

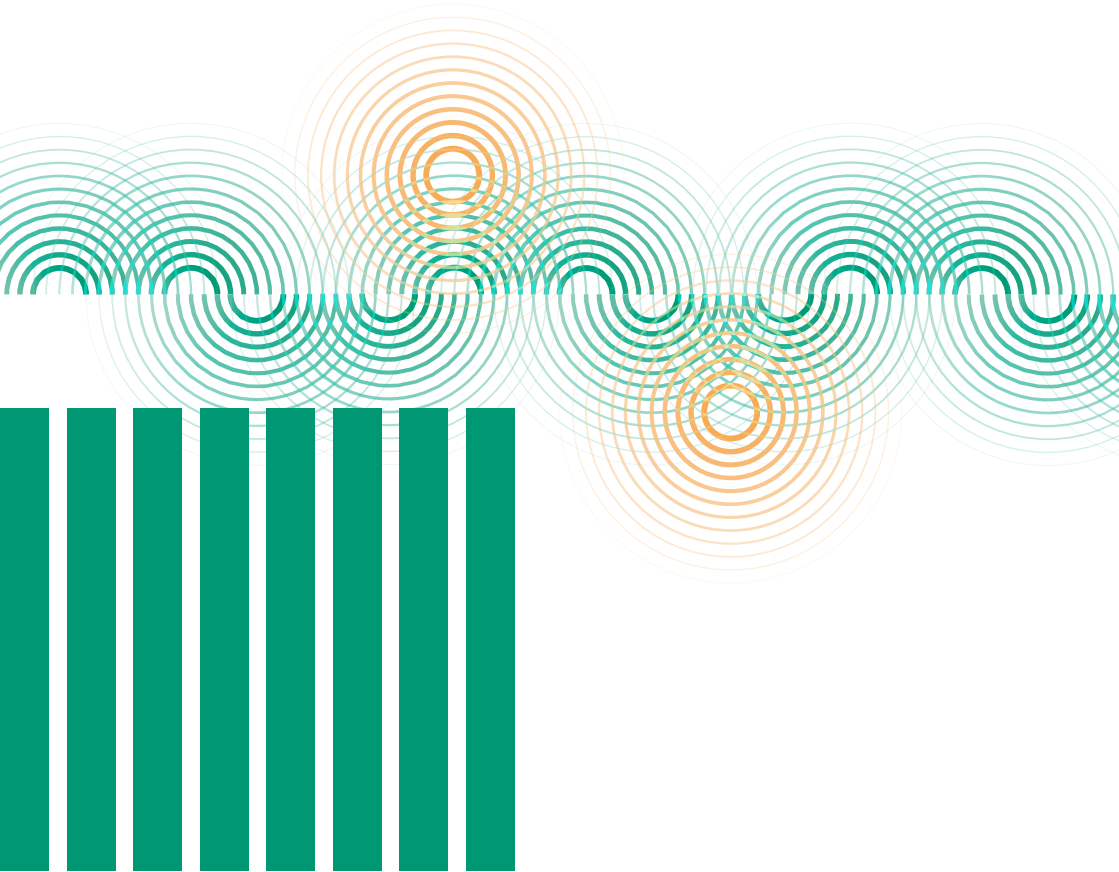
TECH-GIGANTERNES ROLLE SOM DIGITAL INFRASTRUKTUR

Delafrapportering 3 fra regeringens ekspertgruppe om tech-giganter



Regeringens ekspertgruppe

TECH-GIGANTER



TECH-GIGANTERNES ROLLE SOM DIGITAL INFRASTRUKTUR

November 2024

Digitaliseringsministeriet
Stormgade 2-6,
1470 København

+45 72 28 24 00
digmin@digmin.dk

ISBN 97887-85325-03-7 (digital)
ISBN 97887-85325-02-0 (trykt)

Publikationen kan hentes på:
www.digmin.dk

Design og layout: Erhvervsministeriets kommunikationsenhed og BGRAPHIC

- 4 **FORORD**
- 6 **SAMMENFATNING**
- 12 **EKSPERTGRUPPENS SYV PRINCIPPER**
- 14 **PRINCIP 1**
**DER SKAL VÆRE OVERBLIK OVER TECH-GIGANTERNES
INDFLYDELSE PÅ DEN DIGITALE INFRASTRUKTUR**
- 16 **PRINCIP 2**
**DATA SKAL GØRES TILGÆNGELIGE PÅ MÅDER, DER KAN
GAVNE OG STYRKE INDIVIDET OG FREMTIDENS SAMFUND**
- 19 **PRINCIP 3**
**ALTERNATIVER TIL TECH-GIGANTERNES TJENESTER SKAL
KUNNE OPSTÅ OG VOKSE SIG STORE**
- 22 **PRINCIP 4**
**INGEN SKAL VÆRE TVUNGET TIL AT BRUGE TECH-GIGANT-
ERNES TJENESTER FOR AT FÅ INFORMATION OG DELTAGE I
SOCIALE, KULTURELLE OG DEMOKRATISKE FÆLLESSKABER**
- 24 **PRINCIP 5**
**DEN OFFENTLIGE SEKTOR SKAL IKKE VÆRE AFHÆNGIG AF
TECH-GIGANTERNES TJENESTER**
- 26 **PRINCIP 6**
**DANSKE UDDANNELSESINSTITUTIONER SKAL VÆRE FRI
FRA KOMMERCIELLE TECH-GIGANTER**
- 28 **PRINCIP 7**
**TECH-GIGANTERNES PLATFORME SKAL VÆRE TRYKKE
STEDER AT HANDLE**
- 33 **EKSPERTGRUPPENS SAMMENSÆTNING**
- 34 **EKSPERTGRUPPENS KOMMISSORIUM**
- 36 **KILDELISTE**

FORORD

AF FORMAND FOR EKSPERTGRUPPEN,
PROFESSOR MIKKEL FLYVERBOM



Danmark har en veludbygget og velfungerende infrastruktur – ofte baseret på et samarbejde mellem den offentlige og private sektor – der har skabt fundamentet for både vækst, velfærd og sikkerhed. Infrastrukturen omfatter blandt andet fysiske anlæg og systemer, der skaber stabil adgang til transport, kommunikation og offentlige tjenester, som borgere, virksomheder og institutioner har brug for. Traditionelt har infrastruktur handlet om adgang til f.eks. vand, elektricitet, veje, sundhedsvæsen og uddannelsesinstitutioner. Men i vores tid er vi i stigende grad også afhængige af velfungerende digitale systemer.

Modsat andre former for infrastruktur lever dele af den digitale infrastruktur ikke op til gængse principper om demokratisk kontrol og samarbejde mellem private og offentlige aktører. Når vi i denne rapport taler om det digitale område som infrastruktur, er det for at tydeliggøre, at en stor del af vores kommunikation, arbejdsliv, fritidsliv, skoleliv, offentlige institutioner og andre vigtige samfundsfunktioner er koblet op på tech-giganters platforme, sociale medier, apps, cloudløsninger og andre digitale løsninger. I et gennemdigitaliseret land som Danmark gør den afhængighed os sårbare, særligt når også andre former for forsyning og koordination i stigende grad bliver hængt op på den digitale infrastruktur. Det ser vi for eksempel, når it-nedbrud hos tech-giganter sætter flytrafik og hospitals-systemer ud af funktion, og når andre former for forsyning bliver påvirket af cyberangreb.

Vi er gået fra en situation, hvor det gav mening at tale om det digitale område som et separat cyberspace, til en situation, hvor det digitale har fået tildelt en rolle som samfundets ryggrad. Og når det digitale får denne centrale rolle, er det vigtigt, at det understøtter og bidrager til det demokratiske retssamfund, vi gerne vil bevare og opbygge.

En voksende udfordring er, at dele af den digitale infrastruktur er udviklet, ejet og kontrolleret af tech-giganter, som primært har fokus på teknologiske landvindinger, hurtigt udrulning og kommercielle gevinster og ikke nødvendigvis prioriterer ansvarlighed, beskyttelse af børn og andre borgere og demokratiske værdier. Selv om EU-lovgivning på det digitale område definerer en række spilleregler for store tech-virksomheder, står vi lige nu i en situation, hvor vores samfund i stigende grad er blevet afhængigt af digitale infrastrukturer, som vi har meget lidt kontrol med. Det gør os sårbare på vitale områder som økonomi, demokrati og sikkerhed.

At dele af de digitale infrastrukturer er afkoblet fra demokratisk kontrol, indsigt og almindelige spilleregler er et grundlæggende problem. En sådan afkobling accepterer vi ikke i samme grad, når det gælder anden infrastruktur, som vores samfund er afhængig af for at kunne fungere. Det er svært at forestille sig en situation, hvor al anden infrastruktur fungerer på samme måde som den digitale: At eksempelvis vores vandforsyning eller vejnet var ejet af store globale virksomheder, som egenrådigt lavede spillereglerne, som ikke var



til at komme i kontakt med, og som vægtede profit over hensynet til rettigheder, ansvarlighed, lovlighed, sikkerhed og beskyttelse af borgere. Ligesom andre infrastrukturer er noget, det danske samfund definerer rammerne for, investerer i og koordinerer i samspil med leverandører og andre private aktører, så har vi også brug for digitale infrastrukturer, der matcher vores samfunds behov bedre end de nuværende.

I mange år har der manglet politisk bevågenhed, samfundsmæssig interesse og håndfast regulering på det digitale område. Nu har vi som samfund fået en øget forståelse af de skadelige konsekvenser af tech-giganternes forretningsmodeller og mangel på ansvarlighed og beskyttelse. Men der er brug for mere principielle og grundlæggende indsatser, hvis vi vil undgå at tabe yderligere kontrol til tech-giganterne i en fremtid, hvor digitale systemer væver sig endnu mere sammen med samfundsmæssige og geopolitiske udviklinger.

Mange andre lande, f.eks. Sverige, Tyskland, Frankrig og Holland,¹ bruger i disse år kræfter på at skabe sammenhæng mellem den digitale infrastruktur og det samfund, de ønsker at fremme – netop gennem opbygning af digitale infrastrukturer og øget kontrol på området. Det kræver store investeringer og koordinering mellem leverandører, myndigheder, offentlige institutioner og andre. Til gengæld

er der meget at vinde, også for det danske samfund. Målet med denne rapport er at adressere de strukturelle problemstillinger, som gør det svært for befolkningen at deltage i kulturelle, sociale og demokratiske fællesskaber uden at være afhængig af tech-giganter. Samtidig peger vi på de sårbarheder, som den offentlige sektors afhængighed af tech-giganterne skaber, og på det problematiske ved, at data primært bruges til afgrænsede, kommercielle formål og ikke til at udvikle fremtidens velfærdssamfund. Hvis det skal lykkes at skabe grobund for alternativer til tech-giganter, kræver det, at demokratisk overblik og kontrol med den digitale infrastruktur bliver en politisk prioritet og et konkret langsigtet indsatsområde i både Danmark og EU.

Baseret på sit mandats fokus på de ”strukturelle problemstillinger, hvor tech-giganternes forretningsmodel udfordrer vores samfund, kultur, økonomi, trivsel mv.”, giver ekspertgruppen i denne rapport en række principielle bud på, hvordan Danmark fremadrettet kan mindske sin sårbarhed og aktivt forme den digitale udvikling. Det kræver, at Danmark baner vej for digitale infrastrukturer, der er mere i tråd med demokratiske værdier og mindre styret af tech-giganternes interesser.

