech-industrien), og det er derfor ikke krystalklart, hvad der sker, når man siger nej tak. Det er altid bedst at bruge uafhængige tjenester som nævnt ovenfor.



Video: Sådan installeres en adblocker, og sådan virker den

Ø V E L S E 3.2 🧐: Installer en adblocker på computer eller mobil

Søgning og browsere

Når du søger på nettet, sætter du også digitale fodspor. Hvis du søger på søgemaskiner som Google og Bing, gemmer de data om dig som person og dine søgninger, hvad du søger på, og hvor du klikker. Du kan derfor vælge at bruge alternative søgemaskiner, der ikke profilerer dig. De tjener penge på samme måde, som Google gjorde i begyndelsen - nemlig kun på de ord, du søger på, og ikke på baggrund af massiv dataindsamling om dig, og alt det du laver og har lavet på nettet, så man kan personalisere søgninger og reklamer til dig. Her er nogle af de bedre alternativer, hvoraf nogle er baseret på Google og Bing, men hvor du bliver anonymiseret:

- [Startpage](#) (hollandsk)
- [Qwant](#) (fransk/tysk)
- [Mojeek](#) (britisk)
- [Hulbee](#) (schweizisk)
- [Metager.de/en](#) (tysk)
- [Duckduckgo](#) (amerikansk)
- [Searx.me](#) (meta søgemaskine for nørderne)

Det er vigtigt at forstå forskellen på en browser og en søgemaskine. Du kan bruge ovenstående søgemaskiner i alle browsere. Mange browsere har præ-installeret en søgemaskine, nemlig Google, fordi Google betaler for det (Firefox, Safari, Cliqz og selvfølgelig Googles egen Chrome). Så når du søger direkte i de browsere, bruger du google.com. Hvis du vil bruge en privat søgemaskine, skal du altså selv installere den i browseren. Cliqz er klart den bedste browser her, for den har allerede lagt de private søgemaskiner ind. Tryk på Cliqz, på Preferences og på Search - så kan du vælge en standardsøgemaskine som Startpage, Qwant eller Duckduckgo og dermed undgå at bruge Google hele tiden og fodre datamonopolet med flere penge (=data).

Ø V E L S E 3.3 🧐: Installer en privat søgemaskine

KAPITEL 4. DATASIKKERHED

Åbne wi-fi er også for hackere

Du sidder på en cafe og logger dig på cafeens gratis wi-fi. Du er på en halv time, og da du forlader cafeen, tænker du ikke mere over det. Men uden du aner det, har en hacker været inde på din telefon og taget en kopi af dine fotos, beskeder, passwords i din browser og meget mere. Hvordan pokker kan det ske?

Det kan ske på flere måder. Åbne gratis wi-fi netværk er generelt noget, du skal holde dig væk fra, medmindre du bruger VPN (se senere): Enten kan du komme til at logge på et netværk, som lokker dig til afgive data, uden at du nogensinde får adgang til et netværk, men hackeren får adgang til dine ting. Eller en hacker kan simpelthen komme ind på din gadget, mens du er på det åbne gratis wi-fi, fordi du ikke har beskyttet din gadget med en VPN, der krypterer trafikken mellem din gadget og så wi-fi'et. Så ud over at bruge en VPN, så tjek altid, at det netværk, du vil logge på, tilhører den café, du besøger. Endelig er det en god ide at slå den automatiske wi-fi login-funktion fra på din telefon (den, der hele tiden leder efter et wi-fi og forsøger at hoppe på, når den finder et), så du selv er i kontrol over, hvilke netværk du hopper på).

Phishing

Du får en e-mail fra Apple-ID, hvor de takker for din bestilling i App-store. Dit Apple-ID er blevet brugt til at handle med gennem App-store. Men du har ikke bestilt noget, og du tror, at andre har fået adgang til din konto. I givet fald skal du IKKE klikke på linket i e-mailen men logge direkte ind på Apple-ID og ændre din adgangskode med det samme.

Mailen er sandsynligvis en såkaldt phishing-mail, som du også kan få via fx Facebook Messenger. De lægger som regel op til, at du skal sende nogle vigtige persondata retur ved at klikke på et link, men din bank og andre seriøse virksomheder, du handler med, kunne aldrig finde på at sende dig sådan en mail.

Der er flere og flere kreative metoder til at lokke os med, og mange hopper i. Unge som ældre. Tryk heller ikke 'afmeld nyhedsbrev' i en mail, hvis du modtager sådan et link. Det er sandsynligvis også fup.

Phishing-beskeder kan genkendes på følgende måde:

- Det er for godt til at være sandt, fx at du har vundet 10 mio. kr. eller en ipad
- Kommer fra en modtager, du aldrig har hørt om før (klik på e-mail-afsender og se, hvad der står - hvis det er fra 'Apple', står der sandsynligvis noget andet med 'Apple' i
- Hvis beskeden ikke stemmer overens med, hvad du har foretaget dig på nettet
- Hvis der er stavfejl og sprogfejl, og de beder om dine personlige oplysninger, fx CPR-nr. eller kontonr.

Test evt. dig selv i quizzen her: <https://www.forbrug.dk/raad-og-rettigheder/snyd-og-bedrag/phishing/>

Passwords



Du bør ikke bruge det samme kodeord på de fleste eller alle dine tjenester. Det er alt for risikabelt; hvis nu en af dem bliver hacket, så kan man stjæle din identitet og bruge den på alle dine tjenester.

Men hvad gør man? Det er umuligt at huske mange lange og svære passwords. Det nytter ikke noget at skrive dem i dine noter på telefonen, for så er de for nemme at få fat i. Det samme hvis du skriver dem

ned på en seddel og har dem i din pung (men det er bedre end at have dem på dine noter i telefonen). Den allerbedste løsning er en såkaldt passwordmanager. Det kan fx være:

- Keepass.com
- 1password.com
- Lastpass.com

Der er en gratisversion på alle tre tjenester, men det er en god ide at betale for en af dem. Du kan bruge den på alle dine gadgets og din computer. Og du skal bare huske ét langt og svært password, der helst indeholder både tal, store og små bogstaver og et specialtegn såsom et komma eller udråbstegn. Dvs. når du skal ind på din passwordmanager-app, så skal du først bruge koden til din tlf./computer og derefter den svære kode til appen. Men herinde kan du så lægge alt fra dit kreditkortnummer til koder på alle dine tjenester.

Det er altid bedst at bruge uafhængige tjenester som en af de tre nævnte, men hvis du har en iphone, er der en indbygget passwordmanager under 'indstillinger', 'adgangskoder' og 'koder til websteder og apps', som du også kan bruge og sætte den til 'autoudfyld adgangskoder'. Det er i hvert fald bedre end ingenting, hvis du ikke orker en uafhængig passwordmanager.



Video: Mere om passwords og tofaktoridentifikation her : <https://nycdigitalsafety.org/module/securing-accounts-and-devices/>

Sådan sætter du dine mobil-indstillinger



Video: Lytter nogen med via din mobils mikrofon?

Med din mobil går du rundt med en tracking (sporing) device i lommen. Det betyder, at rigtig mange andre end dig kan følge med i, hvor du går hen, hvilken musik du hører, hvis du ser på frække billeder, hvor du køber ind, og hvad du køber ind mv. Mange af dine apps kan følge, hvor du er henne hele tiden og støvsuge alle dine fotos og kontakter, hvis du har givet dem tilladelse til det. De kan i princippet også lytte med på alt det, du taler om i den analoge verden. Det siger tech-virksomhederne, at de ikke gør (se video), men uanset hvad de siger, kan du overveje at kigge på, hvem der har adgang til din mikrofon i din mobils indstillinger.

