SAMFUNDS
TANKER

DET DIGITALE EUROPA

– Kunstig intelligens, konkurrence og rettigheder i lovmaskinen

DEO

DET DIGITALE EUROPA

– Kunstig intelligens, konkurrence og rettigheder i lovmaskinen

Redigeret af Rasmus Nørlem Sørensen

DEO

Tidligere udkommet i serien:
Samfundstanker 1: Hvad vil vi med bankerne?
Samfundstanker 2: Er fri bevægelighed EU's fremtid?
Samfundstanker 3: Sikkerhed i et åbent Europa
Samfundstanker 4: Kan EU redde klimaet?
Samfundstanker 5: Hvordan demokratiserer vi EU?
Samfundstanker 6: Hvem skal betale skat?
Samfundstanker 7: Kan EU skabe fred i verden?
Samfundstanker 8: Er der arbejde til alle i fremtidens EU?
Samfundstanker 9: Vælgerens håndbog i EU
Samfundstanker 10: EU-valgets ti store spørgsmål
Samfundstanker 11: Skal hele Balkan med i EU?
Samfundstanker 12: Har EU råd til fremtiden?
Samfundstanker 13: Kan EU sikre retsstaten?
Samfundstanker 14: EU's Green Deal
Samfundstanker 15: Hjælp dem i nærområderne?
Samfundstanker 16: EU: Sammen hver for sig?
Samfundstanker 17: 8 bud på EU's fremtid

Det digitale Europa

Kunstig intelligens, konkurrence og rettigheder i lovmaskienen

SAMFUNDSTANKER 18

Tekst:
Andrea Bang Christensen, projektmedarbejder, DEO
Rasmus Nørlem Sørensen, sekretariatsleder og chefanalytiker, DEO
Staffan Dahllöf, EU-journalist og researcher, DEO
Tina Mensel, projektleder og kommunikationsmedarbejder, DEO
Vibe Termansen, arrangementschef og senioranalytiker, DEO

Redaktør og ansvarshavende: Rasmus Nørlem Sørensen
Layout og tryk: Notat Grafisk
Udgiver: DEO med støtte fra Europa-nævnet EUROPA nævnet

September 2021

ISBN: 978-87-94125-10-9

INDHOLDSFORTEGNELSE

INDLEDNING:
DET DIGITALE SAMFUND

Kina leverer hardwaren, USA producerer softwaren, og EU byder ind med love og regler. Sådan kan den globale arbejdsdeling i den digitale udvikling de seneste par årtier groft skitseres. Det er i samme periode blevet mere og mere tydeligt, at det digitale ikke blot er et hjørne af økonomien eller en ubetydelig del af samfundet. Det digitale er en integreret del af virkeligheden.

En stor del af samfundsdebatten har i mange år foregået på sociale medier som Facebook og Twitter, men under pandemien er det derudover blevet normalt, at familierelationer holdes ved lige på Skype og boligforeningens bestyrelsesmøder foregår på Zoom eller Teams. Paratviden googler man sig frem til, og dybere viden tilegner man sig ved at høre podcasts eller se Youtube-videoer. Livet foran skærmen er ikke længere adskilt fra livet som sådan.

Økonomien er digitalt forankret i en sådan grad, at man kan komme i tvivl om, hvorvidt den helt har sluppet fortøjningerne til den fysiske verden. Finansverdenens handler har været digitale i årevis, de digitale penge har reelt fordrevet kontanterne fra forbrugernes lommer, men også i økonomien i bredere forstand vokser online-handel med tøj, dagligvarer, rejser, bøger og faktisk stort set alle varegrupper.

Den digitale virkelighed omfavner så mange dele af livet, at det står klart, at der er brug for at oversætte almindelig moral og etiske principper til det digitale liv. Men der er også brug for, at lovgivning og regulering følger med ind i den digitale virkelighed.

Hvordan beskytter man forbruger- og borgerrettigheder på nettet? Hvordan regulerer man tech-giganterne? Hvem må indsam-

le, opbevare og bruge al den data, som vores digitale færden genererer? Hvilke nye trusler findes der i den digitale verden?

Det er spørgsmål, som EU's digitale strategi forsøger at give svar på. Den går under navnet "Et Europa klar til den digitale tidsalder", og det er én af seks hovedprioriteter i EU-Kommissionen femårige arbejdsprogram. Den hovedansvarlige kommissær for området er danske Margrethe Vestager, der får assistance fra en hel stribe af de øvrige kommissærer, da de digitale spørgsmål berører alt fra handel over forbrugerrettigheder og til industripolitik.

I EU og medlemslandene er det lønlige håb, at det digitale tog ikke er kørt, og at det stadig er muligt for EU at opnå "teknologisk suverænitet". Det vil sige, at EU skal blive i stand til at konkurrere med Kina om industriproduktionen til den digitale virkelighed – eller som minimum kunne forsyne sine medlemslande med sikker, europæisk produceret infrastruktur for eksempel i form af 5G-netværk. Det indebærer også, at EU vil kæmpe for at gøre sig fri af de monopollignende, amerikanske tech-giganter, der i dag sidder tungt på platformene til nethandel og på de sociale medier.

I denne bog forsøger vi først at give svar på det grundlæggende spørgsmål: Hvad er det digitale Europa? Vi kigger nærmere på EU's regulering af det digitale område både før, nu og fremover. Herefter dykker vi ned i fem digitale temaer på områder, hvor der aktuelt bliver arbejdet på ny lovgivning eller ændringer af den eksisterende: Forbrugerbeskyttelse, kunstig intelligens, industripolitik, sikkerhedspolitik og censur af terrorrelateret indhold på nettet.

Bogens kapitler er forfattet af EU-journalist Staffan Dahllöf, arrangementschef og senioranalytiker Vibe Termansen, projektleder og kommunikationsmedarbejder Tina Mensel og projekt-

medarbejder Andrea Bang Christensen. Der er desuden et bidrag fra undertegnede, der også har redigeret den samlede bog. Tak til Fatme Chahrour for researchbidrag og Chris Lehmann for sparring og inspiration.

Rasmus Nørlem Sørensen, redaktør

DET DIGITALE EUROPA: VÆKST, KONKURRENCEEVNE OG FOLKELIG TILLID

Af Staffan Dahllöf

Det digitale årti kalder på fælles EU-lovgivning for alle slags net-tjenester. Udfordringen er at få skabt vækst gennem investeringer, uddannelse og nye tekniske løsninger. Men debatten om den nye lovgivning handler i lige så høj grad om afvejninger mellem det forbudte og det tilladte på det grænseløse net og om rækkevidden af fælles EU-lovgivning.

Lad os starte med et citat, der er lettere manipuleret:

"Kommissionen ser et behov for ensartede regler, hvis det indre marked skal fungere. Der er en risiko for, at enkelte medlemslande blokerer for udveksling af data over grænserne ved erhvervstransaktioner, toldbehandling, og lægebehandling, hvis man ikke kan stole på, at den personlige integritet beskyttes fuldt ud i andre lande," siger Alain Brun, embedsmand i Kommissionen.

Udsagnet er sådan set rigtigt nok. Alain Brun er ikke fejlciteret. Manipulationen ligger i nutidsformen "siger". For udtalelsen fra embedsmanden hr. Brun i Bruxelles faldt i 1994, for 27 år siden, i et interview med det svenske fagblad Journalisten. Han talte om et dengang aktuelt forslag til et databeskyttelsesdirektiv, en EU-lov som de færreste hæftede sig ved dengang, men som senere skulle blive genopfrisket, udbygget og kendt som GDPR – databeskyttelsesforordningen fra 2018. Den kan ingen EU-borgere i dag undgå at blive påvirket af eller støde hovedet imod.