SAMMENFATNING

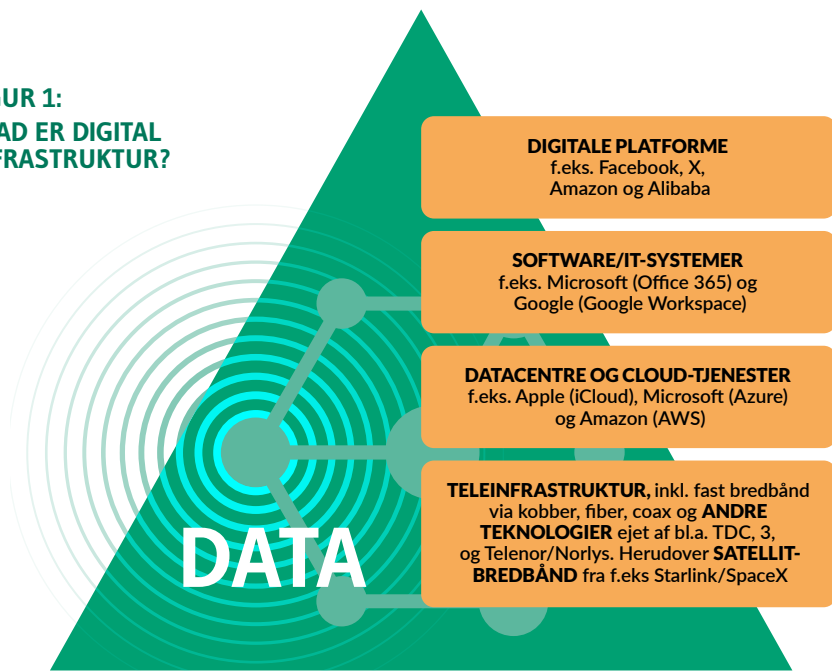
Ekspertgruppen har i de to første rapporter sat fokus på de problemstillinger, der opstår på grund af tech-giganternes forretningsmodeller, kommercielle interesser og udruiningen af kunstig intelligens. Den økonomiske og teknologiske magt, som de foregående rapporter peger på, gør det nødvendigt også at fokusere på den omfattende rolle, tech-giganterne udøver som digital infrastruktur i samfundet. Tech-giganternes indflydelse og samfundsmæssige magt øges nemlig, når deres investeringer i infrastruktur understøtter og forstærker virksomhedernes eksisterende magtpositioner, f.eks. inden for kunstig intelligens.

Danmark er et af de mest digitaliserede lande i verden, og en stadig stigende del af samfundets funktioner og kommunikation foregår digitalt. Det gør vores samfund effektivt, men skaber også en række sårbarheder. Det gælder særligt, hvis der ikke er tilstrækkeligt overblik, kontrol og eftertanke med hensyn til, hvem der får adgang til at eje og drive den digitale infrastruktur i bred forstand.

Ved at se på den digitale infrastruktur i bred forstand er det muligt at tydeliggøre, hvor store dele af det danske samfund tech-giganterne påvirker. Det fokus er vigtigt for at gøre det muligt at løse de strukturelle problemstillinger, som tech-giganterne skaber, og som ekspertgruppen har fået mandat til at arbejde med.

Den digitale infrastruktur udgør fundamentet i gennemdigitaliserede samfund og gør det muligt at udveksle digital information mellem myndigheder, borgere og virksomheder. Den omfatter alt fra grundlæggende fysisk netværksinfrastruktur til de tjenester, vi anvender i det daglige, f.eks. Outlook, MitID, Aula og Digital Post. Den omfatter også de apps, hjemmesider og digitale platforme, som bruges til kommunikation, information, koordinering, køb og salg. Gennem hele den digitale infrastruktur løber de data, der bliver genereret og indsamlet, når vi bruger internettet. Figur 1 giver et overblik over de forskellige typer digital infrastruktur, som denne rapport omhandler.

**FIGUR 1:
HVAD ER DIGITAL
INFRASTRUKTUR?**



Dele af den digitale infrastruktur anses for *kritisk* digital infrastruktur. Den er nødvendig for at opretholde eller genoprette samfundsvigtige funktioner som f.eks. energi, drikkevand, fibernet og mobilnetværk. Den kritiske infrastruktur er ofte underlagt lovgivning, som blandt andet skal sikre tilgængelighed, stabil drift og forsyning. En del kritisk infrastruktur er også underlagt økonomisk regulering for at sikre effektiv drift og rimelige forbrugerpriser. Det gælder f.eks. vandforsyningen. Der kan også være krav om, at den geografiske place-

ring af kritisk infrastruktur skal være i Danmark. Databeskyttelsesloven og retshåndhævelsesloven² indeholder f.eks. et sådant lokationskrav.³ Formålet er, at danske myndigheder har adgang til de pågældende it-systemer og mulighed for inden for lovgivningens rammer bl.a. at modvirke uretmæssig udnyttelse af personoplysninger i systemet. Systemer som MitID, CPR-registret og Digital Post er omfattet af lokationskravet.

➤ REGULERING AF INFRASTRUKTUR OG CYBERSIKKERHED

INVESTERINGSSCREENINGSLOVEN

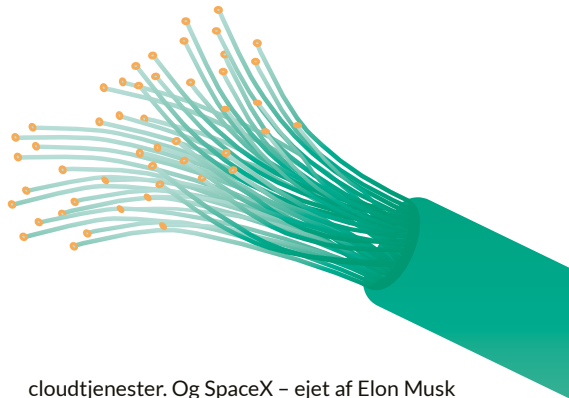
Kritisk infrastruktur er underlagt investeringscreeningsloven, hvilket betyder, at udenlandske investeringer mv. i virksomheder inden for kritisk infrastruktur kræver forhåndstilladelse.⁴ Formålet er at kunne afskære visse virksomheder fra at drive eller udvikle kritisk infrastruktur i Danmark, hvis der er risiko for, at aktiviteten kan udnyttes til f.eks. spionage. Erhvervsstyrelsen har eksempelvis i maj 2023 i henhold til investeringscreeningsloven givet afslag på godkendelse af NKT's frasalgs af et datterselskab.⁵ Loven er fra den 1. juli 2023 blevet udvidet markant. Det skal særligt ses i lyset af de nye geopolitiske forskydninger, den øgede stormagtskonkurrence og Ruslands invasion af Ukraine. Det har skærpet sikkerhedstruslen mod Danmark og dansk kritisk infrastruktur markant i de seneste år.⁶

NIS2 OG CER

Cybersecurity Directive (NIS2) skal sikre, at virksomheder og myndigheder i EU, der er en del af væsentlig eller vigtig infrastruktur, opnår et højt fælles cybersikkerhedsniveau.⁷ Blandt andet gennem skærpede krav til ledelsen, minimumskrav til styring af cybersikkerhedsrisici, krav om underretning af myndigheder om sikkerheds-hændelser inden for nærmere angivne frister samt bøder for overtrædelse. Critical Entities Resilience Directive (CER)⁸ skal styrke kritisk infrastrukturens modstanddygtighed over for fysiske trusler, f.eks. naturkatastrofer, terrorangreb, insidertrusler eller sabotage. Hvis en virksomhed eller organisation er karakteriseret som kritisk infrastruktur, er der f.eks. krav om procedurer for baggrundskontrol af personer, der udfører følsomme opgaver eller har adgang til virksomhedens lokaler, oplysninger eller kontrolsystemer.

CYBER RESILIENCE ACT

Cyber Resilience Act (cybersikkerhedsforordningen) skal sikre et minimumsniveau af cybersikkerhed for digitale produkter i EU, så de har færre sårbarheder, når de sættes på markedet, og løbende modtager softwareopdateringer. Samtidig skal den gøre det lettere for forbrugerne at gennemskue cybersikkerheden i produkterne og anvende dem sikkert. Med forordningen følger fælleseuropæiske cybersikkerhedskrav for alle, der fremstiller, udvikler og importerer produkter med digitale elementer, herunder både software og hardware.⁹



Herudover er det besluttet, at den danske stat i nogle tilfælde skal have ejerskabet over visse selskaber for at imødekomme et behov for kontrol med kritisk infrastruktur.

Der er også infrastruktur, der ikke i dag er defineret som kritisk, og som derfor ikke er reguleret på samme måde. Den spiller dog alligevel en vigtig rolle i vores samfund. Denne rapport fokuserer på tech-giganternes rolle som – og indflydelse på – digital infrastruktur i bred forstand.

Tech-giganterne ejer i dag forskellige dele af den digitale infrastruktur i Danmark og Europa. Tech-giganter som Alphabet og Meta udbyder de mest brugte hjemmesider og apps, indsamler store mængder af brugerdata og investerer i infrastrukturer som f.eks. datacentre.¹⁰ Amazon og Microsoft ejer de største

cloudtjenester. Og SpaceX – ejet af Elon Musk – skal sørge for hurtigt satellitinternet til Molslinjens færger i Danmark.¹¹ Google og Meta er med i et konsortium, der skal bygge et transatlantisk, undersøisk fiberkabel på over 7.000 kilometer mellem Esbjerg og New Jersey i USA.¹²

Tech-giganternes tjenester bliver desuden anvendt i store dele af den offentlige sektor: Chromebooks i folkeskolerne, iPhones og iPads i ministerier og styrelser, og i kommunerne stiger udgifterne til Microsoft for brug af bl.a. deres cloudtjeneste. Ovenpå alt dette er der et lag af søgemaskiner, sociale medier og markedspladser – ejet af tech-giganterne – der fungerer som digital infrastruktur for information, samtaler, køb og salg.



EKSPERTGRUPPENS FORSTÅELSE AF TECH-GIGANTER

Ekspertgruppen har ikke arbejdet ud fra en fasttømret definition af "tech-giganter" – for at undgå at fokusere på navngivne virksomheder. I stedet har ekspertgruppen brugt en løsere definition: Teknologivirksomheder, der gennem udbredelsen af deres platforme og tjenester har opnået en særlig og i nogle tilfælde dominerende status på centrale samfundsområder og derfor indvirker på brugernes grundlæggende rettigheder. Det er virksomheder, som i varierende grad bygger deres forretningsmodel på at indsamle enorme mængder data til anvendelse og videreformidling til bl.a. tredjeparter, der f.eks. anvender oplysningerne til annoncering.

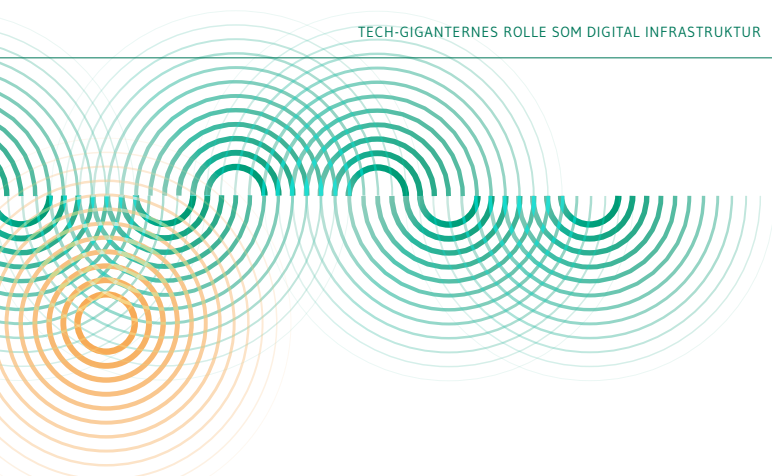
Tech-giganternes ejerskab og indflydelse gør Danmark sårbar. Sårbarheden opstår overordnet på grund af tre typer udfordringer: økonomiske, demokratiske og sikkerhedspolitiske.

De *økonomiske* sårbarheder opstår, når vi bliver afhængige af tech-giganterne, og tech-giganterne opnår en markedsmagt, der sætter den effektive konkurrence ud af spil. Effektiv konkurrence skal sikre lavere priser, højere kvalitet og et bredere udvalg af produkter og tjenester. Afhængighed gør forhandlinger om f.eks. priser vanskeligere og kan medføre, at der betales for meget, eller at der accepteres nogle vilkår, som ellers ikke ville blive accepteret.