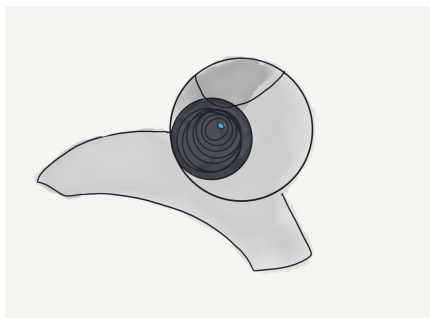
ØVELSE 4.0 🧐

Din IP-adresse (din lokation) er guld værd for mange virksomheder. Den fortæller mere om os, end de fleste tror. Hvor vi bor, går i skole og arbejder, hvilke fritidsinteresser vi har, vores venner og bekendte og ikke mindst vores interesser (sidder vi meget foran computeren og spiller spil, eller er vi ude og motionscykle). Lokation bruges også af mange virksomheder til at give dig en

personaliseret pris, fordi varer jo har forskellige priser fra land til land. Derfor kan du lukke for adgangen til din IP-adresse i din mobilts indstillinger.

ØVELSE 4.1 🧐

Dæk kameraet



Ud over indstillingerne på din mobil kan det være en ide at dække dit webcam til, når du ikke bruger det. En hacker kan hacke sig ind i din computer/gadget og se på dig gennem dit webcam. Det ér sket før - også i Danmark - fx da en DJ lurede på mange piger, før han blev stoppet og fik en dom. Du kan sætte tape eller et klistermærke eller en lille klap på din computer/gadgets webcam og så tage det af, når du skal bruge det.

Styr din IP-adresse med en VPN

Som beskrevet i kapitel 1, 'Prisdifferentiering', får du ikke nødvendigvis den samme pris på produkter og tjenester, som andre får, når du handler på nettet. Det afhænger af, hvor meget sælgeren ved om dig, især *hvor* du befinder dig i verden, når du er ved at købe noget. Regional prissætning er udbredt, især blandt amerikanske tjenester som Amazon og Hotels.com, men også flere og flere flyselskaber. Bor du i Tyskland, kan du ofte få det billigere, end hvis du bor i Danmark, hvor priserne generelt er højere. Det er umuligt at lave en guide til, hvordan du får billigere priser, da det er en gråzone og ikke foregår i det åbne. Men uanset hvad er det altid en god ide at kunne ændre sin IP-adresse og se, om man kan få prisen ned. Det betyder intet for levering af varer, betaling med dit danske kreditkort eller andet. Du er jo bare i udlandet, når du køber det.

For at ændre og kontrollere din IP-adresse/lokation skal du bruge en VPN (som står for Virtual Private Network). En VPN er vigtigt for datasikkerheden, fordi den krypterer trafikken mellem din gadget og nettet (den wi-fi eller server du er på). Den fungerer som en slags vejbohm på den digitale landevej. Når du går på gratis og åbne wi-fi, der ofte er på hoteller og cafeer, så sikrer din VPN, at ingen kan hacke dig. Og med VPN-tjenesten kan du så også kontrollere din lokation og selv bestemme, hvor i verden, du ønsker at befinde dig digitalt. Ud over at du kan opnå billigere priser med en VPN, kan du fx også se dansk tv, mens du er i udlandet, så længe den VPN-tjeneste du har købt, har servere i Danmark.

De gode VPN-tjenester koster penge (men så betaler du heller ikke med dine data). Når du vil købe en VPN-tjeneste, er det en god ide at vælge en, der er udviklet af et europæisk firma, da de er underlagt stramme europæiske regler. Og vælg en med mange servere i de lande, du har brug for at være i digitalt.

Eksempler på nogle gode VPN-værktøjer:

- IBVPN.com (rumænsk) - mange servere
- Earthvpn.com (cypriotisk) - mange servere
- F-secure.com (finsk)
- Ipredator.se (svensk)

Med den norske browser Opera kan du få gratis adgang til en VPN, men du kan ikke vælge det land, du vil være i, kun kontinent. Download browseren på opera.com gå ind i indstillingerne under 'beskyttelse af personlige' og scroll lidt ned. Her kan du aktivere VPN, så kan du lade, som om du er i en anden region.

Du kan altid se din IP-adresse på [Whatismyipaddress.com](https://whatismyipaddress.com).

 Video: Sådan installerer du VPN.

ØVELSE 4.2 😊

KAPITEL 5. DATAETIK, DATARETTIGHEDER & NY TECH¹¹

Hvad er dataetik (definition og principper)

Dataetik er ansvarlig og bæredygtig brug af data. Dataprocesser bør være designet som bæredygtige løsninger - dvs. først og fremmest til gavn for mennesket.

Dataetik er skridtet videre end efterlevelse af persondatalovgivningen. Før vi kan tale om dataetik, skal vi altså efterleve EU's lovgivning inklusive GDPR, General Data Protection Regulation.

De 5 principper inden for dataetik lyder sådan:

1. MENNESKET I CENTRUM

Menneskets interesse har altid forrang for institutionelle og kommercielle interesser. Mennesket er unikt med empati, vilje, uforudsigelighed, intuition og kreativitet, og mennesket har altid højere status end maskinen.

2. INDIVIDUEL DATAKONTROL

Det er det enkelte menneske, der har den primære kontrol over, hvad deres data bruges til og i hvilke sammenhænge, samt over hvordan deres data aktiveres. Fremfor at kontrollen over data ligger hos staten eller virksomheder.

3. GENNEMSKUELIGHED

Databehandling og automatiserede beslutninger skal give mening for det enkelte menneske. De skal være transparente og skal kunne forklares.

4. ANSVARLIGHED

Ansvarlighed er en organisations bevidste, saglige og systematiske brug og beskyttelse af persondata. En organisations ansvarlighed bør også gælde for underleverandører og samarbejdspartnere.

5. LIGE VÆRDIGHED

Demokratisk databehandling tager udgangspunkt i, at dataprocesser er med til at bevare, reproducere og skabe magtfordelingen i samfundet. I en databehandling skal der tages særlige hensyn til sårbare mennesker og undgå at udsætte dem for diskrimination eller stigmatisering.

¹¹ Mere læsestof:

- Dataetisk spørgeramme: <https://dataethics.eu/da/dataetiske-principper/>
- <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top> side 28
- Arbejdsbetingelser hos Amazon <https://edition.cnn.com/2019/07/15/business/german-amazon-workers-strike-prime-day-scli-intl/>

Hvordan ved man, om en tjeneste er dataetisk?

For at en tjeneste er dataetisk, skal den 1) efterleve GDPR og anden data-og menneskerettighedslovgivning og 2) leve op til en række dataetiske krav. Det er svært selv at vurdere, om en tjeneste er ok at bruge eller ej, og i fremtiden vil vi også kunne få hjælp til sådanne overvejelser af professionelle organisationer, der tester og whitelister tjenester efter, hvor etisk ansvarlige de er med persondata - lige som vi gør med fair trade og økologi. Men der er ikke mange af disse tjenester endnu. I USA findes CommonSense Media (<https://www.commonsensemedia.org/>), der tester produkter målrettet børn, inklusive EduTech, men det er baseret på amerikanske værdier og lovgivning, som ikke er lige så god som i Europa.

Nedenfor er en række spørgsmål, du kan prøve at stille dig selv og undersøge på tjenestens hjemmeside under Terms of Conditions / Handelsbetingelser og/eller Privacy Policy / privatlivspolitik, datapolitik og/eller cookie-politik. Overordnet skal du vurdere, om brugervilkårene og privatlivspolitikken er rimelig og forståelig.