Næsten alt det, som vi i dag kalder digitalt, var anderledes og nyt i 1994. Internettet var endnu ikke et etableret fænomen. Det

billedmæssigt mest spændende, som det nye World Wide Web kunne fremvise, var fotos af en kaffemaskine. Universitetet i Cambridge fik installeret verdens første net-opkoblede kamera i 1993 og interesserede kunne billede for billede se, hvordan kaffen dryppede ned i en glaskolbe et sted i Cambridge.

Men EU-Kommissionen var på banen. Ny teknologi var på vej og lovgivningen humpede efter. Hvis det indre marked skulle blive til noget, skulle der tages initiativ. Dén tilgang lever stadig i bedste velgående.

Digital selvstændighed

Det digitale område er i dag uendeligt meget større end i 1990'erne, men opgaven, som Kommissionen har stillet sig selv, kommer fra samme skuffe. Der skal banes vej for den bedst mulige udnyttelse af den eksisterende, men også den kommende, nye teknologi. Kommissionen, EU's daglige embedsmandsledelse, ønsker, at de 27 medlemslande får *"sikret sig en digital selvstændighed"* ved blandt andet en ensretning af lovgivningen om databehandling, fuldstændig som i 1994.

Et af seks prioriterede politikområder for den nuværende Kommission, der tiltrådte i 2019, bliver på lidt gumpetungt EU-dansk kaldt for "Et Europa klar til den digitale tidsalder", på engelsk "Fit for the Digital Decade". Kommissionsformanden, Ursula von der Leyen, noterede i sin opgavebeskrivelse til den danske kommissær, Margrethe Vestager, i december 2019:

"Din opgave er at sikre, at Europa fuldt ud udnytter potentialet i den digitale tidsalder og styrker sin industrielle og innovative kapacitet. Dette er en central del af indsatsen for at styrke vores førerposition på det teknologiske område og vores strategiske autonomi."

Margrethe Vestager har taget opgaven på sig, og hun har siden været rejsende i et flittigt gentaget, politisk budskab om behovet

for at finde en europæisk model for det digitale årti. EU skal ikke gå den statskontrollerede kinesiske vej, og heller ikke den amerikanske, hvor udviklingen er styret af de markedsdominerende og kapitalstærke IT-selskaber, bedre kendt som tech-giganterne. Ifølge den danske kommissær skal kendetegnet for den europæiske vej være en digitalisering, som sætter befolkningen i centrum.

En lang ønskeliste

Set fra Bruxelles er befolkningens adgang til og deltagelse i det digitale univers et demokratisk mål i sig selv, men også et middel til at opnå økonomisk vækst og en stærkere europæisk konkurrenceevne. Uden menneskers tillid til portaler, sociale platforme, onlinebutikker, kunstig intelligens og datahåndtering i det dele taget, så risikerer det teknisk mulige at blive en praktisk umulighed. Det er den samme logik, som fik Kommissionen at foreslå fælles regler for persondatabeskyttelse i 90'erne. Hvor fælles, tillidsskabende og problemfri databeskyttelsen dengang endte med at blive, er en anden historie.

Der er rigtig meget at komme efter. Udfordringerne strækker sig helt fra globale forhold til individuelle borgere. Fra til markedsandele til ligestilling. I dag forvaltes omkring 90 procent af EU's data af amerikanske virksomheder og kun 4 procent af de største onlineplatforme er europæiske. Kun en ud af seks specialister indenfor naturvidenskab, teknologi, og matematik er kvinder, ifølge tal, som Kommissionen mener, er alarmerende.

I en meddelelse fra marts 2021 ridsede Kommissionen op, hvad der konkret skal indhentes i det kommende årti. Det blev til en forholdsvis omfattende bestilling, måske kan man sige en ønskeseddel, henvendt til EU's institutioner, medlemslandenes regeringer, parlamenter, virksomheder og i sidste ende til os alle som EU-borgere.

Senest 2030 skal der i EU gerne være:

- 20 millioner **it-specialister** (i dag 7,8 millioner), med en balance mellem kvinder og mænd (i dag er 18 procent kvinder)
- **Netadgang** med gigabitdækning, 1.000 Megabit/sekund typisk gennem optiske fiber for alle europæiske husholdninger (i dag 59 procent), og **5G** dækning til alle befolkede områder (i dag 14 procent).
- Produktion af **halvledere** eller mikrochip svarende til mindst 20 procent af verdensproduktionen (i dag 10 procent)
- 10.000 klimaneutrale **edge-node** computere koblede til internettets hovedforbindelser for hver 100 km med ventetider for brugere på få millisekunder for at muliggøre det såkaldte "internet of things" (tingenes internet), hvor maskiner, sensorer, køretøjer, forsyningsinstallationer, husholdningsudstyr med videre kobles direkte på nettet. (findes ikke i dag.)
- En **kvantecomputer** i 2025 (eksisterer ikke i dag)
- **Cloud computing**, sky-tjenester som Dropbox, Onedrive, Google Drive, Document cloud og iCloud i brug af 75 procent af alle virksomheder (i dag 26 procent), ligesom behandling af **Big data** (store datamængder i dag brugt af 14 procent) og **AI,** kunstig intelligens (i dag brugt af 25 procent).
- **Databehandling** på et grundlæggende niveau i 90 procent af alle små og mellemstore virksomheder (i dag 60,6 procent).
- En fordobling af antallet "**enhjørninger**" – IT-virksomheder stiftet efter 1990 med en salgsværdi på over 1 milliard amerikanske dollar. (I dag findes 703 enhjørninger i USA, 206 i Kina og 122 i EU).
- 100 procent onlineadgang til centrale **offentlige tjenester** (i dag 75 procent) adgang for alle borgere til elektroniske **patientjournaler** (udbredelsen i dag er ukendt), brug af 80 procent **digitalt ID** for 80 procent af alle borgere (i dag 58 procent nationalt, 9 procent for tjenester over grænserne).

IT-brug kan Kommissionen kun påvirke indirekte, men man har om ikke andet lagt sig fast på at bruge beregningsmodellen kaldet DESI (Digital Economy and Society Index), så udviklingen kan følges og vurderes i forhold til målsætningerne.

Udbredelsen af teknisk udstyr som computere og netadgang er nem at måle, men visse dele af ambitionerne er vanskelige at indfri. Kvantecomputere og den ønskede edge-node computerteknologi er endnu ikke udviklet og kan derfor ikke blot bestilles hjem på Amazon.

Den udstyrsmæssige tilgang omfatter derfor også andre politikområder og generaldirektorater, end dem som Margrethe Vestager er hovedansvarlig for. Det gælder det syvårige forsknings- og udviklingsprogram Horizon Europe, under Mariya Gabriel fra Bulgarien, genopretningsplanen NextGenerationEU, 750 milliarder euro i bidrag og lån til økonomisk genstart, styret af Paolo Gentiloni fra Italien, og så EU-klassikeren det indre marked under den franske kommissær Thierry Breton. Det, som Margrethe Vestager ønsker sig, kan hun måske få hjælp med fra disse tre kolleger og deres budgetter.

Udvikling, forskning og markedsudvikling kan næppe styres fra toppen. Noget anderledes forholder det sig med love og retningslinjer, som må siges at være Kommissionens stærkeste disciplin. Lovgivning er EU-samarbejdets historiske kerneområde, og ønsket om at gøre EU til en digital supermagt skaber ikke store uenigheder blandt medlemslandene.