De *demokratiske* sårbarheder opstår, når tech-giganterne af kommercielle eller andre årsager udfordrer eller forsøger at omgå de regler og rettigheder, som vores demokratisk valgte politikere har besluttet, og de afgørelser, som myndighederne har truffet. Det er også en demokratisk udfordring, hvis der ikke er transparens om tech-giganternes indflydelse via f.eks. donationer til kommuner, skoler, universiteter og tænketanke.¹³ Endelig udfordres den demokratiske samtale og adgangen til troværdigt indhold, når tech-giganternes algoritmer ud fra kommercielle hensyn bestemmer det indhold, brugerne ser på deres tjenester, og tech-giganterne ikke vil oplyse, hvilke opslag der bliver promoveret eller fjernet, og hvorfor.

De *sikkerhedsmæssige* sårbarheder opstår, når tech-giganterne bliver så magtfulde, at de kan udøve en form for udenrigs- og sikkerhedspolitik og bliver en del af geopolitiske spændinger. Et nyere eksempel er Elon Musk, ejeren af X, der med Starlink-satellitterne har spillet en vigtig rolle i krigen i Ukraine.¹⁴ Eksemplet illustrerer, hvordan en tech-gigant via en enkeltperson fører sin egen udenrigs- og sikkerhedspolitik. Et andet eksempel er TikTok, som indsamler meget store mængder data om sine brugere. De bliver brugt til spionage, afpresning mv.¹⁵ Endelig kan tech-giganterne via deres tjenester påvirke valg, forstærke spændinger og konflikter og så tvivl om fakta bag politiske beslutninger. Der eksisterer også andre sikkerhedsmæssige sårbarheder, når det gælder den kritiske infrastruktur, f.eks. risikoen for hacking, cyberangreb, fysisk sabotage og lignende. Disse cybersikkerhedssårbarheder udgør en del af bagtæppet for denne rapport, men vil ikke blive beskrevet nærmere.

I både Danmark og EU tales der om behovet for at styrke og genvinde den "digitale suverænitet",¹⁶ dvs. mindske politisk, økonomisk og teknologisk afhængighed af bestemte virksomheder og lande, for at reducere vores sårbarhed, beskytte demokratiske værdier og sikkerhedspolitiske interesser og styrke den europæiske konkurrenceevne.^{17 18 19}



EU spiller en helt central rolle i at sikre, at spilleregler bliver fastsat og overholdt. Det er afgørende for denne rolle, at reguleringen implementeres og håndhæves effektivt. Det gælder særligt de nyligt ikrafttrådte EU-forordninger AI Act, Digital Services Act, Digital Markets Act, Data Act og Data Governance Act. Men ekspertgruppen vurderer, at der skal mere til, hvis man vil øge den demokratiske kontrol.

I denne rapport kommer ekspertgruppen med en række bud på, hvordan samfundets digitale infrastruktur kan se ud, hvis man vil øge den demokratiske kontrol, og hvilke pejlemærker vi kan sigte efter for at komme derhen. Det handler i høj grad om, hvad der kan *bygges op* og *bruges som alternativer* til tech-giganternes tjenester, og hvilke spilleregler tech-giganterne skal efterleve. Dette er nødvendigt for at løse de strukturelle problemstillinger, som ekspertgruppen har fået mandat til at arbejde med, og som primært opstår på grund af tech-giganternes forretningsmodeller.

Rapporten præsenterer syv principper, som ekspertgruppen anbefaler bliver brugt, når der fremadrettet bliver truffet beslutninger om tech-giganternes rolle i det danske samfund. Ved at følge principperne vil det blive muligt at håndtere mange af de udfordringer ved tech-giganterne, som regeringen har givet ekspertgruppen mandat til at behandle. Dermed sikres en ansvarlig teknologisk udvikling, der understøtter Danmarks demokrati, velstand og sikkerhed i en globalt forbundet verden.

De første tre principper handler om, hvordan vi overordnet ønsker den digitale infrastruktur indrettet i fremtiden. Der skal være mere kontrol med tech-giganterne, vi skal understøtte alternativer og sikre, at data styrker individet og fremtidens samfund. De sidste fire principper fokuserer på forskellige dele af det danske samfund og beskriver, hvilke principper der bør gælde for tech-giganternes indflydelse.

EKSPERTGRUPPENS SYV PRINCIPPER

1

**DER SKAL VÆRE OVERBLIK OVER TECH-GIGANTERNES
INDFLYDELSE PÅ DEN DIGITALE INFRASTRUKTUR**

2

**DATA SKAL GØRES TILGÆNGELIGE PÅ MÅDER, DER KAN
GAVNE OG STYRKE INDIVIDET OG FREMTIDENS SAMFUND**

3

**ALTERNATIVER TIL TECH-GIGANTERNES TJENESTER
SKAL KUNNE OPSTÅ OG VOKSE SIG STORE**

4

**INGEN SKAL VÆRE TVUNGET TIL AT BRUGE TECH-GIGANTERNES
TJENESTER FOR AT FÅ INFORMATION OG DELTAGE
I SOCIALE, KULTURELLE OG DEMOKRATISKE FÆLLESSKABER**

5

**DEN OFFENTLIGE SEKTOR SKAL IKKE VÆRE
AFHÆNGIG AF TECH-GIGANTERNES TJENESTER**

6

**DANSKE UDDANNELSESINSTITUTIONER SKAL VÆRE FRI FRA
KOMMERCIELLE TECH-GIGANTER**

7

**TECH-GIGANTERNES PLATFORME SKAL VÆRE
TRYGGE STEDER AT HANDLE.**

PRINCIP 1

DER SKAL VÆRE OVERBLIK OVER TECH-GIGANTERNES INDFLYDELSE PÅ DEN DIGITALE INFRASTRUKTUR

PEJLEMÆRKER

- a. Der er et offentligt tilgængeligt overblik over ejerskabsstrukturen i den digitale infrastruktur. Overblikket bliver løbende opdateret, og ejerskabet monitoreret.
- b. Der er dannet alliancer med ligesindede lande om at fremme europæiske investeringer og samarbejde inden for udviklingen af digitale løsninger, der understøtter demokratiske retssamfund.
- c. Der er et bredere udvalg af cloudløsninger og kunstig intelligens-modeller af høj kvalitet til rådighed i Danmark og Europa.



Tech-giganterne spiller flere væsentlige roller i og som digital infrastruktur, også i det danske samfund. Google og Meta udbyder de mest anvendte hjemmesider og apps, indsamler store mængder af brugerdata og investerer i f.eks. datacentre. Microsofts produkter er de mest anvendte til f.eks. tekstbehandling og e-mail på regerings- og myndighedskontorer overalt i verden. Aula hostes af Amazon Web Services (AWS).²⁰ Og regeringer og offentlige myndigheder er i nogle tilfælde afhængige af tech-giganterne, når de udfører centrale nationale sikkerhedsopgaver. Storbritanniens regering indgik f.eks. en aftale med Amazon i 2021 om varetagelse af clouddata fra alle deres efterretningstjenester samt deres forsvarsministerium.²¹

I Danmark er dele af den digitale infrastruktur, der tidligere har været på danske hænder, det ikke længere. Centrale dele af den danske betalingsinfrastruktur ejes fortsat af Nationalbanken, dvs. den danske stat, men eksempelvis Dankortet ejes i dag af virksomheden Nets, som er blevet købt af det italienske Nexi Group. Nets har solgt tjenesten Betalings-service til Mastercard. Ejerforholdene af Nets har ændret sig over tid gennem fusioner og opkøb. Fra at være bankejet under navnet Pengeinstitutternes Betalings Service, er Nets i dag ejet af et italiensk firma, som igen ejes af en række udenlandske kapitalfonde.

De komplekse ejerstrukturer ændrer sig løbende. Det rejser spørgsmålet, om der er tilstrækkeligt overblik over, hvem der ejer og driver den digitale infrastruktur og de digitale

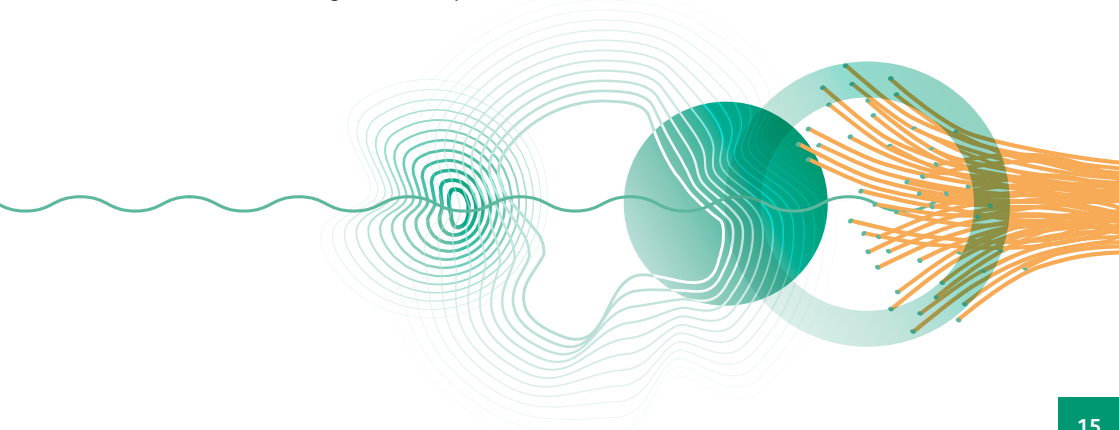
løsninger, som væsentlige dele af samfundet er bygget på og er afhængige af. Ikke bare i tilfælde af forsyningskriser, men også når det gælder den løbende påvirkning af Danmark, som et ejerskab kan anvendes til. Endelig er der risiko for, at ejerskabet vægter kommercielle interesser højere end f.eks. datasikkerhed og driftssikkerhed. F.eks. blev Nets tidligere på året stærkt påvirket af et DDoS-angreb, som er et simpelt og gammeldags hackerangreb.²²

Tech-giganterne er også ved at vinde fodfæste på markedet for betalingsinfrastruktur. Tal fra 2022 viser, at mere end hver femte forbruger benyttede en digital betalingsløsning ved deres seneste betaling i en fysisk forretning. Apple Pay blev anvendt af ca. 10 pct. af forbrugerne ved deres seneste betaling.²³ I dag betaler de fleste kunder med Visa- eller Mastercard-delen af deres kort, når de bruger Apple Pay. De fleste danske banker har nemlig endnu ikke integreret Dankortet i mobilbetalingsløsninger som Apple Pay.²⁴ Samtidig var det indtil for nylig ikke muligt for konkurrenter til Apple at få adgang til den kontaktløse NFC-chip i iPhones. Apple har udtalt til Europa-Kommissionen,²⁵ at de arbejder på at gøre det muligt for f.eks. Vipps Mobilepay og Nets at udvikle konkurrerende betalingsløsninger til Apple Pay. Det er dog endnu ikke klart, hvilke vilkår Apple vil fastsætte for brugen.²⁶

At en stadig større del af vores liv og samfundets nøglefunktioner foregår digitalt, er en kæmpe styrke. Men det skaber også økonomiske, demokratiske og sikkerhedspolitiske

udfordringer. Den udbredte anvendelse af tech-giganternes digitale infrastruktur kan, i kombination med stærkt begrænset adgang til tech-giganternes maskinrum og beslutninger, skabe afhængighed og medføre sårbarheder. Tech-giganterne kan have økonomiske interesser, som ikke stemmer overens med samfundets værdier, og de kan være underlagt stater, der ikke ønsker Danmark det godt. Hvis den digitale infrastruktur drives, uden at danske myndigheder eller offentlighed har effektiv adgang til og indflydelse på maskinrummet, mister samfundet muligheden for at monitorere og identificere potentielle risici og sårbarheder og dermed træffe de nødvendige foranstaltninger til at sikre den demokratiske kontrol.