Generelle spørgsmål

- *Hvad lever virksomheden af? Dine data eller dine penge? (man kan godt give lidt væk, men oftest vil det være for at reklamere for noget andet, du så skal betale for)*
- *Hvor har tjenesten hovedsæde? (kan være svært se finde ud af, men prøv: <https://craft.co>) (EU har den bedste lovgivning)*
- *Kan du se, hvilke mennesker der står bag hjemmesiden?*
- *Hvad har andre evt. skrevet om virksomheden?*
- *Er det for godt til at være sandt, dét, den giver eller lover?*



Privatlivspolitik

- *Har virksomheden en privatlivspolitik eller en datapolitik, du som lægmand kan forstå?*
- *Hvilke data indsamler tjenesten, hvorfor og hvordan?*
- *Hvordan beskytter tjenesten brugernes data?*
- *Hvor opbevares data? (hvis de ikke skriver noget om det, kan man altid undersøge det her: <https://webbkoll.dataskydd.net>)*
- *Er der rimelige begrænsninger i tjenestens dataindsamling?*
- *Sælges eller videregives data til tredjepart? (ikke ok)*
- *Sælges data som mønstre i aggregeret anonymiseret form? (ok)?*
- *Bruger tjenesten 3. part-cookies - altså de cookies, som deler data med alle mulige andre? Hvis de ikke skriver noget om det i deres privacy policy, kan du altid tjekke det her: <https://webbkoll.dataskydd.net/>)*
- *Hvilke muligheder har brugerne for selv at skjule eller slette data?*
- *Får man en fornemmelse af, at tjenesten prioriterer brugerens rettigheder over kommercielle eller institutionelle interesser?*
- *Benyttes privacy by design-principper (er optimalt, hvis de gør)?*
- *Behandler tjenesten data på din device, fx telefonen, frem for at trække data over på en server i virksomheden? (Apple og HelloClue bruger 'on device processing' - se under dataetiske eksempler)*
- *Bruger tjenesten data til at profilere og forudse adfærd på individ-niveau (ikke godt medmindre du selv har bedt om det)*
- *Er der tale om manipulerende adfærdsdesign? Et eksempel på det er SnapChat, der med SnapMaps lokker lokationen ud af børn, så de på en map kan se, hvor deres venner er.*

Eller man skaber afhængighed med Streaks; hvis du ikke svarer inden for 24 timer på en samtale på SnapChat Streaks, ryger du ud, hvorfor børnene passer hinandens telefoner.

ØVELSE 5.0 🧐 (Kahoot)

Dataetiske eksempler

Der er endnu ikke et mylder af rollemodeller inden for dataetik. Men mange både offentlige og private virksomheder og instanser arbejder med dataetik i beta. De er på vej. De gør noget. Og det er bedre end ingenting.

LEGO & Edulab - Både LEGO og Edulab har med børn at gøre, hvorfor de er blandt dem, der først arbejdede med dataetik - også selvom det samme ikke er tilfældet for LEGO's konkurrenter i fx USA. Begge virksomheder opererer ikke med 3. part-cookies - herunder Facebook Connect og Google Analytics. De deler altså ikke børns data med tredjeparter. De lagrer data i Danmark eller Europa, modererer alt indhold, *før* ungerne ser det (ikke som YouTube, hvor indhold skal anmeldes, før det evt. tages ned). Edulab har også dataetiske retningslinjer¹², og hverken Edulab eller LEGO bruger manipulerende adfærdsdesign eller støtter mindreårige Youtuber-influencere.

AULA - den nye danske kommunikationsplatform for lærere, forældre og elever har mange dataetiske elementer og har også en dataetisk politik¹³: Meget af det, LEGO og Edulab gør, gør AULA også. AULA, der er ejet og betalt af KL, har desuden besluttet, at der ikke skal være *likes* på platformen, da det ikke passer ind i den danske pædagogiske tradition og ofte er grund til mobning. Eneste etiske udestående hos AULA er, at de bruger Amazon Web Services. Det kan sagtens være fuldt ud lovligt, men det er ikke ensbetydende med, at det nødvendigvis er etisk forsvarligt. I hvert fald reagerede en del forældre negativt på det, da det kom frem. Der er mange etiske argumenter imod Amazon, der af nogle kritiseres for at være et aggressivt datamonopol, der ikke betaler skat i Europa, og som behandler deres medarbejdere særdeles dårligt.

Apple - Apple tjener langt de fleste penge på at sælge gadgets - computere, iPads, iPhones samt tilbehør. Dermed adskiller den sig væsentligt fra rene databaserede virksomheder, der primært lever af data og annoncering, fx Google og Facebook.

Apple arbejder med privatliv på en seriøs måde med følgende principper¹⁴:

- Personlige gadgets er private gadgets, og det er *dine* beskeder, fotos og kontakter etc.
- Individer skal kunne kontrollere, hvilke data der indsamles om dem, og hvad de bruges til
- Enten indsamler Apple ikke data, eller også lader Apple data være på folks egne gadgets - såkaldt on-device-processing (vores gadgets har så megen computerkraft i dag, at man kan gøre det). Hvis Apple trækker data ind på deres egne servere, så anonymiseres data, siger Apple.

Apple har desuden privatlivs-ekspertter med i alle innovative processer og tager ansvar for underleverandører og IOS-platformen.

Clue - Clue er en tysk app, der efterlever den strenge tyske datalov modsat en af konkurrenterne Glow, som i USA ikke er underlagt samme strenge lovgivning. I USA er det kun læger og forsikringsselskaber, der skal efterleve en streng sundhedslov, når de håndterer

¹² <https://edulab.dk/vi-tager-ansvar/>

¹³ <https://aulainfo.dk/wp-content/uploads/Aulas-dataetiske-regels%C3%A6t.pdf>

¹⁴ <https://dataethics.eu/da/apples-dataetiske-forretningskultur/>

sundhedsdata. Alle andre - som apps, der indsamler sundhedsdata - reguleres efter en slappere forbrugerlov. Clue har en meget specifik og forståelig privatlivspolitik¹⁵, og du kan bruge den anonymt, hvis du ikke vil have personaliseret rådgivning. Clue profilerer ikke deres kunder, og dine adfærdsdata lagres separat fra dine identitets-data. Hvis du vælger en anonym konto, lover de: "If you don't register an account with Clue, all of your data will be stored solely on your device."

Google Education

I USA kan man tale om en googlifikation af klasseværelset, som Google har erobret fra Apple og Microsoft med billige labtops og 'gratis' apps¹⁶. Googles motivation er ikke nødvendigvis at tjene penge på skolerne, men at fostre generationer af fremtidige kunder. Jo tidligere man får loyalitet, des bedre kunder. Mange er bekymrede for dette og børnenes ret til privatliv, men Google siger, at Google Drive aldrig bliver skannet for data for at sælge adgang til brugerne - modsat gmail, search og alle de andre 'gratis' services fra Google.

Mange skoler i Danmark gør som i USA. I Århus har kommunen besluttet, at alle skolerne skal bruge Google Suite for Education (GSfE) og forsikrer¹⁷, at *"Når dit barn er logget ind i GSfE på skolen med sit UNI-Login, viser løsningen hverken annoncer eller reklamer. Google indsamler og anvender heller ikke dit barns data i reklameøjemed."* Den enkelte skole lover desuden¹⁸:

- Google ejer ikke dit barns data. Du og dit barn har til enhver tid ret til de dokumenter og data, dit barn gemmer i Google. Forlader dit barn skolen, vil konto med tilhørende data automatisk blive slettet
- Google er annoncefri. Google anvender derfor ikke dit barns data til andre ting - hverken til marketing eller videresalg

Datarettigheder¹⁹

Med GDPR har den enkelte europæer fået nye rettigheder til egne data, som de ikke har i de fleste andre lande. Disse rettigheder betyder, at man faktisk kan kontrollere sine egne data, og at EU arbejder for et datademokrati (se kap 1).

Disse rettigheder er kort sagt:

- **ADGANGSRET.** Du har ret til at få information om behandlingen af dine personoplysninger (gratis)
- **RET TIL BERIGTIGELSE.** Du kan få rettet forkerte, unøjagtige eller ufuldstændige personoplysninger
- **RET TIL SLETNING.** Du kan anmode om at få personoplysninger slettet, når de ikke længere skal bruges, eller hvis det er ulovligt at behandle dem. Der er dog data, som anden lovgivning kræver bevares i et række år, fx bogholderi
- **RET TIL BEGRÆNSET DATABASEHANDLING.** Du kan anmode om begrænsning af behandlingen af dine personoplysninger i bestemte tilfælde

¹⁵ <https://helloc clue.com/privacy>

¹⁶ <https://www.nytimes.com/2017/05/13/technology/google-education-chromebooks-schools.html>

¹⁷ <https://aarhus.dk/borger/pasning-skole-og-uddannelse/skole-sfo-og-klub/foer-dit-barn-starter-i-skole/en-god-skolestart/samarbejde-mellem-skole-og-hjem/foelg-med-i-dit-barns-hverdag/google/>