Nye lovforslag i EU

Under overskriften "Den digitale tidsalder" er der tre nye lovinitiativer, som er særligt vigtige. Der er en forordning om digitale markeder (DMA – Digital Markets Act), en forordning om digitale tjenester (DSA – Digital Services Act) og en forordning om regler for kunstig intelligens (Artificial Intelligence Act – regler

for kunstig intelligens). Forslagenes indhold diskuteres nærmere i de efterfølgende kapitler.

Forordninger er EU-love, som gælder i hele EU umiddelbart efter, at de er blevet vedtaget. De skal i modsætning til direktiver ikke implementeres gennem lovgivning i medlemslandene for at træde i kraft. Persondataforordningen GDPR fra 2018 er derfor mere stram, detaljeret og ensrettet end persondatadirektivet fra 1994.

De tre lovforslag har alle i varierende grad kontroversielle dele og følgevirkninger. Det kan ses på antallet af udvalg i EU-Parlamentet, som er blevet bedt om at komme med synspunkter. Udover det udvalg som er hovedansvarligt for, hvad Parlamentet skal mene, er der otte udvalg, der inddrages i forhandlingerne om forordningen om tjenesteydelser (DSA), syv i forhold til markedsreguleringen (DMA) og seks udvalg skal komme med indspark til forslaget om kunstig intelligens (AIA).

Konkurrencelovgivning
Markedsforordningens mål er at bryde de store net-virksomheders dominans. Google, Amazon og andre store udbydere af platformstjenester skal ikke længere fungere som gatekeepers (portvagter) med mulighed for at favorisere deres egne produkter og ydelser. Gatekeepers definereres i forslaget som virksomheder med omsætning i EU-området på 6,5 milliarder euro, der har mindst 45 millioner brugere hver måned eller 10.000 aktive erhvervskunder om året. Forslaget har foreløbigt fået en positiv modtagelse, men er langt fra vedtaget.

Forslaget til markedsforordningen får, hvis det bliver gennemført, i hovedsagen konsekvenser for de udpegede gatekeepers, og kun indirekte betydning for os alle som forbrugere eller erhvervsdrivende, hvis de store virksomheders monopolstilling med tiden bliver brudt.

Forbrugerbeskyttelse
Forslaget til forordningen om digitale tjenester får en hurtigere og mere umiddelbar betydning for mange flere mennesker.

For det første fordi, forslaget vil gøre det synligt, hvordan alle tjenesteydere målretter markedsføring af deres tjenester. Det skal stå klart, hvordan mit besøg på en hjemmeside om for eksempel byggematerialer straks udløser en bølge af reklamer for spånplader eller haveredskaber, når jeg går ind på helt andre sider. Den socialistiske gruppe i Parlamentet overvejer et direkte forbud mod den type af "mikro-markedsføring", altså reklamer baseret på den enkeltes net-trafik, som i dag er meget udbredt på tværs af næsten alle platforme.

For det andet vil forordningen få direkte effekt, fordi salg af produkter og tjenester, som er ulovlige eller på anden måde regulerede i fysiske forretninger, skal være lige så forbudte eller regulerede ved salg på nettet. Platforme, som formidler salg, kan blive ansvarlige for de produkter eller tjenester, de linker til.

For det tredje lægger lovforslaget op til, at der skal gælde de samme regler for opslag på Facebook, Twitter, Instagram, medieplatforme, og andre net-sider, uanset om de er slået op i Bulgarien eller Finland. Det vil i realiteten medføre en EU-harmoniseret ytringsfrihed online.

Det socialdemokratiske medlem af EU-Parlamentet, Christel Schaldemose, er ordfører eller i EU-sprog rapportør og dermed hovedansvarlig for Parlamentets kommende stillingtagen til forslaget. Hun skriver i en nøglesætning i sin betænkning, at: "*Ulovligt indhold bør så hurtigt som muligt fjernes fra formidlingstjenester, samtidig med at der tages højde for grundlæggende rettigheder.*"

Men hvad er ulovligt indhold, og hvad er kun skadeligt eller uønsket? Hvem definerer på EU-niveau, hvad der skal være til-

ladt? Det står endnu ikke klart i lovforslaget. En parallel speciallov om terrorrelateret indhold online, har dog taget stilling til nogle af disse spørgsmål, og er allerede vedtaget og trådt i kraft – se diskussionen heraf i kapitel 5.

Bliver ytringsfriheden truet?

Christel Schaldemose har selv påpeget, at EU's medlemslande af historiske grunde har meget forskellige opfattelser af, hvad der er tilladt at skrive og formidle. I Tyskland er det ulovligt at benægte de nazistiske folkemord, mens holocaustbenægtelse ikke er strafbart i Danmark. Ytringer om LGBT+ der er eller måske bliver strafbare i Ungarn, Polen eller Slovenien, er fuldt ud lovlige i Danmark. Ensartede regler for ytringer i EU's medlemslande findes ikke i dag, og en harmonisering kan derfor føre til en lavere fællesnævner for ytringsfriheden.

EU-Parlamentets udvalg for Borgernes Rettigheder og Retlige og Indre Anliggender, på EU-fransk forkortet LIBE, har i en foreløbig betænkning rettet 16 principielle indvendinger mod lovforslaget. Herunder at krav om at fjerne ulovligt indhold kun skal kunne rettes til den medlemsstat, hvor ytringen er lagt på nettet. LIBE vil også have, at kun domstole og ikke andre myndigheder skal træffe beslutninger om, hvad der er ulovligt, og hvad der ikke er.

En yderligere fare med lovforslaget er, ifølge rettighedsorganisationen EDRi (European Digital Rights), at det er uklart, hvilke online-tjenester der skal omfattes af den kommende lov. For eksempel ønsker Parlamentets retsudvalg (JURI), at loven udover sociale medier også skal dække besked- og opkaldstjenester som Messenger, WhatsApp og Signal.

En sådan "all inclusive-model" vil komme til at udviske grænserne mellem privat og offentlig kommunikation, og kræve adgang til al krypteret net-trafik. Hvis private beskeder skal over-

våges og analyseres for indhold i forhold til 27 medlemslandes lovgivning, vil det være det samme som at gøre postbudene skyldige i at åbne og læse alle breve og pakker, inden de afleveres. En praksis der kendes fra det tidligere Østtyskland, påpeger EDRi.

På den anden side vil venner af logik og retssikkerhed kunne spørge, hvorfor for eksempel beskedgrupper på WhatsApp og Signal skal kunne formidle indhold, som ikke må formidles på åbne net-sider. Og så er vi tilbage i den øvelse, som rapportøren Christel Schaldemose kalder for balancen mellem at fjerne indhold og tage højde for grundlæggende rettigheder.

For dansk vedkommende kan den øvelse blive aktuel om mindre end et års tid, selvom EU-forordningen nok ikke er færdigbehandlet til den tid. For regeringen vil komme EU-lovgivningen i forkøbet.

Kommer Danmark EU i forkøbet?
Danmarks Radio kunne den 11. august 2021 fortælle, at en kommende lov vil tvinge net-tjenester som Google og Facebook til at fjerne eller blokere klart ulovligt indhold indenfor 24 timer eller indenfor 7 dage, hvis der er tvivl om, hvorvidt indholdet er ulovligt. DR brugte et 15-årigt offer for hævnporno som eksempel, og i en kommentar gav SF's retsordfører udtryk for sin begejstring for forslaget. Forslaget var dog hverken omtalt på Erhvervsministeriets eller Justitsministeriets hjemmesider, da det først vil blive fremsat i februar næste år, oplyser Erhvervsministeriet.

Men DR havde fået en direkte besked fra ministeriet; en ikke helt usædvanlig praksis, når regeringen, men også de politiske partier, baner vejen for kommende forslag ved hjælp af målrettede henvendelser til i forvejen udvalgte medier.