I fremtiden vil endnu flere dele af samfundet være afhængige af og koblet op på digitale løsninger. Det gør kontrol med infrastrukturen helt central. Der findes i dag ikke et offentligt overblik over ejerskabet af den type digital infrastruktur, som ekspertgruppen behandler i rapporten. Ekspertgruppen mener, at der skal være et overblik over samt kontrol med den digitale infrastruktur, der er fundamentet for samfundet og det danske erhvervsliv. Det vil kræve et tæt og effektivt samarbejde mellem myndigheder på tværs af stat, regioner og kommuner. Der kunne desuden etableres et råd eller organ for digital infrastruktur, hvis opgave er at skabe transparens og rådgive om, hvordan den digitale infrastruktur indrettes på en ansvarlig måde, hvor der arbejdes for størst mulig demokratisk kontrol.



PRINCIP 2

DATA SKAL GØRES TILGÆNGELIGE PÅ MÅDER, DER KAN GAVNE OG STYRKE INDIVIDET OG FREMTIDENS SAMFUND

PEJLEMÆRKER

- Tech-giganterne har sikret, at borgerne let kan eksportere og dele deres data med andre aktører på en overskuelig og sikker måde.
- Øget brug og understøttelse af data spaces har gjort det muligt at dele og anvende data på tværs af tjenester til afgrænsede formål på en sikker og effektiv måde.
- Det er nemt for borgerne at få et overblik over, hvad de har givet samtykke til, og hvordan de har kontrol med, hvordan deres data bliver delt.



Data er i dag et værdifuldt aktiv for borgere, virksomheder og samfundet. Data og datastrømme går igennem alle dele af den digitale infrastruktur og bliver af tech-giganterne primært brugt til at optimere tjenester og produkter og til kommercielle formål som reklamesalg og fastholdelse af brugere. Den store koncentration af data hos tech-giganterne gør dem magtfulde, fordi de får stor indsigt i brugernes adfærd og psykologiske profiler. Det er en viden, der er værdifuld, når det gælder markedsføring, men som også kan misbruges til f.eks. at manipulere befolkningsgrupper.

De indsamlede data gavner i alt for lille grad det enkelte individ og samfundet. Brugere kan ofte ikke selv få glæde af deres data, fordi de ligger i lukkede siloer – og ofte hos tech-

giganterne. Det skyldes blandt andet, at brugerne ikke på en nem måde kan benytte data, der er opsamlet hos én tjeneste på en ny tjeneste. Brugere har adgang til deres specifikke data hos hver aktør, men kan ikke udnytte det fulde potentiale af deres samlede data.

Det betyder, at borgere ikke kan drage fordel af deres data på tværs af forskellige tjenester og ikke kan få et samlet overblik over egne data. Eksempelvis ville det kunne skabe bedre og mere personligt tilpassede sundhedsbehandlinger, hvis borgere kunne give sundhedsvæsenet mulighed for at modtage og anvende borgeres selvindsamlede data fra smartphones, smartwatches, pulsøre mv.²⁷ De lukkede siloer kan også begrænse innovation og udvikling af alternative tjenester, der



REGULERING, DER STYRKER ADGANGEN TIL DATA

GDPR

GDPR (databeskyttelsesforordningen) har fundet anvendelse siden 2018 og indeholder en lang række krav, der skal overholdes ved behandling af personoplysninger. Databeskyttelsesreglerne indeholder en lang række rettigheder for den registrerede, bl.a. ret til indsigt i, hvilke oplysninger en dataansvarlig behandler om den pågældende, og ret til dataportabilitet, dvs. visse muligheder for den registrerede til at overføre personoplysninger om den pågældende selv fra én dataansvarlig til den anden.

DIGITAL MARKETS ACT

Digital Markets Act (forordningen om digitale markeder) fastsætter krav til tech-giganterne, f.eks. hvilke data virksomheder, der benytter en gatekeepers tjeneste, skal have adgang til. De data kan give virksomhederne mulighed for at forstå markedstrends og forbrugeradfærd mere dybdegående og hjælpe virksomhederne med at forbedre deres egne produkter og tjenester. Alt det kan være med til at gøre det muligt for danske og europæiske virksomheder at udfordre den indgroede position, som tech-giganterne har på visse markeder.

DATA ACT

Data Act (dataforordningen) skal fremme adgang til og anvendelse af data. Helt centralt vil forordningen gøre det obligatorisk for udbydere at dele data, der er genereret ved brug af et produkt eller en relateret tjeneste ("Internet of Things-produkter") med brugeren. Det vil sige, at enkeltpersoner og virksomheder får en adgangsret til data, de selv genererer ved brug af produkter eller tjenester. Derudover etablerer forordningen regler for databehandlingstjenester, f.eks. cloud-tjenester, der skal gøre det lettere for brugere at skifte mellem databehandlings-tjenester. Der etableres desuden rammer for datadelingsaftaler med henblik på at beskytte mikrovirksomheder og SMV'er mod urimelige aftalevilkår om datadeling. Forordningen indfører foranstaltninger mod beskyttelse af tredjeparters ulovlige adgang til ikke-persondata i EU. Som en del af forordningen vil der blive udarbejdet standarder, der skal understøtte datadeling på tværs af sektorer.

DATA GOVERNANCE ACT

Data Governance Act (datastyringsforordningen) skal skabe en ramme for sikker, fair og åben dataudveksling i EU. Et af forordningens primære mål er at lette dataudveksling på tværs af offentlige og private sektorer samt mellem medlemsstaterne og EU-institutionerne. Data Governance Act skal fremme datasuverænitet og kontrol over data for både EU-borgere og virksomheder for at styrke EU's position i den globale dataøkonomi. Den opfordrer også til øget datadeling i EU, især inden for sektorer som sundhed, miljø og industri, med det formål at fremme innovation og vækst. Forordningen indeholder også bestemmelser om databeskyttelse for at sikre, at datasikkerhed og privatlivsrettigheder overholdes i henhold til GDPR.

kan skabe værdi for den enkelte og for samfundet, idet adgangen til data er begrænset og fragmenteret.

Digital Markets Act giver brugerne af tech-giganternes platforme flere muligheder for at kontrollere indsamlingen og anvendelsen af data, blandt andet ved at gøre det muligt at takke nej til, at tech-giganterne kombinerer brugerens data på tværs af deres platforme.

Mange brugere oplever dog stadig, at de ikke har tilstrækkelig nem adgang til og kontrol over data. Samtidig mangler der muligheder for, at brugerne effektivt kan få adgang til egne data og vælge, om de vil stille dem til rådighed for f.eks. forskere, den offentlige sektor eller private virksomheder, der kan bruge dataene til at løse udfordringer som f.eks. klimaproblemer, sundhedsproblemer og lignende.

En måde at dele data på er ved brug af fælles europæiske dataområder, såkaldte "data spaces". Formålet med data spaces er at skabe en sikker og troværdig infrastruktur til at dele data på tværs af mange forskellige aktører, sektorer og lande. Infrastrukturen skal gøre det lettere og mere gennemsigtigt at give adgang til data til bestemte formål. Ekspertgruppen støtter EU's igangværende arbejde med data spaces.

Ekspertgruppen mener, at der skal sættes fokus på de fordele og gevinster, der kan opnås ved sikker og effektiv datadeling. Det gælder

både for borgeren, det danske samfund og virksomhederne. Derfor er det vigtigt at støtte effektiv implementering af Digital Markets Act, Data Act og Data Governance Act. For at sikre, at data forbliver i Danmark og Europa, vil det desuden være relevant at stille krav om datalokalisering i EU inden for mange områder, der har med digital infrastruktur at gøre. Kravet kan også indebære, at f.eks. cloud-udbydere skal have juridisk hovedsæde i Europa.

Ekspertgruppen mener samtidig, at et vigtigt fokus bør være at informere danske borgere om deres ret til f.eks. at få flyttet deres data, om deres muligheder for at bruge disse data til gode formål, og om deres ret til at klage, hvis deres rettigheder ikke bliver overholdt. Her kan man lade sig inspirere af den danske nonprofitorganisation Data for Good Foundation. Gennem Data for Good-platformen får borgere bedre kontrol og overblik over egne data og mulighed for at dele egne data, når det giver mening for den enkelte. Samtidig bliver der skabt et økosystem, hvor data anonymt kan omsættes til ny viden til gavn for den enkelte såvel som for virksomheder og det offentlige.²⁸

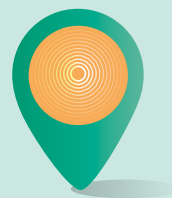
Et område, hvor det vil være relevant at styrke de offentlige datasæt, er beskrevet i National plan for bevægelsesdata,²⁹ hvor det offentlige ved hjælp af f.eks. satellitter og teledata kan understøtte innovation og en uafhængighed af tech-giganter på et voksende marked for mobilitet.

PRINCIP 3

ALTERNATIVER TIL TECH-GIGANTERNES TJENESTER SKAL KUNNE OPSTÅ OG VOKSE SIG STORE

PEJLEMÆRKER

- Danmark og ligesindede lande baner vej for opbygningen af digitale infrastrukturer med fokus på ansvarlighed, sikkerhed og demokratisk kontrol.
- Der er et digitalt indre marked med gode vilkår for investering i europæiske tech-virksomheder for at fremme konkurrenceevnen gennem innovation, forskning og teknologisk udvikling.
- Det er nemmere for tech-iværksættere og -virksomheder at rejse risikovillig kapital i Danmark og på tværs af EU, bl.a. til børsnoteringer og til at vokse sig store og blive inden for EU's grænser.
- Europa-Kommissionen prioriterer håndhævelsen af konkurrencereglerne og Digital Markets Act over for tech-giganterne.



Tech-giganterne har vokset sig så store, at de på mange områder er blevet uomgængelige for både virksomheder, myndigheder og borgere. Vi er afhængige af dem for at kommunikere, interagere og handle med hinanden digitalt. Samtidig har tech-giganternes markedsdominans negative konsekvenser for effektiv konkurrence og innovation og gør det svært for alternative tjenester at få fodfæste. Manglende konkurrence betyder, at priserne er højere og udvalget dårligere end i en situation med velfungerende konkurrence.

Tech-giganter som Amazon og Google kan på grund af deres position rangere, promovere

eller helt udelukke bestemt indhold. Det kan have stor betydning for, hvilke virksomheder der får bedst mulighed for at nå deres kunder, og for, hvilket udbud og hvilke varer forbrugerne bliver præsenteret for. Tech-gigantene kan også spille en dobbelt rolle; nogle driver f.eks. en markedsplads, hvor uafhængige sælgere kan sælge produkter direkte til forbrugerne, og samtidig sælger platformen selv produkter som forhandler og er i konkurrence med disse uafhængige sælgere. Den dobbelte rolle giver adgang til en masse viden og store datasæt om de uafhængige sælgeres aktiviteter på deres platforme, som tech-gigantene kan udnytte til egen fordel, f.eks. når det gælder produktudvikling, produkt-

> CLOUDTJENESTER

Når data er lagret i en cloudtjeneste, er det muligt for brugere at få adgang til deres data fra enhver enhed med internetadgang. Samtidig giver det virksomheder mulighed for at udnytte store mængder data og regnekraft uden at skulle investere i og vedligeholde egne servere. I stedet for at opretholde egne servere og egen infrastruktur kan virksomheder og enkeltpersoner købe adgang til cloudtjenester fra tredjepartsudbydere. Selvom clouddata typisk er krypterede, ligger de stadig hos en privat virksomhed, der dermed har en form for kontrol over dem. Det spiller også en rolle, hvor virksomheden har valgt at placere dataene fysisk, da den fysiske placering kan være underlagt national lovgivning, der giver myndigheder eller efterretnings-tjenester adgang til data. Det gælder, uanset om de er placeret i Kina eller USA.



placering og prissætning. Endelig spiller tech-giganternes vilkår en afgørende rolle for de virksomheder, der bruger tjenesterne til at nå deres kunder. I efteråret 2023 blev Booking.com eksempelvis kritiseret for ikke at betale hotellerne på platformen til tiden, hvilket udfordrede flere små hotellers økonomi.³⁰

De få dominerende aktører inden for cloud-tjenester, hvor særligt Amazon og Microsoft har store dele af markedet, betyder, at virksomheder, offentlige myndigheder og organisationer har begrænsede valgmuligheder. Det kan betyde, at konkurrencen ikke er effektiv, og at priserne er højere, end de ellers ville være.