¹⁸ <https://docs.google.com/document/d/16aBuWm5vzDFUWJPeDuf4nN8Fa0Hfrr3rWOgrOH5Kqf0/edit#heading=h.z6scema44j86>

¹⁹ Mere læsestof:

<https://www.medieraadet.dk/medieradet/nyheder/gdpr-fortalt-til-unge>

- **RET TIL DATAPORTABILITET.** Du har ret til at få udleveret dine personoplysninger i et maskinlæsbart format og sende dem til en anden virksomhed, myndighed eller organisation
- **RET TIL INDSIGELSE.** Du er berettiget til at gøre indsigelse mod visse typer databehandling, fx til markedsføringsformål eller af årsager, der omhandler bestemte forhold, der gælder for dig
- **RET TIL AT SIGE NEJ TIL PROFILERING OG AUTOMATISKE BESLUTNINGER.** Du kan anmode om, at automatiske afgørelser, som omhandler eller i betragtelig grad påvirker dig, og som er baseret på dine personoplysninger, træffes af fysiske personer og ikke kun af computere

Det er desuden forbudt:

- **AT PROFILERE BØRN UNDER 13 ÅR.** Dvs. indsamle data om børn og bruge dem til at målrette budskaber, da de er manipulerbare
- **AT INDSAMLE DATA, DER IKKE ER RELEVANTE**
- **AT OFFENTLIGGØRE BILLEDER AF BØRN,** der kan genkendes uden at have fået **SAMTYKKE**
- **AT DELE DATA** om børn via fx cookies (det kommer mange udenom ved bare at skrive i handelsbetingelserne, at man skal være 13 år. Så hvis børn bruger tjenesten, er det dermed på eget ansvar).

På det norske site slettmeg.no kan man få hjælp til at slette alle mulige profiler af sig selv på nettet. Datatilsynet har en række vejledninger om GDPR²⁰.

Når skaden er sket

Har du skrevet noget dumt, sendt et åndssvagt foto ud eller bare ønsker noget slettet, så er det nogle gange muligt at få det fjernet, hvis det ikke har fået et viralt liv (er blevet delt mange gange). Du skal altså gå til originalkilden og bede om at få det fjernet. Det kan være dig selv eller en veninde, det kan være en hjemmeside med en debat, hvor du har fortrudt din opførsel. Mange vil fjerne det, der står, hvis du beder om det. I nogle tilfælde kan du bede om at få fjernet dit eget navn og i stedet indført et pseudonym, fx hvis det er en debat, og de gerne vil bevare dit indlæg. Hvis de ændrer dit navn, forsvinder forbindelsen mellem dit navn og udtalelsen fra Google efter kort tid, når man søger på dit navn på Google.

Hvis du bliver ringet op af mange sælgere, kan du få dit telefonnummer slettet på robinsonlisten.dk, og hvis du vil have hemmeligt telefonnummer, skal du kontakte dit teleselskab, da dit telefonnummer i Danmark som udgangspunkt er offentligt.

²⁰ <https://www.datatilsynet.dk/generelt-om-databeskyttelse/vejledninger-og-skabeloner/>

Ny teknologi²¹

Tech-industrien har travlt med at få alt connected digitalt i fremtiden. Seneste påhit er fx chips i bleer, så forældre ved, hvornår de skal skifte ble²². Med tracking devices i alt via chips og sensorer bliver det sværere og sværere at købe en bil, en kaffemaskine, et stykke tøj eller en støvsuger, der ikke er forbundet til internettet. Internet of Things bliver stort og nogle gange heldigvis også til fordel for brugerne. Men hvad der ofte glemmes i denne hastige udvikling, er det helt basale spørgsmål: Hvorfor? Er det her virkelig need-to-have eller bare nice-to-have? Hvorfor skal min kaffemaskine egentlig være forbundet til internettet? Så jeg kan fjernstyre den fremfor at bevæge mig ud i køkkenet og trykke på knappen? Hvorfor skal mit barns bleer? Eller mit tøj være det? Måske kan det give mening, at det indeholder en RFID-chip i tøj, der kan tracke tøjets livscyklus, men det skal så heller ikke kunne mere end det. Og ja, måske er det en god ide at lade sin bil overvåge din adfærd, hvis der sker et uheld, og du kan bevise, at det ikke var din skyld - eller betale mere i præmie, hvis det var. Men i givet fald skal de data, bilsælgeren eller forsikringsselskabet indsamler om din adfærd, slettes, så snart der ikke er brug for dem mere - fx løbende efter 24 timer kunne man slette dem. Så er risikoen for misbrug til andet formål elimineret.

Men ikke nok med at chips og sensorer skal ind i ting og forbindes til internettet - såkaldte transhumanister arbejder også for at forbinde os mennesker. Fx er Tesla-ejeren Elon Musk i gang med et projekt, hvor han vil lagre den menneskelige hukommelse på en chip. Og så er der hele Singularitets-bevægelsen, der kommer ud af Silicon Valley og Google, nemlig dem, der tror på, at menneske og computer smelter sammen, og computeren passerer den menneskelige hjerne. Tjek også HBO-serien Year and Years, hvor teenagedatteren ønsker at bliver digitaliseret og gjort udødelig.

En stor del af fremtiden bliver ikke kun at stille krav til teknologi-producenterne om at kunne neutralisere sin kaffemaskine eller kunne købe én, der slet ikke er forbundet til nettet og at behandle vores data etisk ansvarligt, hvis de skal have vores data, lade os selv kontrollere dem og slette dem, når vi vil. En anden væsentlig del bliver at bevare den menneskelige kontrol, den menneskelige krop og form og de demokratiske værdier, vi arbejder efter i Europa, så det hverken er staten eller store tech-og AI-baserede virksomheder, der kontrollerer vores liv.

²¹ Mere læsestof: <https://www.economist.com/science-and-technology/2019/07/18/elon-musk-wants-to-link-brains-directly-to-machines>

²² <https://edition.cnn.com/2019/07/19/tech/pampers-smart-diapers/index.html>

ØVELSER

ØVELSE 1.0 🤖

Hovedstadsregionen beder om budget til at betale TDC eller et andet nordisk teleselskab om at sikre gratis wifi i smart city. Det bliver afvist, for Google har tilbudt gratis wi-fi.

Jeg kan under ingen omstændigheder acceptere Google (Huawei eller andre big tech corporations) bliver en del af vores vitale infrastruktur

Det er en okay gave, når det offentlige er så presset på økonomi og store virksomheder tilbyder deres hjælp



Vælg et af de to svar på dilemma-spørgsmålet og gå til højre eller venstre i klasseværelset efter lærerens anvisninger. Eleverne argumenterer og drøfter, hvorfor de står, hvor de står. De må gerne skifte plads.

Husk at inddrage TDC's beslutning om at droppe kinesiske Huawei til at hjælpe med at opbygge 5G- netværket for i stedet at vælge svenske Ericsson.

ØVELSE 1.1 🤖

Når noget er gratis, er du produktet, siger man. Fordi man i stedet for penge betaler med sine data. Er det okay?

- 1) Ja det er helt fint med mig. Hellere gratis og betale med data end at betale med penge.
- 2) Nej, det er uigennemskueligt, hvilken pris man betaler. Hvad er min fødselsdato og min kroniske sygdom værd? Så hellere betale med penge.



ØVELSE 1.2 🧐

Algoritmer er trænet på rigtig mange data. Det kan give præcise og brugbare resultater, og kriterierne bag kan være svære at forklare.