Af det materiale som ministeriet gav DR, og som DEO efterfølgende har fået tilsendt, fremgår det ingen steder, at forslaget vil

komme til at overlappe den kommende EU-forordning, selvom forslag og problemstillinger nærmest er identiske.

Direktør for tænketanken Justitia, Jacob Mchangama, kommenterede DR-nyheden med, at det danske lovforslag kan komme til at skubbe ytringsfriheden i forkert retning, da det kan blive svært at vurdere, om indhold er ulovligt, indenfor 24 timer eller syv dage:

"I Danmark kan det tage et år, hvis domstolene skal afgøre, om noget eksempelvis er racisme. Der er en lang kategori af ytringer, der er ret komplicerede."

Uanset om Danmark kommer det øvrige EU i forkøbet er problemstillingen den samme i dag, som da EU-kommissionen banede vej for fælles persondataregler for 27 år siden. Det er en problemstilling, som illustrerer, hvordan EU som organisation balancerer mellem på den ene side at være en overstatslig union med bindende regler for alle og på den anden side at fungere som et samarbejde mellem selvstændige medlemslande.

Spørgsmålet er, hvordan man kan regulere den grænseoverskridende, digitale virkelighed og sikre de grundlæggende rettigheder med fælles love for 27 lande med 27 forskellige forfatninger og retstraditioner.

KAN EU HAMLE OP MED TECH-GIGANTERNE?

Af Andrea Bang Christensen og Rasmus Nørlem Sørensen

Sommeren 2021 har budt på en genåbning af samfundet og i Danmark også en del sol. Det har muligvis givet en midlertidig nedgang i antallet af timer tilbragt på internettet, hvor stort set hvert klik på en tast efterlader data. Samme sommer har også pustet nyt liv i EU's GDPR-forordning, som skal sikre, at disse data ikke misbruges. En lov som tech-branchen nok var begyndt at se som en papirtiger uden tænder.

I Luxembourg blev den europæiske lovgivning i juli brugt til at uddele en rekordstor bøde til e-handelsplatformen Amazon på ikke mindre end 746 millioner euro (5,5 milliarder kroner). På sommerens sidste dag uddelte de irske data-myndigheder en kæmpebøde på 225 millioner euro (1,7 milliarder kroner) til WhatsApp, der ejes af Facebook.

De to rekordstore bøder for brud på databeskyttelses-reglerne i EU kommer efter tre år med GDPR, der ellers kun har budt på en enkelt mellemstor bøde fra de franske myndigheder til Google på 50 millioner euro. Vel at mærke en enkelt bøde i en skov af grove overtrædelser af GDPR-reglerne, der især bliver begået af amerikanskbaserede giganter, som har baseret deres forretningsmodeller på aggressiv indsamling og analyse af brugernes data og herefter aggressiv markedsføring på dette grundlag.

Estelle Massé fra data-rettighedsorganisationen *Access Now* har udtalt til EU-mediet Politico.eu, at der er et par opløftende perspektiver i disse domme. Først og fremmest at det er lykkedes at få afgjort sager, der omfatter forhold i flere EU-lande på én gang. Det giver håb om, at datamyndighederne er i gang med at lære,

hvordan de kan håndtere lignende grænseoverskridende sager i fremtiden.

Men det er ifølge Estelle Massé også afgørende, at dommene er faldet i netop Luxembourg og Irland. De to lande fungerer som skattely for internationale firmaer, og mange af tech-giganterne placerer derfor deres europæiske hovedkvarterer her. Data-aktivister har frygtet, at Irland og Luxembourg ville være lige så tilbageholdende med at genere de multinationale selskaber i spørgsmål om data-brud som i sager om skattesnyd.

De to domme bliver formentlig anket, og en eventuel frifindelse på et senere tidspunkt kan ikke udelukkes på forhånd. Men afgørelserne viser, at der er vilje til at håndhæve GDPR-reglerne.

Cambridge Analytica

For 400 år siden konstaterede den engelske filosof, Francis Bacon, i et berømt citat, at "viden er magt". Bacon studerede og underviste på universitetet i Cambridge og fire århundreder og en digital revolution senere blev Cambridge igen forbundet med hans påstand.

EU's GDPR-forordning trådte i kraft i 2018 et halvt år efter, at offentligheden for alvor blev opmærksom på, hvor effektiv politisk markedsføring på baggrund af massiv dataindsamling kan være. Det skete med afsløringen af IT-markedsføringsfirmaet Cambridge Analyticas arbejdsmetoder. Cambridge Analytica indsamlede fra omkring 2010 brugerdata fra op imod 87 millioner Facebookbrugere uden at spørge dem om tilladelse eller gøre opmærksom på det. Datahøsten foregik gennem en app i Facebook, hvor man kunne quizze og svare på spørgsmål om sine personlige præferencer og interesser.

De mange høstede data brugte Cambridge Analytica til at lave detaljerede psykologiske profiler på brugergrupperne, der derefter blev brugt til at designe effektive politiske markedsfø-

ringskampagner for Trump-kampagnen i USA og for Vote Leave -kampagnen i Storbritannien. Lignende metoder blev anvendt (og bliver stadig anvendt) af en række andre virksomheder, men Cambridge Analytica tiltrak sig stor opmærksomhed, fordi de brugte deres store kunder og effekten af deres arbejde på de politiske begivenheder som salgsargument over for andre kunder.

Skandalen satte gang i det, der er blevet kaldt "The Great Privacy Awakening" (den store privatlivs-opvågning), der startede med Edward Snowdens afsløringer af den amerikanske efterretningstjeneste NSA's masseovervågning af borgere i 2013. De to skandaler rykkede bekymringen over borgerrettigheder på nettet fra nørdede forskere og IT-aktivisters lukkede diskussioner og ud i den brede offentlige debat.

Digitalt borgerskab

I EU's digitale strategi er det centralt, at borgerne er villige til at deltage og forbruge på nettet. De skal være digitale borgere i EU, som det i marts i år blev formuleret i en såkaldt meddelelse fra EU-Kommissionen til de lovgivende forsamlinger: Ministerrådet og EU-Parlamentet. Her fremgår det:

"Denne europæiske tilgang for det digitale samfund er også baseret på en fuld respekt for EU's grundlæggende rettigheder:

- Ytringsfrihed, herunder adgang til forskellige, pålidelige og gennemsigtige oplysninger
- Frihed til at oprette og drive egen virksomhed online
- Beskyttelse af personoplysninger og privatlivets fred og retten til at blive glemt
- Beskyttelse af enkeltpersoners egne intellektuelle frembringelser i onlinemiljøet."

De grundlæggende friheder og rettigheder skal sikres på tværs

af en lang række lovinitiativer. Nogle af dem er allerede trådt i kraft, andre er ved at blive implementeret i medlemslandene, og atter andre er foreløbigt kun på forslagsstadiet.

Et godt eksempel på tilgangen er Kommissionens forslag om at etablere en "digital wallet" (en digital pung), hvor kørekort, pas, uddannelsespapirer, boarding passes i lufthavnen og andre formelle dokumenter kan ligge online. Det skal være frivilligt, om den enkelte borger vil bruge tilbuddet, og det er op til medlemslandene at finde den specifikke løsning, de vil tilbyde.

Ligesom i de øvrige retsakter er der tale om et forslag med flere perspektiver. For det første er den digitale pung et led i digitaliseringen, der gerne skulle gøre livet nemmere for både borgere, virksomheder og myndigheder. For det andet er en digital pung et alternativ til lignende løsninger fra Apple, Google og andre tech-giganter, og dermed er der en mulighed for at fravælge private (og typisk amerikanske) løsninger og tilvælge en offentlig og europæisk model.