De store aktører på cloudmarkedet har en betydelig fordel, når det gælder udvikling og drift af kunstig intelligens som f.eks. de store sprogmodeller. Det kræver enorme mængder data og en betydelig regnekraft at træne og drive kunstig intelligens, og cloudtjenester er en ideel infrastruktur til dette. Det kan både give tech-giganterne en fordel i konkurrencen og have betydning for andre virksomheders muligheder. Der har været flere eksempler på, at tech-giganterne har indgået partnerskaber med nye aktører inden for kunstig intelligens, f.eks. Microsofts partnerskab med OpenAI³¹ og franske Mistral³².

Tech-giganternes stærke position på tværs af markeder kan skyldes, at der ikke findes alternativer af lige så god kvalitet eller til samme pris. Det hænger sammen med, at det er svært for andre virksomheder at konkurrere med tech-giganterne på grund af bl.a. netværkseffekter og tech-giganternes store datamængder og økonomiske forspring. Den nye danske supercomputer, som Novo Nordisk Fonden og statens fond EIFO har bevilliget 700 mio. kr. til, fremstår eksempelvis som en meget lille investering sammenlignet med de investeringer, tech-giganterne kan foretage i kunstig intelligens. Alene Meta har tidligere indikeret, at de i 2023 ville bruge 225 mia. kr. på udvikling af deres kunstig intelligenskapacitet.³³ Samtidig kan det være vanskeligt

for mindre virksomheder at rejse den nødvendige kapital og tiltrække de dygtigste udviklere. Små virksomheder bliver med jævne mellemrum opkøbt af tech-giganterne, inden de når at blive seriøse konkurrenter. Overordnet peger en række rapporter på, at Europas konkurrenceevne, særligt på det digitale område, er udfordret og kræver nye indsatser.³⁴

Tech-giganternes dominans på markedet medfører sårbarheder, ligesom den kan påvirke Danmarks autonomi og økonomi. Det er derfor vigtigt, at tech-giganternes rolle udfordres. Danmark og ligesindede lande kan bane vejen for opbygningen af alternativer til tech-giganterne, f.eks. gennem erhvervsregulering, styrket konkurrence, udbudsregler, investeringer og offentlig-private samarbejder. Det kræver fra Danmark og EU et fokus på at gøre det nemmere for iværksættere at starte og skalere deres virksomheder og indføre aktiv kontrol med opkøb og fusioner. Et stærkere samspil mellem universiteter og erhvervsliv kan også være med til at skabe vækst, ligesom der skal være bedre mulighed for it-iværksætteri for forskere og studerende.³⁵

Derudover skal tech-iværksættere nemmere kunne rejse risikovillig kapital, både i Danmark og på tværs af EU, f.eks. til børsnoteringer og vækst. Det kan også overvejes, om statslige investeringer fra f.eks. EIFO, Innovationsfonden samt pensionskasserne i højere grad bør fokusere på danske startups.

PRINCIP 4

INGEN SKAL VÆRE TVUNGET TIL AT BRUGE TECH-GIGANTERNES TJENESTER FOR AT FÅ INFORMATION OG DELTAGE I SOCIALE, KULTURELLE OG DEMOKRATISKE FÆLLESSKABER

PEJLEMÆRKER

- a. Politikere og offentlige organisationer bruger flere kanaler til information og budskaber.
- b. Den offentlige debat foregår på tjenester og inden for nogle rammer, der sikrer, at alle kan komme til orde.
- c. En fri og alsidig mediebranche og stærk public service bidrager til at understøtte den demokratiske samtale.



Mange borgere, foreninger, institutioner, virksomheder og politikere oplever, at de er nødt til at være til stede på tech-giganternes tjenester for at få information og for at kunne interagere og kommunikere med omverdenen samt deltage i den demokratiske samtale. Det er med til at understøtte tech-giganternes forretningsmodeller, der bygger på fastholdelse og indsamling af data om brugerne, jf. ekspertgruppens afrapportering om forretningsmodeller.

På sociale medier kan politikere, eksperter, debattører mv. kommunikere direkte til borgerne. Det øger åbenheden om det politiske arbejde. Sociale medier giver også borgere mulighed for at udtrykke deres synspunkter, modtage information og deltage i diskussioner. Samtidig kommunikerer mange myndigheder via de sociale medier for at kun-

ne nå effektivt ud til borgerne, ligesom den politiske og demokratiske samtale, ud over på de traditionelle medier, i høj grad foregår på sociale medier.

Sociale medier er også blevet et nemt værktøj for mange foreninger, herunder idrætsforeninger og andre fællesskaber, til at kommunikere bredt og styrke fællesskabet om foreningen eller gruppen samt til at rekruttere nye medlemmer. Endelig bruger unge i høj grad sociale medier til at kommunikere med deres venner, f.eks. koordinere aktiviteter og dele stort og småt.

Når de sociale medier spiller en stor rolle i borgernes hverdag, kan det medføre demokratiske og sikkerhedsmæssige sårbarheder. Udfordringerne skyldes blandt andet, at præmis-

sen om offentlighed og den demokratiske samtale, hvor alle i princippet kan komme til orde og være synlige, udfordres af tech-giganternes praksis. Forskning viser, at det med tech-giganternes algoritmer langt fra er alle, der kommer til orde eller er synlige. Tværtimod får følelsesladet eller provokerende indhold hurtigere interaktioner fra andre brugere og bliver derfor spredt mere end neutralt indhold.³⁶ Der har også været flere eksempler, hvor danske politikere uden en egentlig grund har fået blokeret deres profiler på sociale medier eller har fået fjernet opslag, som ikke var ulovlige eller misinformerende – også i perioder med valg.

Når sociale medier er en så integreret del af danskeres hverdag, er det en udfordring for de borgere, der ikke ønsker at være til stede på platformene. Det kan presse borgere til at få profiler på bestemte sociale medier som Facebook og Snapchat, hvis den primære kommunikation med vennerne eller koordinering af den lokale idrætsforenings aktiviteter foregår dér. Borgerne har derfor ikke en reel mulighed for at fravælge tjenesterne, selv hvis de ønsker at være fri for tech-giganternes datahøst.

Når myndigheder er på sociale medier, kan de nå hurtigt ud til mange borgere. Andre kanaler har ofte ikke samme rækkevidde. Men det kan være problematisk, hvis borgerne ikke er bekendt med og kan bruge andre "officielle kanaler" til information fra offentlige myndigheder, politi og beredskab. Det skyldes blandt andet, at forbindelsen på sociale medier går gennem en privat virksomhed, der pludselig kan vælge at begrænse eller lukke for adgangen.

I dag får mange – og særligt de unge – store dele af deres nyheder gennem sociale medier. Via de sociale medier har tjenesterne indflydelse på, hvilke nyheder borgerne præsenteres for, og hvordan. Mange nyheder på platformene kommer ikke fra traditionelle nyhedsmidler eller journalister, som er underlagt et redaktionelt ansvar. Der er også eksem-

pler på, at kendte troværdige journalister og mediers navn misbruges til svindel på sociale medier. Det kan mindske adgangen til reel og relevant samfundsinformation, undergrave tilliden til etablerede medier og øge risikoen for *fake news*, når nyhederne bliver viderebragt uden kritisk journalistik og faktatjek.³⁷ Samtidig tager tech-giganterne en stadig større andel af de samlede annonceindtægter på bekostning af de traditionelle medier,³⁸ hvilket medvirker til at svække mangfoldigheden i mediemarkedet.

Ovennævnte illustrerer nogle af de demokratiske, sikkerhedsmæssige og økonomiske sårbarheder, som tech-giganternes rolle skaber. Ekspertgruppen mener ikke, at tech-giganter i deres nuværende form kan indtage rollen som dominerende digital infrastruktur, såfremt man ønsker at sikre den demokratiske samtale, foreningslivet og nyhedsformidlingen.

Ekspertgruppen mener, at det skal være muligt at følge med i og deltage i den demokratiske samtale uden at gøre brug af tech-giganternes tjenester. Når interaktionen primært sker via sociale medier, kan platformenes algoritmer, funktioner og karakteristika påvirke den demokratiske samtale, fællesskaber og civilsamfundets virke. Det er derfor ekspertgruppens holdning, at eksempelvis politikerne har et ansvar for også at bruge andre kanaler, herunder egne hjemmesider og danske medier – og ikke kun de store sociale medier, når de ønsker at kommunikere med borgerne.

Det er også vigtigt at overveje, hvordan man kan sikre demokratisk deltagelse og offentlig debat, herunder give plads til forskelligartede synspunkter. Det kan f.eks. overvejes, om mediestøtten kan forbedres og gøres mere platform- og teknologineutral ved at tilpasse den medieudviklingen og det digitaliserede og globaliserede medielandskab.

PRINCIP 5

DEN OFFENTLIGE SEKTOR SKAL IKKE VÆRE AFHÆNGIG AF TECH-GIGANTERNES TJENESTER

PEJLEMÆRKER

- a. Den offentlige sektor bruger sikre og ansvarlige tjenester og software, der afspejler danske og europæiske værdier.
- b. Den offentlige sektor har de rette kompetencer til at indkøbe og arbejde med alternative tjenester og software, f.eks. open source.
- c. Den offentlige sektor er ikke afhængig af tech-giganterne og undgår at blive låst fast til én udbyder, bl.a. ved at lægge vægt på interoperabilitet og open source i digitale løsninger.
- d. Den offentlige sektor laver, når det giver mening, flere mindre og opdeltede offentlige udbud, så det bliver muligt for mindre aktører at deltage.



Mange offentlige institutioner og kommuner bruger tech-giganternes tjenester: Office-pakken, Windows som operativsystem og Apples iPhone og iPad. Hvis den offentlige sektor primært anvender tech-giganternes tjenester uden blik for mulige alternativer, kan det være med til at understøtte og udbygge tech-giganternes stærke position, mindske konkurrencen, øge afhængigheden og dermed gøre institutionerne sårbare. Samtidig kan der opstå situationer, hvor det er vanskeligt at skifte væk fra tech-giganternes tjenester – selv i de situationer, hvor priserne stiger. Siden 2018 er kommunernes udgifter til Microsoft-licenser steget fra 313 mio. kr. til 538 mio. kr. – også i takt med, at stadig flere funktionaliteter tages i brug.³⁹ Det er et eks-

empel på en økonomisk udfordring ved tech-giganternes rolle i den digitale infrastruktur.

Tech-giganternes tjenester kan også skabe sikkerhedspolitiske sårbarheder for den offentlige sektor, f.eks. når det gælder spionage.⁴⁰ I mange lande, inkl. Danmark, er der i det seneste år indført forbud mod TikTok på arbejdstelefoner i offentlige myndigheder og flere private virksomheder. Kritikken er toledet. Den handler om både risici ved Kinas adgang til data og bekymringer ved den store dataindsamling, der finder sted. Ud over de sikkerhedspolitiske sårbarheder, som tech-giganterne skaber, er der også rejst kritik af, at

der i de offentlige it-systemer ikke er tilfredsstillende it-sikkerhed, og at flere statslige myndigheder ikke lever op til de tekniske minimumskrav til it-sikkerhed.⁴¹ Dette er dog uden for ekspertgruppens mandat.

En del af forklaringen på tech-giganternes position er, at offentlige udbud nogle gange bliver så store, at kun de største virksomheder har gode muligheder for at vinde kontrakterne. Det var f.eks. tilfældet, da KL og KOMBIT ønskede at udvikle ét samlet it-system til alle kommunale vuggestuer, børnehaver, SFO'er og skoler (Aula). Store udbydere kan give bedre leveringssikkerhed, og de har typisk også flere ressourcer og mere viden. Men i forhold til f.eks. udbuddet af Aula betød det store, samlede udbud, at tidligere og mindre leverandører af tjenester, der havde visse funktionelle overlap med Aula, havde svært ved at deltage og fik dårligere mulighed for at levere lokale og skræddersyede løsninger – og dermed blev deres forretningsgrundlag udfordret.⁴²

I Danmark er der eksempler på, at det offentlige har forsøgt at gøre sig uafhængige af tech-giganternes infrastruktur ved at benytte og styrke danske alternative løsninger. GovCloud er f.eks. Statens IT's cloudløsning.