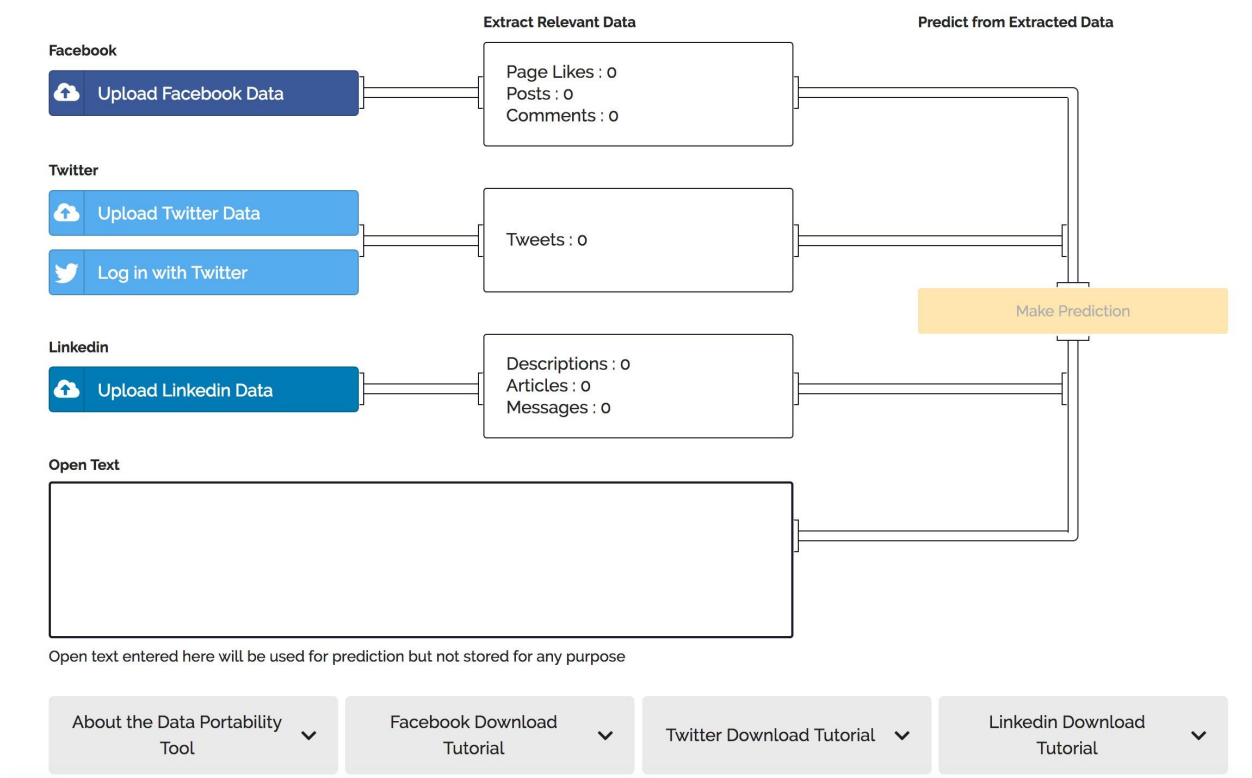
1. Jeg har travlt. Algoritmer gør det nemt for mig. Jeg har tillid til, at jeg får en nogenlunde okay pris og søgeresultat

2. Jeg kan ikke acceptere algoritmer uden en forklaring. Jeg vil forstå hvordan og hvorfor



Vælg et af de to svar på dilemma-spørgsmålet og gå til højre eller venstre i klasseværelset efter lærerens anvisninger. Eleverne argumenterer og drøfter, hvorfor de står, hvor de står. De må gerne skifte plads.

ØVELSE 1.3 🧙‍♂️



Gå ind på <https://applymagicsauce.com/> og log på med din twitter-konto, upload dine Facebook-data (følg instruktionsvideoen) eller nemmere: copy paste en engelsk tekst ind i tekstfelts-analyse og se, hvordan algoritmen analyserer dig.

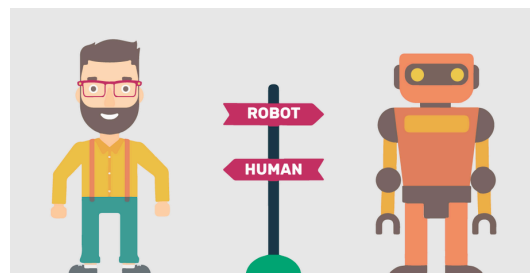
ELLER: find en af Greta Thunbergs taler - https://www.fridaysforfuture.org/greta-speeches#greta_speech_apr16_2019 - og analyser den med applymagicsauce.com

ØVELSE 1.4 🤖

Automatiske afgørelser baseret på kunstig intelligens i forvaltninger kan gøre enhver sagsbehandling lynhurtig både når det gælder sociale ydelser og byggetilladelser

Nej tak. Det har jeg ikke tillid til. Det skal ske via mennesker

Ja lad os få automatisk afgørelser ind, så jeg kan få omgående svar på mine ansøgninger



Vælg et af de to svar på dilemma-spørgsmålet og gå til højre eller venstre i klasseværelset efter lærerens anvisninger. Eleverne argumenterer og drøfter, hvorfor de står, hvor de står. De må gerne skifte plads.

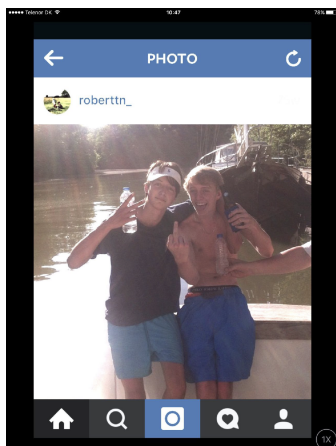
ØVELSE 2.0 🧐

Tjek dine Facebook-'privatlivs-indstillinger'. (Indstillinger og så to steder: 'privatliv' samt 'timeline' og 'tagging').

Især bør du undersøge, om alle kan se dine venner, eller det kun er dig, om din Facebook-profil kan findes via søgemaskiner, og om du har slået den knap til, der gør, at andre ikke kan tagge dig, uden at du giver samtykke (siger ja) til det først.

Tag desuden en diskussion to og to om, hvor I synes, grænsen for deling skal gå. Er det ok at tagge din ven i et vildt grimt foto på Facebook? Er det ok at dele fotos af andre, så man kan genkende dem?

ØVELSE 2.1 🤔🎥



Se video 1 og video 2 ([link](#)) med Robert, der ville til USA efter 9. klasse, men først var nødt til at rense sine digitale fodspor.

Stop, når den anbefaler det, og diskuter de forskellige spørgsmål, der stilles undervejs - herunder især: Hvad betyder kulturforskelle?

Slut med sidste billede med listen over, hvad der er private områder for mange og diskuter, hvilke områder I synes er private for jer.

ØVELSE 2.2. 🧐

Opret et pseudonym/kælenavn/alias på Fakenamegenerator, som du kan bruge andre steder end der, hvor du er professionel/faglig.

HUSKETIPS

- Stjæl aldrig andres navne
- Lad aldrig som om du er en anden, end den du er
- Snyder aldrig dine venner eller andre mennesker. De skal kende dit kælenavn.
Det er for beskyttelse, så du evt. kan begynde at bruge dit eget navn, når du skal opbygge din professionelle identitet
- Del ikke ting i et andet navn, som du synes er private

ØVELSE 3.0. 🍪

Marketing-cookies har eksisteret i mange år og findes på så godt som alle websites. Det betyder, at der deles data med i tusindvis af andre websites.

Alle offentlige websites og sites med følsomme data såsom medicinkøb eller en patientforening burde stoppe med at deltage i den datadeling omgående

