Rådet for Digital Sikkerhed

15. april 2024

Chromebooksagen kalder på et stærkere fokus på dataetikken

Åbent brev til justitsministeren, erhvervsministeren og digitaliseringsministeren

På vegne af bestyrelsen for Rådet for Digital Sikkerhed
Af Henning Mortensen, formand

Resumé

Rådet for Digital Sikkerhed har noteret sig Chromebook-afgørelsen. Rådet finder, at der er behov for en politisk debat om, hvornår der kan videregives oplysninger til leverandøren. Rådet finder desuden, at afgørelsen er et wake-up-call for, at dataansvarlige skal være opmærksom på, hvilke oplysninger, der videregives, på hvilket retligt grundlag og til hvilke formål. Selv om det fra forskellige side er udlagt sådan, ser Rådet ikke afgørelsen som en afvisning af alle videregivelser til formål fastsat af leverandøren. Det er Rådets opfattelse, at problemstillingen kan og bør løses uden, at folkeskoleloven eller anden national lovgivning ændres. Hvis lovgivning skal ændres, skal det være på europæisk plan og med respekt for Chartret. Det er ikke tiden at udvande borgernes fundamentale databeskyttelsesrettigheder og risikere tilliden til digitaliseringen. Til gengæld er der behov for at lave grundige juridiske og risikoafdækkende vurderinger af de teknologier der anvendes, således at der gennem krav til designet og styrkelse af konkurrencen, kan ske en solid understøttelse af databeskyttelsen i det danske samfund.

I januar 2024 kom Datatilsynet med sin længe ventede afgørelse i forhold til anvendelse af Google Workspace for Education i folkeskolen. Den siger kort fortalt, at videregivelse af skoleelevernes persondata til Google er inden for rammen af de regler, der gælder for persondatabeskyttelse, hvis det vel at mærke sker for, at Google kan levere tjenesten, forbedre sikkerheden og garantere pålideligheden. Den dataindsamling, der finder sted, sker med hjemmel i såvel GDPR-reglerne som folkeskolelovens formålsbestemmelser. Det er derimod ikke i orden, at Google anvender de indsamlede data til såkaldt afledte formål, fx den generelle forbedring af Google's styresystem og Google browseren.

Datatilsynets afgørelse er kort sagt et 'wake-up-call' i forhold til digitale produkters afledte strøm af persondata, der for brugeren hverken opdages eller giver mening i forhold til brugen af produktet – og hvor brugeren ikke har en chance for at bevare kontrollen over datastrømmens videre anvendelse til forskellige formål. Rådet for Digital Sikkerhed er enig med KL m.fl. i, at der er behov for en politiske drøftelse af, hvilke data teknologileverandørerne kan benytte til at udvikle deres tjenester.

Skillelinjen i de aftaler, der er indgået mellem kommunerne og Google, mellem relevant dataoverførsel og overførsel af data til formål, som er uvedkommende for Folkeskoleloven og den løbende opdatering af Google Workspace for Education

som læringsmiddel, er simpelthen for uklar. Datatilsynets konklusion lander således på en samlet vurdering af, at overførslerne ikke har den fornødne hjemmel, og lægger i denne forbindelse *"… særligt vægt på, at disse afledte formål (med dataoverførslerne, red.) ikke kun dækker udviklingen af de konkrete undervisnings- og læringsmidler, som kommunerne aftager, men også den generelle udvikling af Googles produkter, f.eks. Chrome OS og Chrome-browseren."*[1]

Efter Rådets vurdering har det afgørende betydning, at navnlig offentlige virksomheder ikke opererer i grumset farvand, når de anvender digitale tjenester med indsamling af persondata – i farvand, hvor der ikke er sat tydelige grænser for dataenes anvendelse, som bør være tæt tilknyttet til eller afledt af den pågældende forvaltningsaktivitet.

Alternativet – det vil sige uklare eller vide rammer – rummer en betydelig risiko for misbrug og brud på de dataetiske præmisser, der er lagt til grund for persondataretten.

Uhensigtsmæssig videregivelse til producenter

Det er således langt fra første gang, der har været nyheder om produkter, der sender oplysninger tilbage til producenten – med eller uden brugernes viden. Et klassisk eksempel er fitness trackeren Strava, som sender oplysninger tilbage til producenten, hvilket kan have den utilsigtede bivirkning, at hvis brugerne er soldater, er hemmelige militære baser blevet afsløret via heat maps[2]. Børns legetøj i flere forskellige modeller kan sende oplysninger tilbage til producenten om børnenes interaktion med legetøjet i form af samtaler. Legetøjsproducenterne har samtidig ikke været kendt for at være de bedste til at beskytte de data, de opsamler, og der er flere eksempler på at producenterne har lækket oplysninger om deres brugere[3].