Hensigten er at tilbyde myndighederne en sikker cloudbaseret driftsplatform bygget på open source. Applikationer og data i GovCloud vil til enhver tid være placeret i Statens IT's datacentre i Danmark. Herudover findes OS2-fællesskabet, der er et samarbejde for offentlige myndigheder, der ønsker at skabe, dele og vedligeholde open source-løsninger med hjælp fra private it-leverandører.

Hvis man vil have mere kontrol og styrke velstand, demokrati og sikkerhed, skal den offentlige sektor gå forrest og vælge alternativer til tech-giganterne, f.eks. når det gælder cloudtjenester og kunstig intelligenssystemer. Fokus skal være på databeskyttelse, dataetik, interoperabilitet og open source.

Sådanne krav bør desuden fremgå af offentlige udbud, jf. ekspertgruppens tidligere anbefaling 4.2. om kunstig intelligens. Der kan i den forbindelse hentes inspiration fra den tyske delstat Schleswig-Holstein, som har forladt Microsoft til fordel for LibreOffice. Som et forsøg kunne der i Danmark udpeges f.eks. tre pilotkommuner, der understøttes økonomisk og fagligt i at overgå til alternativer til tech-giganternes produkter til brug for inspiration og erfaringsdeling med andre kommuner.

> AI ACT

AI Act (forordningen om harmoniserede regler for kunstig intelligens) trådte i kraft den 1. august 2024. AI Act er de første bindende regler for anvendelse af kunstig intelligens på verdensplan. Forordningen indfører forbud mod kunstig intelligens med uacceptabel risiko, f.eks. visse typer brug af ansigtsgenkendelse. AI Act stiller desuden krav til kunstig intelligens med høj risiko, f.eks. i forbindelse med rekruttering eller offentlig sagsbehandling. I forordningen indgår også et transparenskrav, så brugere skal gøres bekendt med, at et produkt eller en tjeneste bruger kunstig intelligens, f.eks. chatbots, eller hvis indhold er genereret med kunstig intelligens, f.eks. deep-fakes.

PRINCIP 6

DANSKE UDDANNELSESINSTITUTIONER SKAL VÆRE FRI FRA KOMMERCIELLE TECH-GIGANTER

PEJLEMÆRKER

- Uddannelsesinstitutionernes digitale værktøjer er alderssvarende, reklamefrie og sporingsfrie og udnytter ikke børns data til kommercielle formål.
- Brug af digitale tjenester må ikke kræve oprettelse af personlige konti, som trækker elever og studerende ind i tech-giganternes økosystem.
- Kommunerne gør i højere grad brug af skandinaviske og europæiske samarbejds-, lærings- og undervisningsværktøjer.



En vigtig grundsten i det danske samfund er vores uddannelsesinstitutioner og en folkeskole, som de fleste danskere benytter. De giver unge mennesker nogle værdier med hensyn til f.eks. tillid, dialog, samarbejde og frisind. Vi skal derfor være bevidste om, hvem vi giver adgang til dette rum.

I dag har tech-giganterne i vidt omfang adgang til børn og unges data. Det sker gennem de sociale netværk, som børnene er på og f.eks. gennem chat-apps, onlinespil mv. Men det kan også ske i klasseværelset og på de uddannelsesinstitutioner, som de unge går på.

Værktøjer som Google Workspace for Education, Microsoft 365 for Education⁴³ og de iPads

og computere, som elever får udleveret og bruger, er en del af den digitale infrastruktur på grund af deres betydning for undervisningen og deres rolle i bl.a. at facilitere kommunikation mellem elever og lærere. 15-årige danske skoleelever bruger i gennemsnit digitale redskaber i 3,8 timer om dagen til læringsaktiviteter i skolen.⁴⁴ Man kan således ikke være elev eller studerende i Danmark uden at blive mødt af og vænnet til tech-giganternes tjenester.⁴⁵

Det giver tech-giganterne en stor fordel, at de allerede fra en tidlig alder kan vænne børn og unge til at anvende deres produkter. Det kan betyde, at børn og unge vil efterspørge de samme produkter, når de skal videre i uddannelsessystemet og på arbejdsmarkedet.

Derfor får kommunerne også produkterne tilbudt til meget lave priser.⁴⁶ Og i en presset kommunal økonomi kan det være svært for kommunerne at afslå et sådant tilbud.

Der er i de seneste år rejst kritik af kommunernes brug af Google Chromebooks og manglende efterlevelse af databeskyttelsesreglerne. Sagen startede i 2019, hvor en far klagede over, at hans søns navn og skole var offentligt på YouTube. Senest har Datatilsynet i januar 2024 vurderet, at de 53 involverede kommuners brug af Google Workspace ikke levede op til databeskyttelsesreglerne. Det skyldtes, at anvendelsen indebar videregivelse af personoplysninger til Google til vedligeholdelse og forbedring af Google-løsninger eller til måling af ydeevne og udvikling af nye funktioner og tjenester, som ikke havde hjemmel i folkeskoleloven. Kommunerne har sammen med Google efterfølgende fundet en kontraktuel løsning på problematikken.

Ekspertgruppen mener, at uddannelsesinstitutionerne skal gøre brug af reklame- og sporing-frie digitale undervisnings- og læringsværktøjer. Som det ser ud nu, er der intet overblik over, hvilke apps og services der bliver brugt hvor og til hvilke aldersgrupper. KL kunne i samarbejde med f.eks. tre kommuner etablere et pilotforsøg i skolerne med at bruge systemer og open source værktøjer, som ikke er ejet af tech-giganterne, og som understøttes økonomisk og fagligt.

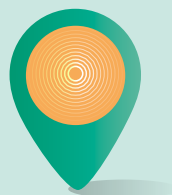


PRINCIP 7

TECH-GIGANTERNES PLATFORME SKAL VÆRE TRYKKE STEDER AT HANDLE

PEJLEMÆRKER

- a. Danske virksomheder, der sælger produkter på tech-giganternes platforme, har rimelige vilkår og kan komme i kontakt med platformene.
- b. Danske forbrugere oplyses om rettigheder og risici ved handel på tech-giganternes platforme, f.eks. med hensyn til forretningsmetoder og arbejdsvilkår.
- c. Handelsplatforme kan kun operere i Danmark, hvis produkterne på deres platforme overholder dansk og europæisk lovgivning f.eks. danske produkt- og sikkerhedskrav.



Tech-giganternes platforme bliver i stigende grad brugt af borgerne til at købe alt fra fly- og hotelbilletter til dagligdagsprodukter og elektronik. Men det er ikke altid platformen, der handles med, men en virksomhed, der sælger sine produkter via platformen. Brugere kan derfor have svært ved at vide, hvem de skal kontakte, hvis der er et problem med en vare eller tjeneste, som de har købt på platformen, f.eks. køb af flybilletter, hotel eller billeje. Det kan også være køb af et produkt på en onlinemarkedsplads, f.eks. Amazon eller Temu, hvor produktet viser sig at være farligt.

Med Digital Services Act (forordningen om digitale tjenester) skal onlinemarkedspladser, f.eks. Amazon, Temu og Wish, leve op til en række forpligtelser såsom at bekæmpe udbredelsen af ulovlige varer. Onlinemarkedspladser skal nu sikre, at sælgere på markedspladserne giver verificerede oplysninger om deres identitet, før de kan begynde at sælge deres varer. Onlinemarkedspladserne skal også garantere, at brugerne let kan identificere den person, der er ansvarlig for salget. Hvis en onlinemarkedsplads får kendskab til sælgerens salg af et ulovligt produkt eller en ulovlig tjeneste, skal brugerne, der har købt den ulovlige vare eller det ulovlige produkt, have besked og oplyses om sælgerens identitet og mulighederne for at klage.

Senest har der været opmærksomhed om den store kinesiske tech-gigant Temu, der på kort tid har gjort indtog i Danmark med billige produkter, som til gengæld er af lav kvalitet og i flere tilfælde har vist sig ikke at overholde europæiske og danske produktregler.

Der har samtidig været eksempler på, at Facebook og Instagram ikke har været hurtige nok til at fjerne reklamer for falske hjemmesider, der lokker med lave priser, men som udelukkende er skabt for at snyde forbrugerne.⁴⁷

Ekspertgruppen ønsker derfor, at borgerne i højere grad gøres opmærksom på såvel deres rettigheder som risici, når de handler på platformene, og at myndighederne håndhæver regulering og har effektive værktøjer til at skride ind og lukke ned for handelsplatforme, der tillader salg af produkter, der f.eks. ikke er sikre at anvende.

➤ PRODUKTLOVGIVNING

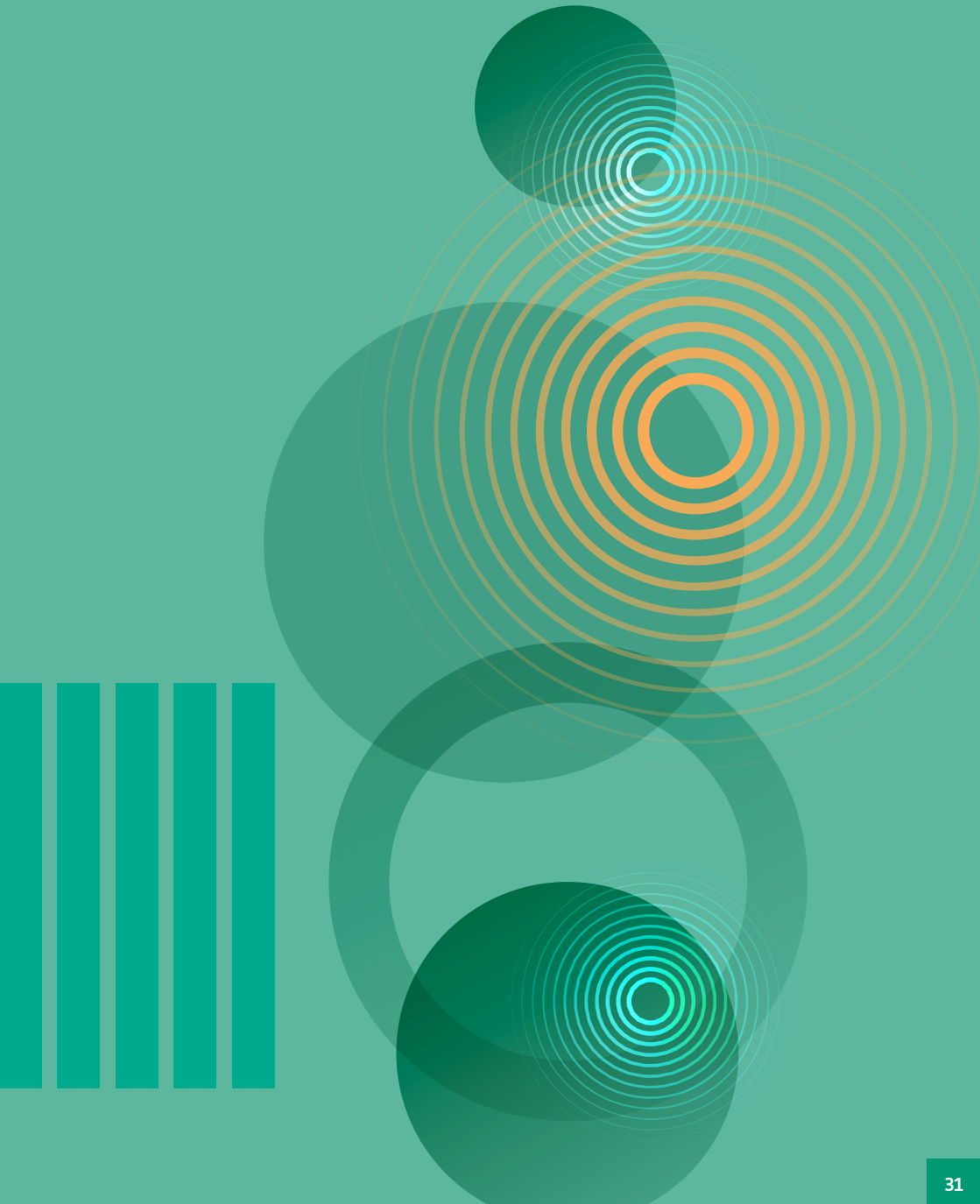
Market Surveillance Regulation (markedsovervågningsforordningen) er en EU-forordning, der fastsætter et fælles europæisk grundlag for produkters lovlighed og myndighedernes overvågning af produkter. Der stilles overordnede krav til de erhvervsdrivende, som gør produkter tilgængelige på det europæiske marked. Forordningen suppleres af en lang række EU-forordninger og -direktiver, der fastsætter krav til specifikke typer af produkter, f.eks. legetøj, maskiner og elprodukter. Produkter, der markedsføres i Danmark og EU, skal overholde produktlovgivningen, uanset om produkterne importeres af forbrugere direkte fra eksempelvis Kina eller tredjelande.