Forslaget skal overleve kritiske spørgsmål om sikkerhed mod hacking og identitetstyveri og sikkert også om brugervenlighed og muligheden for at bruge samme løsning i hele EU. Men 16 lande herunder Danmark har allerede digitale ID, der kan flere af de ting, forslaget lægger op til.

Moderne femkamp

Den teknologiske udvikling er altid et skridt foran lovgivningen. I forhold til beskyttelsen af brugere og borgeres rettigheder, ligner EU's arbejde måske mest af alt moderne femkamp, hvor kampen foregår i mange discipliner. Modstanderne er i denne sammenhæng først og fremmest store online-platforme som Facebook, Apple Store og Google Store.

Nøgleordet er platformsansvar. Udfordringen ligger til dels i, hvordan man skal forstå en platform. Facebook minder ikke rig-

tig om en gammeldags papiravis med ansvarshavende redaktører og journalister. Det minder heller ikke om læsesalen i et bibliotek, hvor aviserne kan læses. Facebook er heller ikke et klassisk reklamebureau, der indrykker annoncer og trykker plakater for kunderne. Platformen har heller ingen adresse i for eksempel Danmark, selvom den har masser af indholdsproduktion og indtægter i landet.

Det rejser nogle spørgsmål. Hvilket ansvar har platformene for at fjerne ulovligt indhold? Hvordan må platformene anvende de data, som de indsamler om brugerne? Hvordan sikres brugernes ytringsfrihed, hvis platformene fjerner det indhold, de har delt? Hvilke rettigheder til for eksempel royalties har producenterne af det indhold, der bliver delt på platformene?

Apples tiltag mod børneporno

I forslaget til det digitale tjeneste-direktiv lægges der op til, at platformene har ansvaret for at fjerne ulovligt indhold hurtigt og effektivt. Men det er ikke helt uproblematisk at overlade løsningen med at regulere uønsket eller skadeligt indhold til et privat firma. For eksempel har Apple for nyligt annonceret en plan for at modvirke misbrug af børn i den digitale sfære. Apple planlægger at bruge en overvågningsalgoritme til at finde seksualiseret indhold, for eksempel nøgenbilleder, som deles af børn under 18. Overvågningen skal omfatte alt fra internet-lagerplads i iCloud til børns private beskeder, der sendes med sms igennem iMessage.

Apple er som sådan helt på linje med EU-direktivet, der sigter på at skabe et sikkert digitalt liv for børn og andre sårbare digitale brugere. Apples tilgang har også fået opbakning fra EU-Parlamentet, der i juli måned stemte for et forslag om netop at give platforme lov til at overvåge deres brugeres indhold for at beskytte børn mod seksuelle krænkelser. Men det konkrete initiativ har også fået massiv kritik. 90 borgerrettigheds-organisatio-

ner har i et fælles brev opfordret Apple til at droppe ideen og EU til at trække sin opfordring tilbage.

"Lige så snart denne mulighed er bygget ind i Apple-produkter, vil dets konkurrenter stå over for et enormt pres – og potentielt også lovkrav – fra regeringer rundt om i verden, der gerne vil have fotos scannet ikke blot for børneporno, men også for andre billeder, som en regering finder problematiske," står der blandt andet i brevet.

Organisationerne er stærkt kritiske over for den form for algoritme, som Apple planlægger at bruge til at opspore seksuelt indhold af børn. Lignende algoritmer, der tidligere har været brugt af andre virksomheder, er ifølge brevet, notorisk upålidelige. Selve ideen med at overvåge brugerne, mener de også er problematisk. Den slags overvågningssoftware vil med sikkerhed indskrænke børnenes ret til privatliv og det, der i gamle dage blev kaldt brevhemmelighed, men det er usikkert om den rent faktisk vil være gavnlig for deres sikkerhed på nettet.

Endelig peger citatet på en risiko for, at overvågning for at forhindre deling af børneporno blot er et første skridt ud på en glidebane, hvor ytringsfriheden ender med at blive truet.

Google cookie-politik

GDPR-forordningen gjorde os alle opmærksomme på, at der er noget, der hedder cookies, og at de bruges af for eksempel Google til at spore vores adfærd og derefter til at målrette annoncer til os. Men forordningen fik faktisk også effekt på de store platformes dataindsamling. Apple ændrede allerede i 2019 sin standard webbrowser, Safari, der bruges af alle Apple-telefoner og iPads, så den ikke længere samlede data ind på vegne af "tredjepart". Det vil sige, at Apples firmakunder ikke længere kunne indsamle data om Apples brugere. Det var nok et fremskridt for databeskyttelsen, men ikke et stort tab for Apple, der tjener sine penge på telefoner og programmer. Ikke annoncer.

Google lever derimod stort set udelukkende af annonceindtægter, og derfor vakte det en del opsigt, da tech-giganten i 2020 annoncerede, at de også ville stoppe med at tillade tredjepartscookies. En vigtig del af forklaringen er, at GDPR-reglerne kræver, at brugeren accepterer tredjepartcookies én efter én for alle de tredjeparter Google sælger dataadgang til.

Googles måde at komme rundt om reglerne ser ud til at blive, at de skifter modellen for tracking eller sporing af brugerne. Det skal ikke længere være muligt for et firma at spore kunder, der bruger Google. De kan fremover kun spore kunderne, mens de er på firmaets egen hjemmeside. Men GDPR-reglerne forbyder i udgangspunktet ikke, at Google kan spore og indsamle data fra brugere, der er logget på Googles tjenester. Og der er det sådan, at alle, der har en Android-telefon, og alle, der bruger Google som standard-søgemaskine, stadig kan få høstet deres data. 70 procent af mobiltelefoner i EU er Android. Omkring 95 procent af internetbrugerne i EU bruger Google som søgemaskine.

Hvordan de data så kan videresælges af Google, og under hvilke betingelser? Det må nye lovinitiativer fra EU eller domme fra EU-domstolen afgøre.

Copyright-direktivet

Hvem har rettighederne til et musiknummer, der ligger på Youtube? Det er et spørgsmål, der viser en tredje måde, hvor EU lægger arm med platformene. I april 2019 vedtog EU-Parlamentet og Ministerrådet direktivet om ophavsret, også kaldet copyright-direktivet. Der er særligt to af direktivets artikler, der har givet anledning til debat.

Artikel 13 slår fast, at platforme skal sørge for, at copyright-beskyttet materiale ikke deles på deres platform – uden rettighedshaverens tillade. Der må ikke ligge en koncertoptagelse af David Bowies "Life on Mars", som en tilfældig bruger har uploadet på

YouTube. Der må ikke deles en avisartikel på Twitter. Det vil i praksis sige, at ingen sociale medier eller platforme kan fungere på den måde, de gør i dag. De skal finde en måde at tage indhold ned, der strider mod copyright-bestemmelserne, men der er indtil videre ikke nogen, der har fundet en nem metode til at finde og fjerne sådan indhold.

Artikel 11 omhandler en såkaldt link-skat, så man skal betale en afgift til for eksempel en avis, hvis man deler hele eller dele af en artikel, som avisen har ophavsretten til. Præcis hvor mange ord af en artikel, man må dele gratis, står endnu ikke helt klart. Det står også lidt uklart, hvem der er "man" i denne sammenhæng, for ikke-kommercielle delinger fra privatpersoner er undtaget. Men er en influencer med 10.000 følgere en privat eller kommerciel aktør?

Direktivet skulle have været implementeret i alle medlemslandes lovgivning i juni i år, men det er endnu ikke lykkedes i alle EU-lande. I Danmark er det stadig ikke lykkedes at implementere de to dele af direktivet. I marts foreslog daværende kulturminister Joy Mogensen indførelsen en link-skat som beskrevet i direktivet. Lovforslaget mødte massiv kritik fra medier, offentlighed og politiske partier og er endnu ikke vedtaget.