Mange af de apps, vi har installeret på vores smartphones, sender data hjem til producenten. Formålene kan være mange – f.eks. forbedring af produktet men også mere alternative formål, som f.eks. videregivelse af oplysningerne til tredjemand med henblik på reklamer. Det har vi f.eks. set i tilfældet med dating appen for LGBT+, Grindr, som har delt oplysninger om GPS-lokation, IP-adresse, reklameID, alder og køn – og fået en bøde på 65 mio. NKR for det[4]. Vi har også set det med forskellige menstruationsapps, der deler data med Facebook[5]. Generelt set er det sådan, at

[1] https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/jan/datatilsynet-giver-paabud-i-chromebook-sag.
[2] https://thehackernews.com/2018/01/strava-heatmap-location-tracking.html.
[3] https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/ og https://www.vice.com/en/article/yp3z5v/one-of-the-largest-hacks-yet-exposes-data-on-hundreds-of-thousands-of-kids.
[4] https://www.datatilsynet.no/en/news/aktuelle-nyheter-2023/record-fine-grindr-confirmed/.
[5] https://www.computerworld.dk/art/248855/menstruations-apps-deler-dybt-fortrolige-data-om-brugernes-sexliv-med-facebook.

Vester Farimagsgade 37B, 1.th., 1606 København V
Telefon: +45 24 90 25 22 mail: info@digitalsikkerhed.dk web: www.digitalsikkerhed.dk

mange af de produkter, vi omgiver os med, lytter til os og bringer vores stemme tilbage til producenten[6].

Databrokers

Mange af de data, som opsamles, videregives til databrokers. Herfra kan de købes i såkaldt anonymiseret form. Det er imidlertid sjældent, at data er rigtig anonymiseret, bl.a. fordi der er lokationsoplysninger tilknyttet. Med jævne mellemrum får pressen øje på problemstillingen og køber data fra databrokerne, som f.eks. da et norsk medie for 35.000 NKR købte oplysninger om 140.000 norske mobiltelefoner og på den baggrund kortlagde militærpersoners færden[7]. Faktisk er det sådan, at disse såkaldt anonyme data med mellemrum også købes af efterretningstjenester, for at de tilsyneladende kan komme udenom begrænsende national lovgivning[8].

Kompensation til leverandøren

Det har således stået på i lang tid fra mange forskellige leverandører, at brugerne giver leverandørerne både penge som betaling og personoplysninger. Der er meget høj grad af uigennemsigtighed på området, og det er derfor meget uklart, hvilken datastrøm der foregår, og om der sker en unødig ophobning af personoplysninger hos leverandørerne. Hvor mange havde troet, at deres fitnessapp kan udgøre en potentiel sikkerhedstrussel, eller at legetøjsproducenterne nærmest har tovejs-livetransmission til børneværelset? At samtaler i nærheden af mobiltelefoner måske bliver transskriberet og at metadata om folkeskoleelevers adfærd blev brugt til at forbedre Googles browser?

Ovenstående eksempler viser, at det i en lang række tilfælde ikke indlysende er i brugernes interesser, at der sendes data tilbage til producenten. Det er derfor, at brugerne er beskyttet af de persondataretlige regler, og det er derfor Datatilsynet har sat foden ned. Det er også derfor, det er nødvendigt med en nuanceret drøftelse af, hvornår det kan være relevant, at brugerne deler deres data.

Åben op for debat i stedet for at lukke

Tilbage til Chromebook-sagen. Rådet finder i lighed med Datatilsynet, at det ikke er en kommunal opgave at understøtte Googles og andre techaktørers forretningsudvikling med elevernes data. Rådet er således forundret over KL, der til Ingeniøren udtaler: *"Vi skal have nogle hjemler anno 2024. For ellers bliver konsekvensen, at mange af de her større globale systemer, bliver svære at bruge i Danmark"* (Ingeniøren 23.2.24). KL fortsætter i Computerworld: *"… at optimere brugeroplevelsen… kræver, at man kan overvåge brugernes adfærd inde i*

[6] https://edition.cnn.com/2017/01/12/tech/voice-technology-internet-of-things-privacy/index.html.
[7] https://www.nrk.no/norge/xl/avslort-av-mobilen-1.14911685.
[8] https://www.version2.dk/artikel/dokument-secret-service-har-koebt-lokationsdata-hentet-fra-almindelige-apps.

systemerne… det er jo også noget, vi som brugere langt hen ad vejen gerne vil have, fordi vi gerne vil have gode systemer" (Computerworld 29.2.24)[9].

Med sådanne udtalelser synes KL ikke at åbne meget op for debatten om, hvordan og hvornår vi skal dele data – men i stedet bare åbne op for at dele data med leverandørerne og springe debatten over.