> DIGITALE PLATFORMES ANSVAR MED HENSYN TIL DE VARER, DER SÆLGES PÅ PLATFORMENE

Digital Services Act giver platformene en pligt til at sikre, at forbrugerne kan se, at det ikke er platformen, forbrugeren handler med, men derimod en tredjepartssælger. Den oplysning kan dog præsenteres på mange måder, og i virkelighedens verden er det ikke altid tydeligt for forbrugeren, om det er platformen, der er ansvarlig for handlen, eller om den kun formidler ydelsen. Det kan have konsekvenser for forbrugernes rettigheder, da ansvaret som udgangspunkt er sælgerens.

Platformene er, som reglerne er i dag, som udgangspunkt ikke ansvarlige, hvis der sælges ulovlige produkter på deres platforme. Hvis en platform får kendskab til et ulovligt produkt på platformen, kan platformen dog have et straffe- og/eller erstatningsretligt ansvar efter anden lovgivning, f.eks. produktsikkerhedsreglerne, hvis platformen ikke straks tager skridt til at fjerne produktet.







EKSPERTGRUPPENS SAMMENSÆTNING

Ekspertgruppen har ved afgivelse af denne delafrapportering haft følgende sammensætning:

- Mikkel Flyverbom (formand), Copenhagen Business School
- Lars Thinggaard, Tech for Life
- Lone Sunesen, TV MIDT/VEST
- Mie Oehlenschläger, Tech & Childhood
- Miriam Michaelsen, Medierådet for Børn og Unge
- Pernille Tranberg, DataEthics
- Rebecca Adler-Nissen, Københavns Universitet
- Rikke Frank Jørgensen, Institut for Menneskerettigheder
- Sune Lehmann, Danmarks Tekniske Universitet
- Thomas Bolander, Danmarks Tekniske Universitet
- Peter Svarre, digital strateg, foredragsholder og forfatter

Erhvervsministeriet og efterfølgende Digitaliseringsministeriet har udgjort ekspertgruppens sekretariat i samarbejde med andre relevante ministerier, herunder Kulturministeriet, Udenrigsministeriet, Justitsministeriet og Børne- og Undervisningsministeriet.

EKSPERTGRUPPENS KOMMISSORIUM

De internationale tech-giganter har meget stor indflydelse på samfundslivet, økonomien og almindelige menneskers hverdag både nationalt og internationalt. Regeringen har igangsat en række initiativer, men der vil fortsat være brug for politisk udvikling og nye tiltag.

Regeringen nedsætter på den baggrund – som led i regeringens udspil ”Tech-giganter: mere retfærdig konkurrence og bedre forbrugerbeskyttelse” fra august 2021 – en ekstern ekspertgruppe. Ekspertgruppen får til formål at understøtte regeringens arbejde med at håndtere problemstillinger, der er forbundet med tech-gigant-dagsordenen i et nationalt og internationalt perspektiv.

Baggrund

Konsekvenserne af tech-giganternes udvikling og indflydelse har betydning på en lang række områder, herunder på skatte-, kultur- og konkurrenceområdet. Fælles for de store tech-giganter er, at deres indtog på det danske marked er båret af stor efterspørgsel på deres ydelser fra både virksomheder og borgere.

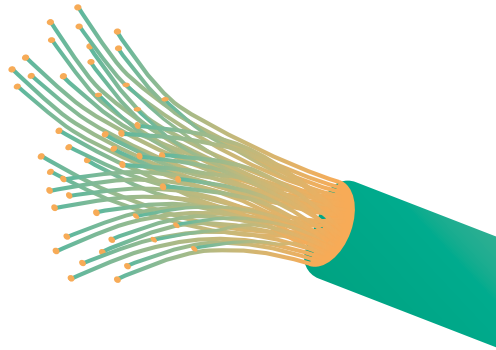
Tech-giganters tilstedeværelse og udvikling medfører dog samtidig en række udfordringer, som også har grænseoverskridende karakter.

Tech-giganterne opererer som oftest ud fra en forretningsmodel, der er baseret på at indsamle så mange data om deres brugere som muligt. Det er i praksis umuligt for brugerne at vide, hvilke data de frivilligt og ufrivilligt har videregivet til tech-giganterne, og hvordan dataene anvendes til videresalg, markedsføring mv.

Mange af de mest udbredte onlineplatforme er ejet af internationale tech-giganter og er i dag fora for kommunikation og offentlig debat. På den måde får tech-giganterne stor indflydelse på spillereglerne i den offentlige debat og demokratiske samtale.

Ligeledes er der udfordringer i forbindelse med spredning af ulovligt og skadeligt indhold, unfair konkurrencevilkår, skatteforhold, digital mistrivsel hos børn og unge, uigennemsigtige algoritmer og polariserende mekanismer. Desuden udfordrer tech-giganterne ordentlige arbejdsmarkedsvilkår, herunder særligt lønmodtagerrettigheder.

Endelig spiller tech-giganterne en voksende udenrigs- og sikkerhedspolitisk rolle i kontekst af den fortsatte teknologiske stormagtsrivalisering mellem USA og Kina, hvorfor det vil være vigtigt at balancere kritisk dialog med perspektiver på muligheder for vidensdeling, innovation og samarbejde.



Opgavebeskrivelse

Ekspertgruppen skal overordnet fungere som forum for drøftelse af strukturelle problemstillinger, hvor tech-giganternes forretningsmodel udfordrer vores samfund, kultur, økonomi, trivsel mv. I forlængelse heraf vil regeringen have mulighed for at anmode ekspertgruppen om at forholde sig til og vurdere konkrete sager og dilemmaer inden for tech-dagsordenen.

Konkret skal ekspertgruppen:

- Drøfte udfordringer ved tech-giganternes forretningsmodel og dens konsekvenser for det danske samfund, herunder for den demokratiske samtale.
- Komme med oplæg til, herunder belyse mulige positive såvel som negative konsekvenser, hvordan den demokratiske kontrol med tech-giganterne kan styrkes, herunder med særligt fokus på deres forretningsmodel.
- Identificere andre problemstillinger for det danske samfund i lyset af de strukturelle udfordringer, der følger af tech-giganternes forretningsmodel samt kvalificere disse og deres konsekvenser for det danske samfund.
- Fremlægge forslag og konkrete anbefalinger til håndtering af disse problemstillinger, herunder overveje, om de skal løses i nationalt eller EU-regi.

- Inddrage og drøfte internationale erfaringer i arbejdet for at sikre en ansvarlig teknologisk udvikling, der understøtter Danmarks demokrati, velstand og sikkerhed i en globalt forbundet verden.

Den enkelte ressortminister har mulighed for at fremsætte ønske om, at ekspertgruppen inddrages, når det gælder konkrete problemstillinger og dilemmaer inden for dennes ressortområde.

Ekspertgruppen skal i sit arbejde sikre løbende inddragelse af Dataetisk Råd.

Organisering

Ekspertgruppens formand og medlemmer udpeges personligt af erhvervsministeren. Ekspertgruppen forventes at bestå af 12 medlemmer med ekspertise og erfaring inden for tech-gigant-dagsordenen.

Ekspertgruppen nedsættes i første omgang for en toårig periode.

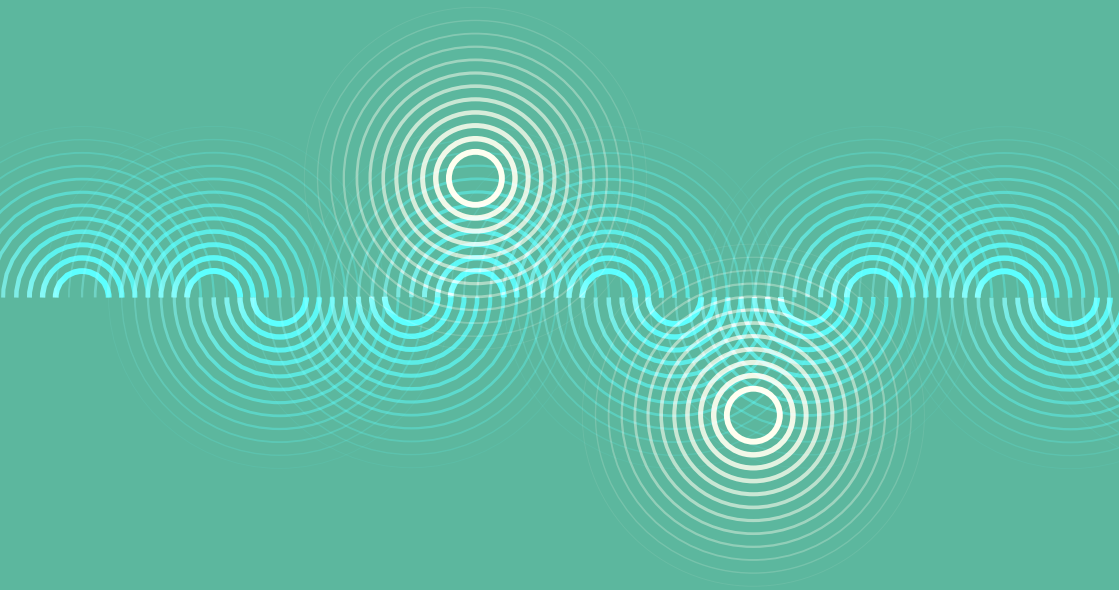
Ekspertgruppen vil blive sekretariatsbetjent af Erhvervsministeriet.