Det er langt fra første gang, et land er mislykkedes med at indføre link-skat. I 2014 forsøgte Spanien at indføre lovgivning, der skulle få Google til at betale for at linke til spanske nyhedssider. Google svarede igen ved at lukke ned for deres nyhedsapplikation Google News i hele landet. Tidligere i år lykkedes det dog Frankrig at gennemføre forhandlinger om en link-skat med Google med copyrightdirektivet i hånden. Direktivet fastslår nemlig, at Googles trussel om nedlukning af adgang til deres nyhedsmedier kan kategoriseres som misbrug af en monopollignende position, og det er ulovligt ifølge både fransk og europæisk lovgivning.

Man kan håbe, at digital kommissær, Margrethe Vestager, får ret i det, hun sagde i en tale for European Internet Forum i marts i år:

”Jeg er sikker på, at meget snart vil nye regler være på plads, der kan sikre, at vores demokratier og ikke blot en håndfuld store online-platforme tager de beslutninger, der afgør vores fremtid.”

MISTÆNKT SOM UDGANGSPUNKT

Af Vibe Termansen

Vi efterlader fodspor i form af data alle vegne. Et af de centrale spørgsmål i EU-lovgivningen på det digitale område er derfor, hvem der må gøre hvad med de oplysninger, men måske især hvordan kunstig intelligens må bruges til at analyse og overvåge de enorme mængder data.

"Ugyldighed" indenfor forvaltningsret betyder ifølge Den Store Danske Encyklopædi, at "en afgørelse ikke får de tilsigtede retlige virkninger; den gælder ikke, fordi den er retsstridig."

"Uanvendelig" betyder derimod blot, at den ikke kan bruges. Hvis det kun er dele af afgørelsen, der er uanvendelige, kan resten godt bruges. Hvis afgørelsen derimod er ugyldig, fordi den er retsstridig, er det det hele, der skal skrottes.

Og nej, det handler ikke om den store søndags kryds-og-tværs. Det handler om, hvorvidt dansk lovgivning eller EU-ret skal gælde, og om danske teleudbydere må gemme oplysninger om, hvem deres kunder ringer og sms'er til, samt hvilken mobilmast telefonen forbinder til på det tidspunkt – altså cirka hvor kunderne befinder sig henne imens. At gemme alle disse oplysninger kaldes "logning".

Det er mange oplysninger om mange mennesker. Som de danske regler er nu, skal teleselskaberne gemme dem et år tilbage i tiden, så de blandt andet kan udleveres til politiet i forbindelse med efterforskninger.

Fordelene er indlysende. Har en mistænkt ringet til sin bedstemor, sit bibliotek eller den rare pizzamand fra Hjørring 3 minutter og 47 sekunder efter at et mord er blevet begået i Sorø, skal politiet måske se sig om efter en anden mistænkt.

Ulemperne er lige så indlysende, mener for eksempel Foreningen imod Ulovlig Logning. Foreningen anlagde sag mod Justitsministeriet for år tilbage, efter at EU-Domstolen i den såkaldte Tele2-sag slog fast, at EU-retten er til hinder for en generel og vilkårlig logning af telekommunikationsdata, og at medlemsstaterne kun kan vedtage den slags lovgivning som forebyggende foranstaltning for *udvalgte personer* og alene med det formål at bekæmpe *grov kriminalitet*. Man må altså ikke give tilladelse til at logge diverse småkriminelle og naturligvis heller ikke alle de helt almindelige ikke-kriminelle.

EU-dom mod Danmark

EU-Domstolen fandt i Tele2/Watson-sagen i 2017, at både den svenske og den britiske lovgivning om logning var i strid med retten til privatliv og databeskyttelse, der begge er beskyttet af EU-chartret for grundlæggende rettigheder.

Daværende justitsminister i Danmark, Søren Pape Poulsen, anerkendte dengang, at også de danske regler skulle laves om til en mere målrettet logningsmodel, så det ikke var *alle* landets borgere, der var omfattet af overvågningen og dermed på forhånd – for en sikkerheds skyld – potentielt mistænkte.

De nye regler skulle på plads "hurtigst muligt". Imens ville man fortsætte som hidtil – de loggede oplysninger var nemlig ifølge Justitsministeriet meget vigtige for politi og anklagemyndighed, som Information beskriver det i en artikel den 30. juni 2021. Søren Pape Poulsen gik af som justitsminister i 2019, og Nick Hækkerup tog over, men "hurtigst muligt" kom aldrig.

Det var derfor en selvsikker talsperson for Foreningen imod Ulovlig Logning, der i juni i år mødte op ved Østre Landsret for at læse dommen. Men glæden varede kort – retssagen var tabt. Og nu er vi tilbage ved forskellen på "ugyldig" og "uanvendelig".

Justitsministeriet anerkender EU-rettens forrang (via EU-Dom-

stolens afgørelse) over dansk lovgivning. Men Justitsministeriets argument - som retten altså købte – lød, at der ikke er dansk retspraksis for at erklære en bekendtgørelse "ugyldig", hvis den strider mod EU-retten. I stedet skal de dele af bekendtgørelsen, der strider mod EU-retten, betragtes som "uanvendelige". Bekendtgørelsen om logning gælder altså stadig, dele af den kan bare ikke anvendes.

Desuden mente Justitsministeriet, at justitsminister Nick Hækkerup faktisk havde handlet "hurtigst muligt". Ikke med ny dansk lovgivning, men med et brev til teleselskaberne i januar 2021 hvor han skrev, at EU-dommene ikke betød, at "de gældende danske logningsregler sættes ud af kraft eller bliver umiddelbart ugyldige."

Ministeren anerkendte alligevel, at der var et problem, da han godt kunne se, at EU-Domstolen mente, at man kun måtte bruge loggede oplysninger i sager om grov kriminalitet og trusler mod statens sikkerhed.

Da de danske regler er meget bredere, og ikke lavet om endnu, mente ministeren, "at teleselskaberne, indtil vi har de nye logningsregler på plads, ikke vil kunne straffes, hvis de ikke følger reglerne om logning i logningsbekendtgørelsen."

Der er altså 1) en dom fra EU-Domstolen, som siger, at medlemsstaternes myndigheder kun må bruge loggede oplysninger i sager om grov kriminalitet og 2) en dansk lovgivning, der siger, at teleselskaberne skal logge *alle* deres kunder et år tilbage i tiden. Der er 3) en dansk minister, der beder de danske teleselskaber om at fortsætte med at logge, samtidig med at han 4) skriver, at de ikke kan straffes, hvis de lader være. Og endelig er der 5) en dansk domstol, Østre Landsret, der mener, at selvom de danske logningsregler er uanvendelige, er de ikke ugyldige.

Elementært, min kære Watson!

Overvågning med kunstig intelligens

Sagen om logning er kun en ud af flere meget omtalte sager i Danmark. For eksempel brugte Gladsaxe kommune i deres iver efter at opspore udsatte børn et system med kunstig intelligens (Artificial Intelligence, AI), hvis algoritmer diskriminerede personer af anden etnisk herkomst end dansk. AI var racistisk.

Intentionen var ellers god. Den såkaldte Gladsaxe-model skulle ved at samkøre data om børn og forældres adfærd og historie opdage udsatte børn tidligere, end mennesker kunne. De såkaldte risikoindikatorer var blandt andet, at børnene ikke kom til tandlægen eller sundhedsplejen samt forældrenes psykiske lidelser, arbejdsløshed eller skilsmisse.