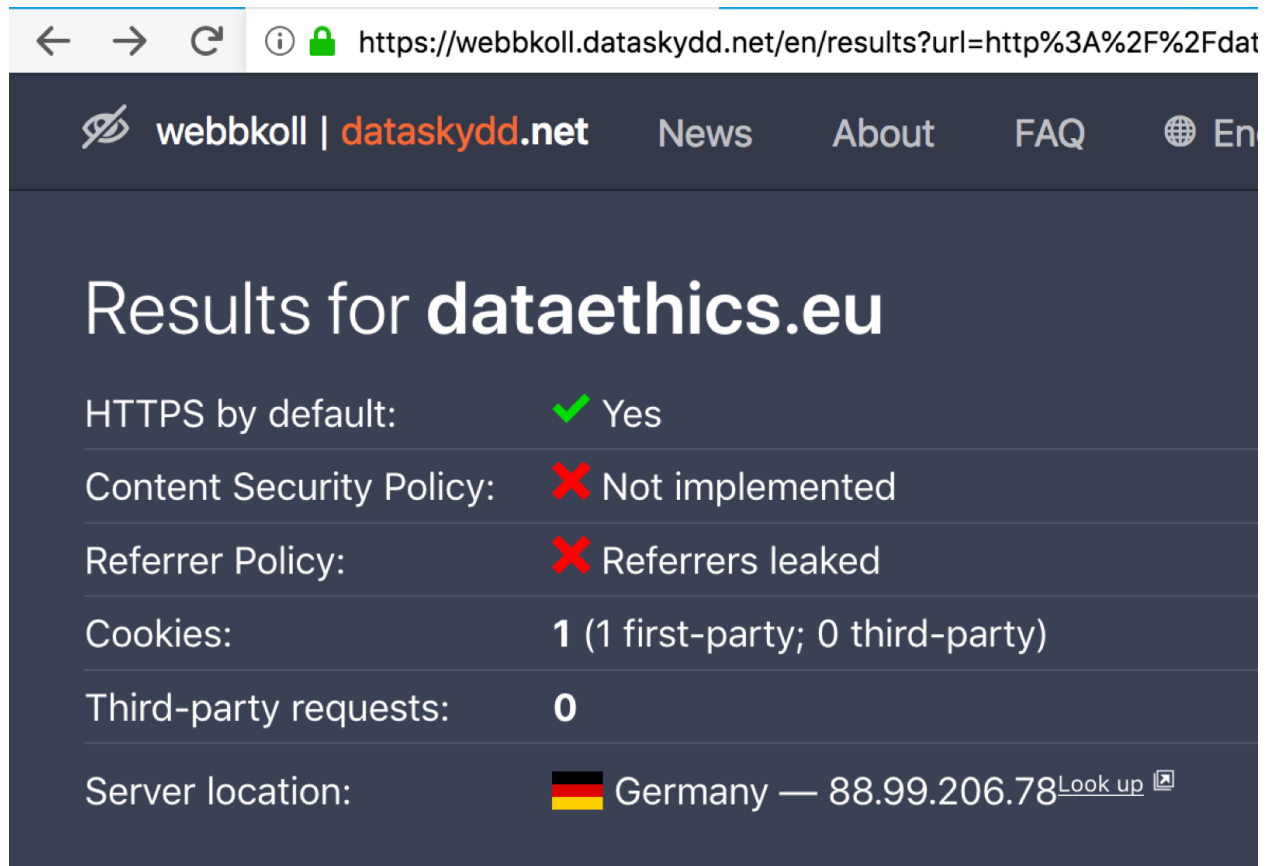


Det er ok, at det offentlige og andre deltager i den datadeling, da de også har brug for viden om, hvad deres brugere laver andre steder end hos dem selv

Vælg et af de to svar på dilemma-spørgsmålet og gå til højre eller venstre i klasseværelset efter lærerens anvisninger. Eleverne argumenterer og drøfter, hvorfor de står, hvor de står. De må gerne skifte plads.

ØVELSE 3.1. 🧐

Analyser websites for cookies. Brug dette fine værktøj: <https://webbkoll.dataskydd.net/> som både viser, hvad der ligger af 1. og 3. part cookies samt hvilket land, websitet lagrer sine data i. Eksemplet nedenfor er et af de helt rene websites.



The screenshot shows a web browser window with the URL <https://webbkoll.dataskydd.net/en/results?url=http%3A%2F%2Fdataethics.eu>. The website header includes the logo 'webbkoll | dataskydd.net' and navigation links for 'News', 'About', 'FAQ', and a language selector 'En'. The main content area displays the title 'Results for dataethics.eu' and a list of security and privacy metrics:

HTTPS by default:	✓ Yes
Content Security Policy:	✗ Not implemented
Referrer Policy:	✗ Referrers leaked
Cookies:	1 (1 first-party; 0 third-party)
Third-party requests:	0
Server location:	🇩🇪 Germany — 88.99.206.78 Look up 🗺️

ØVELSE 3.2 🤗

Installer en adblocker på computer eller mobil. Se videoen (link) og prøv så selv:

Cookie- og adblockers

Ghostery.com



Disconnect.me/disconnect

Ublock.org



Adblockfast - app

ØVELSE 3.3 🤔

Installer en privat søgemaskine i din browser, så den bliver standardsøgemaskine:

- [Startpage](#) (hollandsk)
- [Qwant](#) (fransk/tysk)
- [Mojeek](#) (britisk)
- [Hulbee](#) (schweizisk)
- [Metager.de/en](#) (tysk)
- [Duckduckgo](#) (amerikansk)
- [Searx.me](#) (meta søgemaskine for nørderne)

ØVELSE 4.0. 🧐

Hvad har dine apps adgang til?

Iphone:



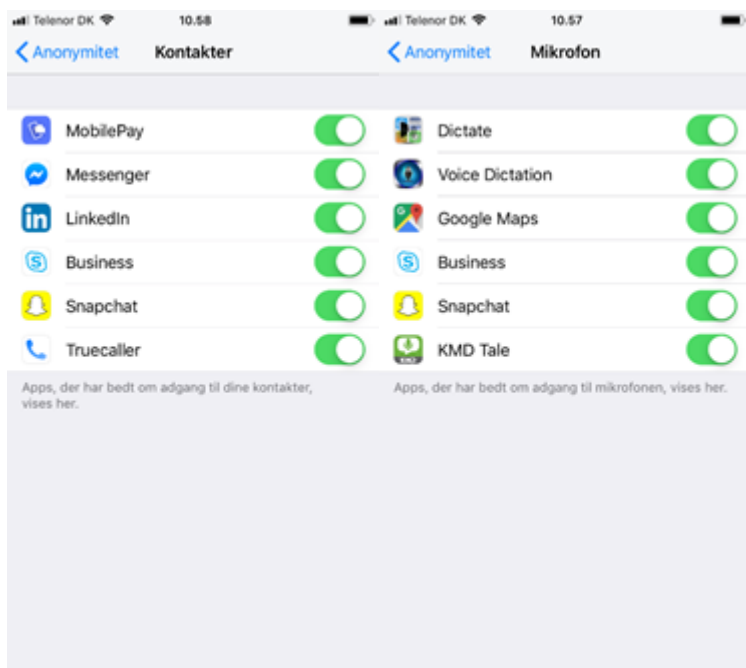
Følgende indstillinger findes under:

Scroll til den nederste del af indstillinger. Her finder du alle installerede apps og kan se, hvad de har adgang til.

Vælg forskellige apps og læg mærke til, hvad de har adgang til.



Du kan også se dine apps' adgang på en anden måde. Vælg 'anonymitet' under indstillinger og undersøg, hvilke der fx har adgang til mikrofon eller kontakter.



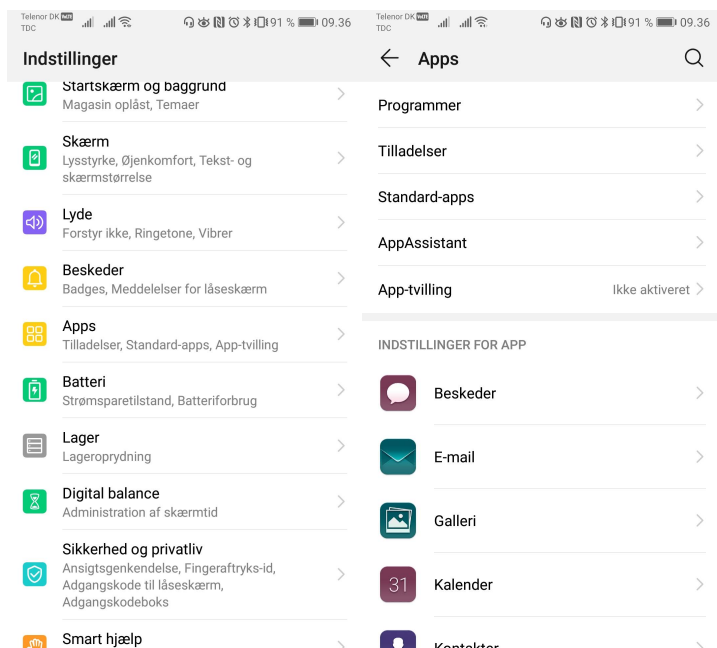
Android:

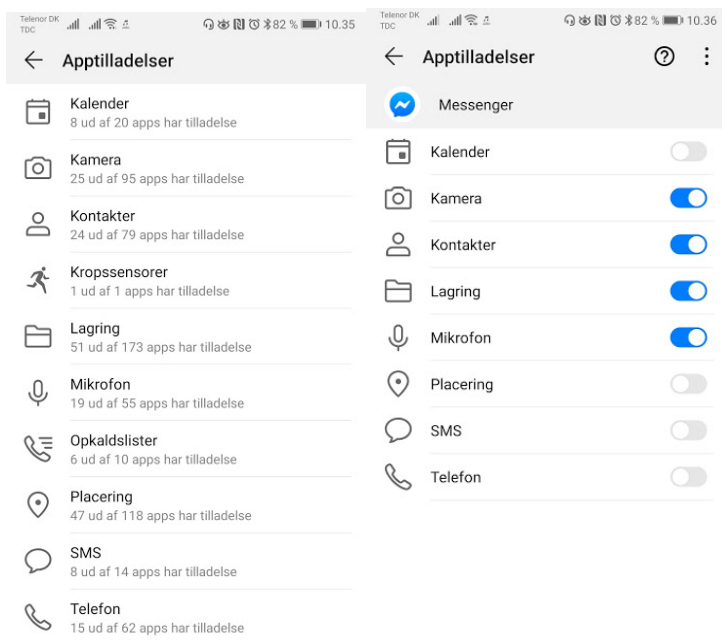
Der kan være lidt forskel på, hvordan det ser ud, alt efter hvilken version android man har installeret, og hvilken telefon man har.



Følgende indstillinger findes under:

Scroll til den midterste del af indstillinger. Her finder du 'apps' og kan se, hvad de har adgang til. Du kan enten trykke på 'programmer' og se, hvilke tilladelser de enkelte apps har, eller du kan trykke på 'tilladelser' og få et overblik over hvilke apps, der har adgang til hvad.

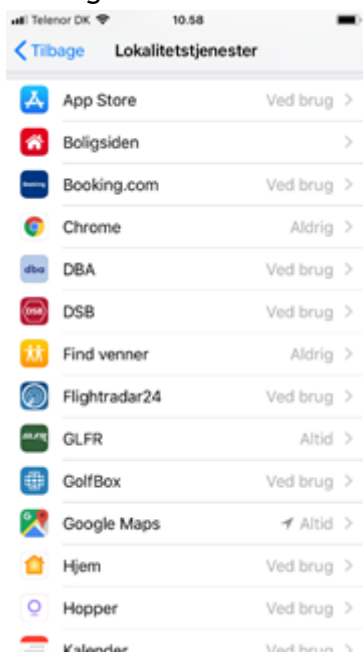




ØVELSE 4.1. 🤔

Iphone:

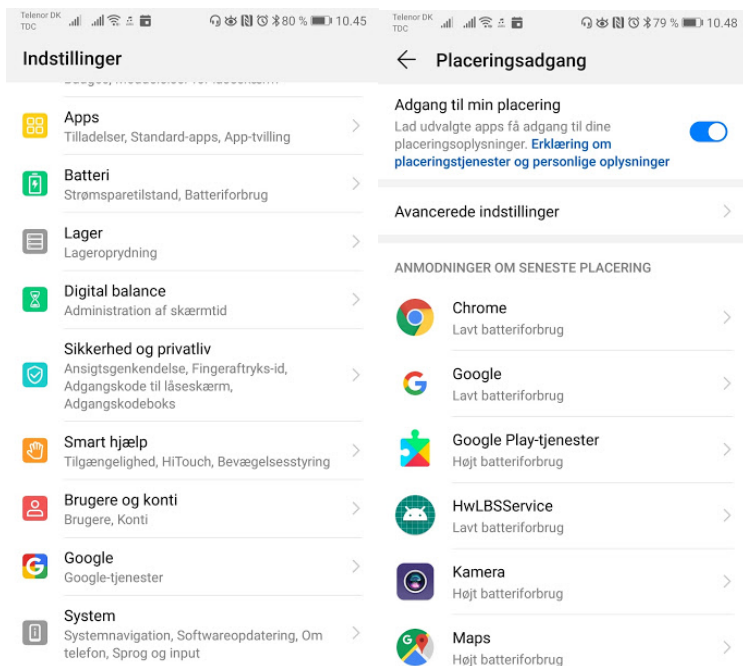
Gentag øvelse 4.0 bare med 'lokalitetstjenester' under 'anonymitet'.



Hvis du har en iPhone, kan du se alle de lokationer, du er mest på - og slå dem fra, hvis du ikke har tillid til Apple (se under dataetik). Gå ind på 'indstillinger', 'anonymitet', 'lokalitetstjenester', scroll ned til 'systemtjenester' og tjek 'væsentlige lokaliteter'. Her kan du se alle de steder, du kommer og hvor mange gange, du har været der. Ifølge Apple har de ikke adgang til de data. De ligger kun på din device.

Android:

Gentag øvelse 4.0 bare med 'placeringsadgang' under 'sikkerhed og privatliv'.



Hvis du har en Android-telefon, kan du se, hvilke placeringer du har været på - og slå dem fra ved at gå ind på 'sikkerhed og privatliv', 'placeringsadgang', scroll ned i bunden og vælg 'Google placeringshistorik'.

Ø V E L S E 4.2 🧐

Installer og brug en VPN (en købt eller gratis Opera.com, hvor man ikke selv kan bestemme land, kun region).

📺 Video: Sådan installerer du VPN.

Se videoen og køb og installer en VPN.

ØVELSE 5.0. 🏡

Kahoot bruges ofte i undervisningen af både lærere og elever. I denne øvelse prøver vi at tjekke, om Kahoot egentlig er forsvarligt for en skole at bruge i forhold til dataetik - herunder hvilke vilkår og betingelser, der er forbundet med brugen af platformen.



DEN KORTE VERSION:

Kig på Kahoot.com og tjek, om den er dataetisk. Diskutér to og to, hvad man skal kigge efter, hvad der er godt og skidt.

DEN LANGE VERSION (som vi laver hvis der er tid - ellers får de den med hjem)

1. Første indtryk:

Åbn Kahoot på <https://kahoot.com/> og dan dig et første overblik over artefaktet. Hvad er Kahoot, og hvem henvender platformen sig til?

2. Kig nu nærmere på de beskrevne vilkår og betingelser:

Nederst på forsiden findes links til brugervilkår m.m. Undersøg disse.
Start med: <https://kahoot.com/terms-and-conditions/>

Overordnet læsning:

- Hvilken overordnet oplevelse har du af teksten?
- Er der afsnit, som gør dig tryk ved brugen af Kahoot?
- Er der afsnit, som vækker bekymring i forhold til brugen af Kahoot?
- Er der afsnit, som du ikke forstår betydningen af?
- Hvor har virksomheden hovedsæde?

3. Kritisk læsning:

Se på nedenstående deltekst og overvej, hvorfor den er problematisk?

“Although Kahoot! will endeavor to provide the Kahoot! Service in the best possible way without interruptions, you understand and agree that the Kahoot! Service is provided “as is” and “as available”, without any express or implied warranty, condition or assurance of any kind. This means that we do not represent or warrant to you that:

1. the use of the Kahoot! Service and the Resources will meet your needs or requirements.
2. the use of the Kahoot! Service and the Resources will be uninterrupted, timely, secure or free from errors.
3. the information obtained by using the Kahoot! Service and the Resources will be accurate or reliable, or
4. any defects in the operation or functionality of Kahoot! Service or any Resources we provide will be repaired or corrected.”

Er der andre steder i den fulde tekst, som bør fremhæves som problematiske, enten pga. indhold eller layoutmæssige aspekter?

4. Særlige nedslag:

- Kig særligt på sektion 7 vedr. Third Party Applications. Hvad betyder dette? Kan du finde information nogle steder om, hvilke tredjeparts applikationer og brugervilkår, der er tale om?
- Kig særligt på sektion 8. Hvilke implikationer har denne sektion for brugeren? Mener du, at vilkårene er rimelige?
- Kig særligt på sektion 14. Er vilkårene rimelige? Hvilke muligheder har man som bruger, hvis man er utilfreds? Er Kahoot fritaget for alt ansvar?