Løsninger

Rådet finder, at det i en lang række sammenhænge kan være yderst nyttigt for brugerne (og for teknologi- og produktudviklingen), at der deles data med leverandøren. Rådet finder også, at det i en række tilfælde er og bør være lovligt. Til gengæld finder Rådet, at der ikke skal udstedes en blanco-check til, at leverandørerne kan indhente brugernes personhenførbare oplysninger. Centralt i den konkrete sag har det jo været, at der er tale om behandlinger af børns oplysninger, og at der er en betydelig asymmetri mellem børn, som er tvunget til at anvendes udstyret, på den ene side, og kommunen som offentlig myndighed på den anden side. Generelt er det vigtigt, at den lovgivning som kommer fra EU i disse år i form af bl.a. GDPR, AI-act, Produktansvarslovgivningen, Digital Services Act mv. implementeres så harmoniseret som muligt og ikke undermineres gennem nationale regler eller forplumres i sektorlovgivning, som fx folkeskoleloven.

Når man politisk og som led i den efterlyste debat skal vurdere, om det er relevant, at der videregives oplysninger til leverandøren, bør man lægge vægt på navnlig følgende forhold:

- Dataetiske og juridiske aspekter
- Tekniske løsninger
- Konkurrenceforholdene på markedet for digitale løsninger
- Muligheder og barrierer for ændret lovgivning

Dataetiske og juridiske aspekter

Videregivelsen skal være nødvendig og proportional, rimelig, lovlig, oplyst/gennemsigtig og til brug for præcise og afgrænsede formål. Så nej man kan ikke opsamle oplysninger fra elevers digitale undervisning til generelt at forbedre en browser og et styresystem, men man kan godt gøre det mhp. at forbedre et undervisningsprodukt eller skabe god sikkerhed.

[9] https://www.computerworld.dk/art/286381/kl-efter-chromebook-sag-vi-har-brug-for-at-kunne-overvaage-brugernes-adfaerd-der-er-brug-for-en-lovaendring.

Tilsvarende vil man formodentlig også i en lang række tilfælde kunne videregive brugerdata fra medico-teknisk udstyr eller fra maskiner, hvor safety er et formål, der skal opfyldes. Rådet er af den opfattelse, at Chromebook-afgørelsen og det tilknyttede svar fsva. Microsoft Office 365[10], ikke skal ses som en generel nedlukning af videregivelse af oplysninger til leverandøren, men opfordring til at se på lovligheden af videregivelsen. Tværtimod er Rådet af den opfattelse, at der kan findes gode eksempler på danske løsninger, hvor der har været fokus på designet, og hvor der sker en videregivelse som er lovlig, bl.a. også med det formål at justeret funktionalitet til en konkret bruger.

Når man vurderer de dataetiske og juridiske forhold, skal der også lægges vægt på, hvilken målgruppe der behandles oplysninger om. Er der tale om børn eller andre, som i ringe grad kan forsvare deres rettigheder. Dette forhold spiller en særlig rolle i den konkrete sag. Der skal også lægges vægt på graden af oplysningers følsomhed. Dette forhold spiller næppe en rolle i den konkrete sag.

Man skal også lægge vægt på, hvem der behandler oplysningerne. Når offentlige myndigheder behandler oplysninger om borgerne, skal de opfylde det dobbelte legalitetsprincip, hvilket betyder, at de kun må gøre det. som eksplicit er tilladt i lovgivningen. Private virksomheder kan derimod nøjes med det almindelige legalitetsprincip, hvorefter de ikke må gøre noget, der strider mod loven. Det vil formodentlig give private videre rammer til at behandle personoplysninger (med hjemmel i interesseafvejning).

Endelig kan det også være relevant at vurdere, om man kan opfylde sit formål og efterleve nogle af de databeskyttelsesprincipper, som er nævnt ovenfor ved at designe sit produkt, så videregivelsen er så lidt indgribende overfor brugerne som muligt[11]. Databeskyttelse gennem design og default har et kæmpemæssigt potentiale til at sikre compliance med de persondataretlige regler samtidig med at man fået understøttet den teknologiske udvikling maksimalt.

Tekniske løsninger

I den konkrete sag ville det være naturligt at kigge på anonymisering af brugeres identiteter, deres IP-adresser og deres øvrige personoplysninger m.v., således at man med tekniske løsninger helt kan komme uden om de persondataretlige regler. Rådet har i forbindelse med udfordringerne med Schrems II og tredjelandsoverførsler skrevet om brugen af kryptering med europæiske krypteringsnøgler. Rådet har også af flere omgange skrevet vedledninger med anbefalinger om pseudonymisering og anonymisering[12].