Efter at over 20.000 borgeres fortrolige oplysninger var blevet lækket og flere tilfælde af ulovlig databehandling var blevet afsløret, blev projektet droppet.

Det er ikke kun i Danmark, der er udfordringer med masseovervågning.

En koalition af 12 menneskerettighedsgrupper har slået sig sammen i en europæisk bevægelse, Reclaim Your Face, der kræver et forbud mod de såkaldte biometriske genkendelsessystemer, der muliggør masseovervågning. På www.reclaimyourface.eu skriver de, at ansigtsgenkendelse kan og vil blive brugt mod os alle af regeringer og selskaber, på baggrund af hvem vi er, og hvordan vi ser ud.

Derefter linker de direkte til en side, hvor man kan skrive under på et europæisk borgerinitiativ, der opfordrer Kommissionen til strengt at regulere brugen af biometrisk teknologi for at undgå "unødig indblanding i de grundlæggende rettigheder."

Som begrundelse skriver de, at "der er evidens for, at biometrisk masseovervågning i medlemsstaterne og EU-agenturer har resulteret i overtrædelse af EU's databeskyttelseslovgivning og

unødigt begrænset folks rettigheder, herunder deres privatliv, ret til ytringsfrihed, ret til at protestere og til ikke at blive diskrimineret. Den udbredte anvendelse af biometrisk overvågning er en trussel mod retsstaten og vores grundlæggende rettigheder."

Det er specielt ansigtsgenkendelse, den mest almindelige form for biometrisk overvågning, der bekymrer bevægelsen, fordi den bliver udbredt med alarmerende hast over hele Europa i for eksempel skoler, stadioner, lufthavne og kasinoer. Den bliver brugt forebyggende for at pågribe kriminelle og under corona-krisen også til at håndhæve afstandsreglerne gennem apps og video-overvågning. I Tyskland, anfører bevægelsen, har politiet blandt andet brugt biometrisk masseovervågning til G20-demonstranter i Hamburg. For at have data nok at sammenligne med har ansigtsgenkendelsesfirmaet ClearviewAI ulovligt indsamlet og brugt billeder af folk, der bor i Tyskland, fra internettet.

Derudover kritiseres biometriske overvågningssystemer for ikke at være præcise nok, og for at de systemer, der skal forudsige følelser eller adfærd, mangler videnskabeligt grundlag.

Big Brother

Rettighedsorganisationen European Digital Rights, EDRI, advarer mod regeringer der, i et år med en verdensomspændende sundhedskrise, har begrænset folks bevægelses- og forsamlingsfrihed og mod private firmaer, der har udnyttet situationen til at samle mere biometrisk data om os. Vi ville aldrig, skriver organisationen, acceptere, hvis en person konstant fulgte, overvågede og vurderede, hvem vi er, hvad vi gør, og hvor vi bevæger os hen.

Ikke bare fordi vores adfærd automatisk ændrer sig, når man ved, man bliver overvåget, men også fordi vi risikerer at blive opfattet som en trussel, hvis en algoritme fejltolker en bevægelse

eller et ansigtsudtryk. Risikoen er, at man kan blive opfattet som en potentiel kriminel, alene på grund af sit tøjvalg, hudfarve eller fordi man deltager i en demonstration. Ydermere ved vi ikke, hvem der holder øje med os, hvorfor og hvor længe.

Den slags foregår for eksempel i Italien, hvor bystyret i Como med hjælp fra private firmaer som eksempelvis Huawei har installeret og i månedsvis testet et ansigtsgenkendelsessystem med meget lidt gennemsigtighed og uden gyldig lovhjemmel.

Og det foregår i Grækenland, hvor politiet ulovligt har gemt fingeraftryk af alle græske indehavere af et pas og har indgået en kontrakt om at udvikle software, så politiet kan bruge ansigts- og fingeraftryksgenkendelse ved almindelige politikontroller.

Smart, hvis politiet ved brug af dette ved en rutinekontrol kan fange en stor-kriminel. Ikke så smart, at alle andre dermed behandles som potentielt kriminelle – skyldige, indtil det modsatte er bevist.

Et europæisk borgerinitiativ kræver 1 million underskrifter. Derudover skal der være et bestemt minimumsantal underskrifter fra mindst syv EU-medlemsstater for at sikre, at borgerinitiativet kommer fra en bred vifte af lande. Minimumsantallet er baseret på antallet af MEP'er fra bemeldte medlemsstat.

I august 2021 nærmede det totale antal underskrifter på Reclaim Your Face's borgerinitiativ sig 60.000. Der er altså et stykke vej endnu, før Kommissionen behøver at skippe nattesøvn på grund af det.

Lovregulering eller selvregulering

Kommissionens udspil til at regulere AI, kunstig intelligens, kom i april i år. I perioden op til og lige efter udspillet, fra december 2019 til august 2021, har Kommissionen oplyst at have holdt 152 officielle lobby-møder om AI, ifølge en undersøgende artikel i EU-mediet EUObserver. Over 100 af de møder var med

industrien, den sidste tredjedel var fordelt mellem ngo'er, fagforeninger og forskningsverdenen. De fleste fik ét møde med EU. Google fik, med et solidt lobby-budget på 5.750.000 euro, hele ni møder.

Ikke overraskende viste dokumenter fra tech-firmaerne til EU, som EUObserver har set, et pres for mere AI i den offentlige sektor samt for mere selv-regulering, for eksempel med et krav om, at firmaer selv skal vurdere, om deres AI-produkter lever op til EU-standarderne, før de kommer på markedet. Den proces – at stole på firmaers påstande om at de handler etisk forsvarligt i stedet for politisk at kontrollere dem - kaldes af kritikere for "ethics-washing". Det handler ikke blot om det private marked, men i høj grad også om det offentlige område, da offentlige myndigheder sjældent selv har ressourcerne til at udvikle AI-systemer, men må købe løsninger fra private.

Forslag til nye regler

Forslaget til en forordning "om harmoniserede regler for kunstig intelligens (retsakten om kunstig intelligens) og om ændring af visse af Unionens lovgivningsmæssige retsakter" fylder 111 sider.

Først på side 46 står der, hvad der skal være forbudt. Forbuddene fylder en side og to linjer.

Omkring forslagets offentliggørelse var der en del opmærksomhed om Artikel 5, 1., c), nemlig:

"omsætning, ibrugtagning eller anvendelse af AI-systemer fra offentlige myndigheders side eller på deres vegne med henblik på evaluering eller klassificering af fysiske personers troværdighed over en given periode på grundlag af deres sociale adfærd eller kendte eller forudsagte personlige egenskaber eller personlighedstræk, således at den sociale bedømmelse fører til et eller begge følgende udfald:

i) skadelig eller ugunstig behandling af visse fysiske personer eller hele grupper heraf i sociale sammenhænge, som ikke har noget at gøre med de sammenhænge, i hvilke dataene oprindeligt blev genereret eller indsamlet

ii) skadelig eller ugunstig behandling af visse fysiske personer eller hele grupper heraf, som er uberettiget eller uforholdsmæssig i forhold til deres sociale adfærd eller alvorligheden heraf."

Det skal altså være forbudt for offentlige myndigheder at bruge AI til at klassificere fysiske personers troværdighed for at give dem "skadelig eller ugunstig behandling" i anden sammenhæng. Så langt, så godt.

Men på mange andre områder vil offentlig brug af AI stadig være tilladt, selv på områder, der er klassificeret som høj-risiko. Den eneste garanti for, at systemerne overholder andre EU-regler (om for eksempel gennemsigtighed, databeskyttelse og menneskerettigheder) er, at de private firmaer selv har vurderet, at deres høj-risiko-systemer overholder reglerne.