5. Supplerende undersøgelse:

Åbn nu privatlivspolitikken: <https://kahoot.com/privacy-policy/>

- Hvilke data indsamler Kahoot egentlig og hvorfor?
- Hvordan indsamler Kahoot data?
- Hvordan beskytter Kahoot brugernes data?
- Hvor opbevares data? (hvis de ikke skriver noget om det, kan man altid undersøge det her: <https://webbkoll.dataskydd.net/en/results?url=http%3A%2F%2Fkahoot.com>)
- Er der rimelige begrænsninger i Kahoots dataindsamling?
- Hvordan bruger Kahoot 3. part cookies - altså de cookies, som deler data med alle mulige andre? Hvis de ikke skriver noget om det i deres privacy policy, kan du altid tjekke det her: <https://webbkoll.dataskydd.net/en/results?url=http%3A%2F%2Fkahoot.com>)
- Hvilke muligheder har brugerne for selv at skjule eller slette data?

6. Samlet vurdering:

Overvej nu ud fra ovenstående undersøgelser, om du har tillid til Kahoot, og om du vil lade eleverne lave deres egne brugerkonti.

*Svar 1: lærere, elever, virksomheder, private
Gratis version + betalingsversion
Formidling, underholdning, læring*

*Svar 2: meget lang tekst, virker grundig pga. tillidsvækkende overskrifter. Brug af versaler flere steder signalerer advarsler. Korrekt engelsk. Samtidig svær at overskue pga. længden + der henvises til andre dokumenter undervejs og uspecificerede tredjeparter.
Hovedsædet er Norge <https://craft.co/kahoot/locations>) - bedre end hvis USA eller Kina pga. god europæisk*

datalovgivning.

Svar 3:

Det er et problem, at punktopstilling signalerer, at det er dette, man får, men i sætning lige før står, at Kahoot **ikke** gør dette. Det er misvisende.

Ligeså er afsnit med versaler problematisk, da man automatisk tror, dette så er det vigtigste, selvom det ikke nødvendigvis hænger sådan sammen.

Sætninger, såsom "We reserve the right to change or withdraw features, specifications, services and content of a Service Plan at any time, without notice to you" er ligeledes problematiske, fordi de ikke påtager sig at give brugeren besked om væsentlige ændringer.

Generelt handler en del af teksten om ansvarsfritagelse fra Kahoot's side + begrænsninger af brugerens rettigheder.

Svar 4: Man kan ikke gennemskue, hvilke tredjeparter der er tale om, og dermed heller ikke deres brugervilkår + afsnit længere nede om tredjeparts rettigheder handler om Apple - det er altså ikke den samme tredjepart, som dette afsnit refererer til.

Alle intellektuelle rettigheder overdrages til Kahoot - måske okay pga. dele- og remix-funktionen, men alligevel interessant, at man ikke kan få registreret sin bruger som ophavsmand til indhold.

Som udgangspunkt er brugerens eneste mulighed at slette app og tredjepartsprogrammer - dette synes mangelfuldt. "YOU HEREBY AGREE THAT, TO THE EXTENT PERMITTED BY APPLICABLE LAW, YOUR SOLE AND EXCLUSIVE REMEDY FOR ANY PROBLEMS OR DISSATISFACTION WITH THE KAHOOT! SERVICE IS TO UNINSTALL ANY KAHOOT! SOFTWARE AND TO STOP USING THE KAHOOT! SERVICE". Dette gælder også ved eksempelvis tab af data eller anden utilsigtet fejl på platform. Til sidst står dog, at Kahoot ikke er begrænset eller fritaget i forhold til gældende lov, fx i forbindelse med svindel og grov uagtsomhed, så måske er vilkårene rimelige nok?

Svar 5. Alle svar findes i det linkede dokument. Der indgår forskellige elementer, som Pernille, har været igennem forinden, fx forretningsmodel, aggregering, cookies, relation til GDPR osv., så deltagerne burde kunne gennemskue dokumentet med brug af disse begreber. Helt overordnet kan dog siges at:

Hvilke data?:

- 1) For accountholders:
 - a) Name
 - b) Email address (required)
 - c) Date of birth (required for students and social users)
 - d) Company or organization (of work-related users)
 - e) Financial information (required when signing up for Kahoot Plus "the Paid Subscriptions")
 - f) School or university (of students and teachers)
 - g) Biographical information (for teachers who elect to provide it)
 - h) Chosen username and password for Kahoot account (required)
 - i) Profile picture
 - j) Your interests (such as arts, biology, chemistry, history, music, law etc.)
 - k) Your teaching level, if you are a teacher (such as kindergarten, grade level, higher education, etc.)
- 2) Særlige regler for børneprofiler (under 13 USA) under 16 uden for USA)
- 3) Ingen data for spillere

Hvordan indsamles data?

- platform
- offline, fx kontakt til kundeservice
- Third party, fx google, microsoft og lign.

Derudover indsamler Kahoot "Other Information" is any information that does not reveal your specific identity or does not directly relate to an individual, such as:

Browser and device information

App usage data

Information collected through cookies, pixel tags and other technologies

Demographic information and other information provided by you

Aggregated information”

Kahoot fralægger sig ansvar for dataindsamling hos tredjeparter.

Hvorfor indsamles data?:

- funktionalitet
- marketing
- analyse med henblik på forretningsmodeller og personaliserede services
- for at brugeren kan deltage i konkurrencer m.m.
- anonymisering og aggregering af data
- til forretningsformål, fx udvikling af nye services, sikkerhedsforanstaltninger, osv.

Hvordan beskyttes data?

Ikke særlig fyldestgørende beskrevet. Der står blot:

“We seek to use reasonable organizational, technical and administrative measures to protect Personal Information within our organization. Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of your account has been compromised), please immediately notify us in accordance with the “Contacting Us” section below.”

Hvordan opbevares data?

“Your Personal Information may be stored and processed in any country where we have facilities or in which we engage service providers, and by using the Services you understand that your information will be transferred to countries outside of your country of residence, which may have data protection rules that are different from those of your country.”

Hvis data fra EU-borgere opbevares i andre lande uden for EU, garanterer Kahoot, at de opfylder EU-regler alligevel.

Begrænsninger i Kahoots dataindsamling?

Som udgangspunkt synes Kahoots dataindsamling at være i orden i forhold til deres beskrevne brug af denne. (forretningsmodeller, registrering af brugere, osv.). Derudover beder de om, at man ikke deler personfølsomme oplysninger om fx religion, sundhed, m.m. gennem deres platform.

Hvilke muligheder har brugerne for selv at skjule eller slette data?

Dette kan ske gennem henvendelse til Kahoot og lyder, som om brugeren har fine muligheder for at skjule sine data. Dog kan noget være delt (remixed) af andre og dermed ikke muligt at fjerne i den remixede version.

Svar 6: *Generelt kan man være nogenlunde tryk ved at bruge en tjeneste, der har hovedsæde i Norge, da Norge efterlever GDPR bedre end fx Danmark, og de har et skrappt og vakst datatilsyn. Hvis man søger på det, har der heller ikke været sager mellem Kahoot og det norske datatilsyn eller Forbrukerrådet, der er kendt for at teste tjenester og dukker mv målrettet børn.*

Nu er Kahoot stor i USA, hvorfor det er en god ide at søge på, om der har været sager, og der har CommonSense Media, der tester edu-tech, anbefalet: Use with Caution: <https://privacy.commonssense.org/evaluation/kahoot>

Desuden er der stor brug af tredjepart cookies på Kahoot hvilket betyder, at de deler data med tredjeparter, og de også bruger det til marketing, som de skriver i deres privacy policy. Og de indsamler og bruger og deler altså mange data.

Jeg ville som lærer under alle omstændigheder sikre mig, at eleverne begrænser den persondata, de giver væk ved brugen af Kahoot, og hvis der er tale om følsomme data ved quizzes af mere følsom karakter, ville jeg sikre mig, at data bliver slettet helt bagefter. Eftersom Kahoot er norsk, ville man kunne kræve det ifølge GDPR.