[10] https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/feb/chromebook-sagens-relevans-for-andre-organisationer-og-cloudservices
[11] https://www.digitalsikkerhed.dk/wp-content/uploads/2020/12/RfDS-vejledning-om-DPbD.pdf.
[12] https://www.digitalsikkerhed.dk/wp-content/uploads/2021/02/Vejledning-om-visse-privatlivsfremmende-teknologier-1.pdf.

Hvis man anonymiserer eller pseudonymiserer identiteter (hvor førstnævnte er en stærkere sikring mod, at data kan henføres til de registrerede brugere), vil man kunne løse rigtig mange databeskyttelsesmæssige og sikkerhedsmæssige udfordringer i det danske samfund. Rådet beklager, at der ikke ses mere ind i sådanne løsninger og skal påpege, at Chromebooksagen kunne være en god anledning hertil.

Konkurrenceforhold

Som praksis har været før Datatilsynets afgørelse, har danske elevers personoplysninger bidraget til udviklingen af platforme, teknologier og undervisningsplatform for et amerikansk tech-selskab. Som Datatilsynet også peger på i afgørelsen, er det er bemærkelsesværdigt, at ved at give elevernes data til brug for videreudvikling af Googles produkter bidrager kommunerne til, at styrke selskabets markedsposition. Det bliver hermed sværere for danske eller europæiske serviceudbydere at komme ind på markedet for undervisning; så selvom det ikke er hensigten. Dette endog på trods af at danske leverandører påstår at kunne bidrage til løsning af Chromebook-problemstillingen[13].

Ændring af lovgivning

Ændring af lovgivning, som Datatilsynet angiver som en mulighed, og som KL m.fl. ønsker, er en mulighed. For det første skal man dog ændre ganske meget speciallovgivning for at komme rundt om alle de tilfælde, som det kan være relevant at adressere. For det andet er det – uanset Datatilsynets angivelse af muligheden – Rådets opfattelse, at tilpasning af national lovgivning giver betydelig compliance-risiko i forhold til Charterets garantier. Hvis man skal kigge på ændring af lovgivning, bør dette derfor ske på europæisk plan.

Konklusion

Her på tærsklen til næste digitaliseringsbølge med kunstig intelligens som drivkraft, er det helt afgørende, at persondatabeskyttelsen har allerhøjeste prioritet. På samme måde som Google Workspace for Education har medvirket til at udvikle og styrke undervisningen, vil anvendelsen af kunstig intelligens inden for forvaltning og forretningsudvikling give samfundet helt nye muligheder.

Danmark har imidlertid været for ensidig i vores fokus på digitaliseringens gevinster, og har haft for lidt fokus på, at vores digitale adfærd afkodes og persondata ophobes af leverandørernes til formål, vi ret beset ikke har købt ind på. IDA udtrykker det således*: "Sagen illustrerer jo tydeligt konsekvenserne af den ukritiske fascination af smarte it-løsninger, som desværre har præget den offentlige sektor i alt for mange år"[14] og fortsætter: "Det er en vigtig sag, fordi den udstiller vores afhængighed af*

[13] https://www.computerworld.dk/art/286263/danmarks-stoerste-open-source-leverandoer-vi-kan-komme-chromebook-sagen-til-livs-for-kun-fem-millioner-kroner
[14] https://ida.dk/om-ida/nyt-fra-ida/chromebook-sag-udstiller-danske-tech-afhaengighed

Vester Farimagsgade 37B, 1.th., 1606 København V
Telefon: +45 24 90 25 22 mail: info@digitalsikkerhed.dk web: www.digitalsikkerhed.dk

nogle ganske få store virksomheder… vores børn… betaler prisen, hvis vi ikke hele tiden tænker privacy med fra begyndelsen".

Rådet kan tilføje, at Danmark er blevet nummer 2 i digitalisering i verden, men vi er kun nummer 32 i sikkerhed – fordi vi ikke har den fornødne fokus på privacy and security by design.

Rådet skal derfor anbefale, at man fra politisk side ikke udvander den lovgivning, som grundlæggende skal beskytte borgerne og sikre, at vi alle kan være trygge ved digitaliseringen. Løsningen er at pålægge de dataansvarlige 1) at lave en grundig analyse af de dataetiske og juridiske forhold og 2) at lave risikovurderinger og konsekvensanalyser og efterfølgende vælge sikkerhedsforanstaltninger by design som reducerer den identificerede risiko. Hvis lovgivningen skal ændres, bør det være på europæisk plan og med respekt for Det europæiske Charter.

Danmark har gennem mange år vist nye veje til, hvordan digitaliseringen kan anvendes til sund forretningsudvikling og udvikling af den offentlige service. Det skal vi fortsætte med. Med et stærkere fokus på såvel dataetikken som sikringen mod unødig og ugennemsigtig ophobning af persondata har vi enestående muligheder for at skubbe til udviklingen med mennesket, ansvarlig innovation og det fælles bedste som afsæt.