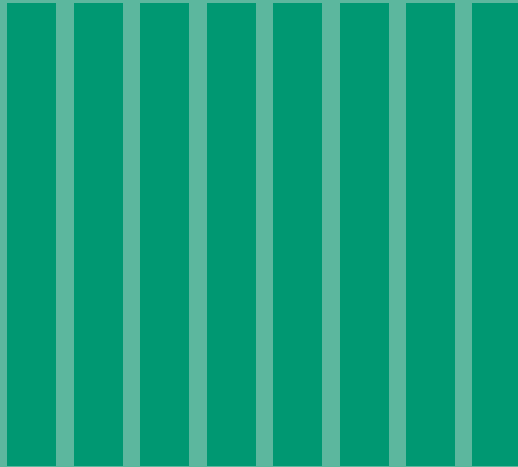
KILDELISTE

1. Se for eksempel <https://www.rdi.nl/radiocommunications-agency>, <https://www.digg.se/ledning-och-samordning/ena---sveriges-digitala-infrastruktur>
2. Databeskyttelseslovens § 3, stk. 9, og retshåndhævelseslovens § 27, stk. 3.
3. Visse it-systemer, som føres for den offentlige forvaltning, og som behandler personoplysninger, kan af justitsministeren pålægges kun at måtte opbevares helt eller delvist her i landet.
4. Erhvervsstyrelsen, *Formål og grundlag for screening af udenlandske investeringer og særlige økonomiske aftaler*. Lokaliseret den 5. november 2024 på <https://erhvervsstyrelsen.dk/formaal-og-grundlag-screening-af-udenlandske-investeringer-og-saerlige-oekonomiske-aftaler>
5. Energiwatch (2023), *NKT får afslag på frasalg af Photonics til japansk køber*. Lokaliseret den 5. november 2024 på <https://energiwatch.dk/Energinyt/Renewables/article15741089.ece>
6. Investeringsscreeningsloven (LOV nr 736 af 13/06/2023), *Lov om ændring af investerings-screeningsloven og lov om Klagenævnet for Udbud*. Erhvervsministeriet. <https://www.retsinformation.dk/eli/lt/a/2023/736>
7. Dansk Erhverv (2023), *Behov for hurtig myndighedsindsats i forhold til kommende EU-regler for kritisk infrastruktur*. Lokaliseret den 5. november 2024 på <https://www.danskerhverv.dk/presse-og-nyheder/nyheder/2023/februar/behov-for-hurtig-myndighedsindsats-i-forhold-til-kommende-eu-regler-for-kritisk-infrastruktur/>
8. CER bygger på og ophæver det nuværende direktiv 2008/114/EF af 8. december 2008 om europæisk kritisk infrastruktur (ECI-direktivet).
9. Dansk Standard, *Cyber Resilience Act*. Lokaliseret den 5. november 2024 på <https://www.ds.dk/da/i-fokus/lovgivning/lovgivning-paa-det-digitale-omraade-og-standarder/cyber-resilience-act>
10. Lai, S. S., & Flensburg, S. (2023), *Gateways: Comparing digital communication systems in Nordic welfare states*. Nordicom, University of Gothenburg, s. 174.
11. Ritzau (2023), *SpaceX-internet til færger i Danmark*. Lokaliseret den 23. august 2024 på <https://via.ritzau.dk/pressemeddelelse/13700555/spacex-internet-til-faerger-i-danmark?publisherId=12030451&lang=da>
12. DR (2008), *Historisk: 7.000 kilometer 'Havfrue' forbinder Danmark med New Jersey*. Lokaliseret den 23. august 2024 på <https://www.dr.dk/nyheder/regionale/syd/historisk-7000-kilometer-havfrue-forbinder-danmark-med-new-jersey>
13. DataEthics.eu (2023), *Big Tech Soft Power Danmark*. Lokaliseret den 23. august 2024 på Big tech soft power Danmark (dataethics.eu).
14. Brev af 15. september 2023 til USA's forsvarsminister Lloyd Austin fra USA's senatorer Jeanne Shaheen, Elizabeth Warren og Tammy Duckworth. Lokaliseret den 23. august 2024 på [Starlink.pdf \(senate.gov\)](#).
15. Ryan, F., Fritz, A. og Impiombato, D. (2020), *TikTok and WeChat Curating and controlling global information flows*. ASPI International Cyber Policy Centre.

16. Gueham, F. (2017), *Digital sovereignty – steps towards a new system of internet governance*. The Fondation pour l'innovation politique.
17. European Parliament (2020), *Digital sovereignty for Europe*.
18. Den 16. marts 2021 nedsatte regeringen Digitaliseringspartnerskabet. Digitaliseringspartnerskabet fik i opdrag at udarbejde anbefalinger til regeringen om, hvordan Danmark skal udnytte digitaliseringens muligheder i fremtiden. Digitaliseringspartnerskabet har blandt andet peget på, at det er i Danmarks klare interesse at fremme en vison for Europas digitale suverænitet, der er åben mod omverdenen, fremmer europæiske styrkepositioner og bygger oven på samarbejdet med andre demokratier. Se mere på: https://fm.dk/media/e53hnrmu/visioner-og-anbefalinger-til-danmark-som-et-digitalt-foregangsland-digitaliseringspartnerskabet_a.pdf, s. 60.
19. Adler-Nissen, R. og Eggeling, K. A. (2024), *The Discursive Struggle for Digital Sovereignty: Security, Economy, Rights and the Cloud Project Gaia-X*. JCMS 2024 Vol. 62, nr. 4. s. 993-1011.
20. AWS er et amerikansk firma, der leverer cloudløsninger og har datacentre i blandt andet Irland, Tyskland og Frankrig. Det indgår i Aula-aftalen, at data skal være placeret i et land i Europa. Se mere på: <https://aulainfo.dk/guide-til-projektledere/sikkerhed-i-aula/>
21. Butler, G. (2023), *UK Home Office signs £450m cloud deal with AWS*. Lokaliseret den 23. august 2024 på <https://www.datacenterdynamics.com/en/news/uk-home-office-signs-450m-cloud-deal-with-aws/>
22. DR (2024), *MitID endnu engang udsat for en type angreb, 'der kan bestilles for prisen af en cafe latte'*. Lokaliseret den 23. august 2024 på <https://www.dr.dk/nyheder/indland/mitid-endnu-engang-udsat-en-type-angreb-der-kan-bestilles-prisen-af-en-caffe-latte>
23. De såkaldte elektroniske "wallets" som f.eks. ApplePay og GooglePay fungerer kort sammenfattet som en elektronisk pung, som brugeren kan lægge et eller flere kort i. Betalingen gennemføres med det valgte betalingskort. Andre typer betalingsløsninger kan fungere anderledes, f.eks. hvor betalingen gennemføres konto-til-konto, eller hvor kunden deler betalingen op og får stillet en kredit til rådighed i forbindelse med købet. Se mere på: <https://www.kfst.dk/media/rbdcu40/20220616-betalingsrapport-2022-final.pdf>
24. Version2 (2023), *Seks banker vil udbyde Dankort i Apple Pay – men løbet er kørt, lyder det fra betalingskampen*. Lokaliseret den 23. august 2024 på <https://www.version2.dk/artikel/seks-banker-vil-udbyde-dankort-i-apple-pay-men-loebet-er-koert-lyder-det-fra-betalingskaempe>
25. Europa-Kommissionen (2024), *Commission seeks feedback on commitments offered by Apple over practices related to Apple Pay*. Lokaliseret den 23. august 2024 på https://ec.europa.eu/commission/presscorner/detail/en/ip_24_282
26. Dansk Erhverv (2024), *Langvarig kamp tager en positiv drejning: Apple frigiver afgørende betalingsteknologi*. Lokaliseret den 23. august 2024 på <https://www.danskerhverv.dk/presse-og-nyheder/nyheder/2024/februar/langvarig-kamp-tager-en-positiv-drejning-apple-frigiver-afgørende-betalingsteknologi/>
27. Digitaliseringspartnerskabet (2021), *Visioner og anbefalinger til Danmark som et digitalt foregangsland*, s. 91.
28. Se mere om DATA for GOOD på <https://dataforgoodfoundation.org/>
29. Klima-, Energi- og Forsyningsministeriet, Transportministeriet, Erhvervsministeriet og Digitaliserings- og Ligestillingsministeriet (2024), *Danmark klar til automatisering – National plan for bevægelsesdata*.
30. Dansk Erhverv (2023), *Dansk Erhverv presser på for manglende udbetalinger fra bookingselskab*. Lokaliseret den 23. august 2024 på <https://www.danskerhverv.dk/presse-og-nyheder/nyheder/2023/september/dansk-erhverv-presser-pa-for-manglende-udbetalinger-fra-bookingselskab/>
31. OpenAI (2023), *OpenAI and Microsoft extend partnership*. Lokaliseret den 23. august 2024 på <https://openai.com/blog/openai-and-microsoft-extend-partnership>

32. Microsoft (2024), *Microsoft and Mistral AI announce new partnership to accelerate AI innovation and introduce Mistral Large first on Azure*. Lokaliseret den 23. august 2024 på <https://azure.microsoft.com/en-us/blog/microsoft-and-mistral-ai-announce-new-partnership-to-accelerate-ai-innovation-and-introduce-mistral-large-first-on-azure/>
33. The Stack (2023), *Meta to spend up to \$33 billion on AI, as Zuckerberg pledges open approach to LLMs*. Lokaliseret den 25. januar 2024 på <https://www.thestack.technology/meta-ai-investment/>
34. Draghi (2024) *The future of European competitiveness*. Lokaliseret den 2. november 2024 på https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en; Letta (2024) *Much more than a market*. Lokaliseret den 2. november 2024 på <https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf>
35. Digitaliseringspartnerskabet (2021), *Visioner og anbefalinger til Danmark som et digitalt foregangsland*, s. 102.
36. The Washington Post (2021), *Five points for anger, one for a 'like': How Facebook's formula fostered rage and misinformation*. Lokaliseret den 23. august 2024 på <https://www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm/>
37. Berlingske (2024), *En løgn spredt sig med rekord fart over hele verden. Men de unge elsker TikTok og vender de gamle medier ryggen*. Lokaliseret den 23. august 2024 på <https://www.berlingske.dk/kultur/en-loegn-spreder-sig-med-rekordfart-over-hele-verden-men-de-unge-elsker>
38. Mediawatch (2023), *Udenlandske selskaber tog større bid af dansk annoncemarked i 2022*. Lokaliseret den 23. august 2024 på <https://mediawatch.dk/Medienyt/Kommunikation/article15698631.ece>
39. Radar (2024), *Få overblikket: Sådan er kommunerne fanget i Microsofts systemer*. Lokaliseret den 23. august 2024 på <https://radar.dk/artikel/faa-overblikket-saadan-er-kommunerne-fanget-i-microsofts-systemer>
40. Center for Cybersikkerhed (2023), *CFCS' anbefaling vedrørende TikTok*. Lokaliseret den 23. august 2024 på <https://www.cfcs.dk/da/nyheder/2023/cfcs-anbefaling-tiktok/>
41. IT-Branchen (2023), *Fremtidens beskyttelse af det digitale Danmark*.
42. Se f.eks. Version2 (2016), *It-firma om offentligt kæmpe-udbud til skoler og børnehaver: De skaber et monopol*. Lokaliseret den 23. august 2024 på <https://www.version2.dk/artikel/it-firma-om-offentligt-kaempe-udbud-til-skoler-og-boernehaver-de-skaber-et-monopol>
43. Børne- og Undervisningsministeriet (2021), *Ny kortlægning: En velfungerende digital hverdag med plads til forbedring*. Lokaliseret den 23. august 2024 på <https://www.uvm.dk/aktuelt/nyheder/uvm/2021/maj/210517-ny-kortlaegning-en-velfungerende-digital-hverdag-med-plads-til-forbedring>
44. Christensen, Beuchert og Rasmussen (2022), *PISA 2022: Hovedrapport, VIVE – Det Nationale Forsknings- og Analysecenter for Velfærd*.
45. Cone og Lai (2024), *A day in the (datafied) life: Digital education platforms, commercial infrastructures, and the (im)possibilities of disconnection*, i *The Digital Backlash and the Paradoxes of Disconnection* / [ed] K. Albris, K. Fast, F. Karlsen, A. Kaun, S. Lomborg, & T. Syvertsen, Nordicom, Lokaliseret den 2. november 2024 på <https://norden.diva-portal.org/smash/record.jsf?pid=diva2%3A1896989&dsid=-1403>
46. Version2 (2024), *Googles skole-software koster det samme som en cheeseburger: Ekspertes er ikke i tvivl om hvorfor*. Lokaliseret den 23. august 2024 på <https://www.version2.dk/artikel/googles-skole-software-koster-det-samme-som-en-cheeseburger-ekspertes-er-ikke-i-tvivl-om-hvorfor>
47. DR (2024), *Danske forældre på jagt efter børnesandaler snydt af falske webshops*. Lokaliseret den 23. august 2024 på <https://www.dr.dk/nyheder/indland/danske-foraeldre-paa-jagt-efter-boernesandaler-snydt-af-falske-webshops>





Regeringens ekspertgruppe

TECH-GIGANTER