Det kræver tillid. Og netop det var ledende næstformand i Kommissionen med ansvar for at fastlægge en "strategisk retning for et Europa klar til den digitale tidsalder", Margrethe Vestager, inde på, da hun præsenterede forslaget:

"De juridiske rammer former den tillid vi skal opbygge, hvis vi gerne vil have folk og firmaer til at omfavne AI-løsninger." Hun fortalte, at hun er bekymret over den måde, folk opfatter AI og for eksempel frygtede, at bystyrer ikke ville tage risikoen ved at bruge AI til at hjælpe socialarbejdere med at finde de rette løsninger for sårbare borgere. "Det ville være en skam," mente Vestager.

Udkastet til en forordning om regulering af AI blev fulgt af løfter om at bruge 1 milliard euro om året på AI, og på at den offentlige sektor skal være dér, hvor AI bliver banebrydende.

TERROR TRUMFER BETÆNKELIGHEDER

Af Staffan Dahllöf

Mandagen den 7. juni 2021 trådte en ny EU-lov i kraft, der gør det ulovligt at tilskynde, hverve og oplære i terrorhandlinger på nettet. Oplæring, hvervning, tilskyndelse til, deltagelse i og finansiering af terror var ulovligt i forvejen, som de fleste nok kan forestille sig. Det nye er, at forbuddet nu også omfatter omtale af den slags på nettet. Loven hedder formelt "Forordning om håndtering af udbredelsen af terrorrelateret indhold online" og blev vedtaget af Parlamentet og Ministerrådet i april i år.

Terrorisme defineres ved en opremsning af en lang række gerninger som legemsangreb, massiv ødelæggelse, gidseltagning eller kapring af fly, hvis formålet er, *alvorligt at intimidere* en befolkning, *tvinge* en regering eller organisation at gøre noget, eller afstå fra at gøre noget, eller at alvorligt *destabilisere* et lands eller en organisations strukturer. De definitioner har været diskuteret i EU i mange år og blev endeligt vedtaget i et retligt bindende direktiv i 2017 om bekæmpelse af terrorisme.

Forbuddet mod terrorindhold online er henvendt til udbydere af tjenester på nettet, på EU-dansk kaldt hosting-tjeneste-udbydere. Det er firmaer, som sælger serverplads til virksomheder, medier, blogs og private hjemmesider. De skal indenfor en time fjerne terror-relateret indhold, hvis en myndighed i et EU-land beder om det. Det indebærer en retshåndhævelse over landegrænserne.

Hvis en polsk myndighed beder en dansk udbyder om at fjerne eller blokere terrorindhold på nettet, skal det gennemføres indenfor 60 minutter. Hvis det ikke sker, kan udbyderen straffes med bøder på op til 4 procent af virksomhedens omsætning.

Der er der en særlig krølle ved den danske håndhævelse. Den er der grund til at vende tilbage til.

Grænse med elastik i

I diskussionen om, hvad der skal være tilladt på nettet, var det i mange år en bred og udtalt politisk holdning, at man skulle fjerne og blokere så lidt indhold som muligt. Det første brud med det princip kom med forbuddet mod børnepornografi på nettet. Den svenske kommissær Cecilia Malmström var tilbage i 2010 ansvarlig for retlige og indre anliggender i EU-kommissionen.

Hun sagde dengang i et interview med magasinet NOTAT:
"Jeg bryder mig ikke om censur på nettet. Der er en masse illegal aktivitet, som man skal prøve på at stoppe ved kilden. Det arbejder politiet også på. Men hvad angår børnepornografi, så har det ikke noget med ytringsfrihed at gøre. Derfor er det en undtagelse."

Går grænsen dér, eller kan du også forestille dig blokering af hjemmesider, som opfordrer til terrorisme?

"Grænsen går dér. Jeg vil ikke foreslå blokering af andre hjemmesider i min mandatperiode."

Den udtalelse havde, ligesom Malmströms mandatperiode, en udløbsdato. Den er for længst overskreden. Grænsen gik ikke ved børnepornografi og heller ikke ved terrorisme. Forslaget til forordning om digitale tjenester (DSA), som diskuteres andetsteds i denne bog, går ud på, at alt som er strafbart i den analoge verden, også skal være strafbart på nettet. Det kan muligvis også komme til at gælde opslag, som kan defineres som skadelige, selvom de ikke er direkte ulovlige.

Bomber, halshugninger og massedrab

I den gradvise udviskning af grænserne for regulering har forbud mod terrorindhold kun mødt mindre bump på vejen. Det er til dels naturligt. Det er nok svært at finde særlig mange, der vil

forsvare, at man publicerer bombemanualer, halshugninger begået af Islamisk Stat eller streamer live-video fra terror-myrderier som i Christchurch i New Zealand 2019.

Der er ført principielle diskussioner om, hvem der skal have adgang til hvad, om hvem der er terrorist, og hvem der er frihedskæmper, og om det ikke er vigtigt at vide, hvordan for eksempel militante islamister ræsonnerer og agerer. De diskussioner er ført mellem i forvejen engagerede politikere og rettighedsorganisationer, men uden at forstyrre særligt mange andre og uden at sætte markante spor i den daglige nyhedsrapportering.

Den lave forbudstærskel, når det handler om terrorisme, har vist sig ved, hvor hurtigt og uproblematisk EU-forordningen blev vedtaget sammenlignet med anden EU-lovgivning. Forslaget blev fremsat i efteråret 2018 og vedtaget i foråret 2021, vel at mærke efter en pause og genstart grundet valget til EU-Parlamentet i 2019 og efter en række Corona-forsinkelser.

Der blev afholdt principielle diskussioner i Europa-Parlamentets udvalg og – formentlig – mellem repræsentanter for Parlamentet og Ministerrådet i de lukkede slutforhandlinger (triloger). Det er bare ikke til at vide for dem, som ikke deltog i forhandlingerne. EU-loven, som kriminaliserer terrorindhold på nettet, blev derefter vedtaget af medlemslandenes regeringer ved skriftlig procedure den 16. marts 2021 uden at ministrene hverken mødtes i virkeligheden eller online. Ingen stemte imod. EU-Parlamentet bakkede også op om den beslutning helt uden afstemning den 28. april.

Artiklen kunne slutte her. Gjort er gjort, der er ikke mere at diskutere. Men der er elementer i terrorforbuddet, som kan komme til at påvirke den omfattende og generelle regulering af nettet, som Kommissionen har foreslået i de tidligere omtalte nye forordninger om digitale markeder (DMA), digitale tjenesteydelser (DSA) og kunstig intelligens (AIA).

Med eller uden filter

På nogle områder blev loven om terrorindhold noget mindre vidtgående, end den kunne være blevet. Loven stiller blandt andet ikke krav om, at serviceudbydere skal installere filtre, som automatisk fjerner forbudt indhold, men de vil kunne installere upload-filtre på eget initiativ. De ansvarlige myndigheder skal indenfor 48 timer informere om, hvorfor et indhold er fjernet eller blokeret, og der skal være adgang til en klagemekanisme.

Dertil kommer, at loven ikke kommer til at gælde for indhold, som er koblet til undervisning, forskning, kunst, journalistik eller polemiske holdninger i den offentlige debat. Hvad der regnes for et acceptabelt formål, skal "*slås fast af en vurdering*". Hvem der skal foretage denne vurdering, og på hvilket grundlag, står der dog intet om i lovteksten.

Op til den endelige vedtagelse af forordningen opfordrede 68 medie- og rettighedsorganisationer - blandt dem danske IT-Politisk Forening, Reporters Without Borders, Amnesty International og Den Europæiske Journalistføderation - EU-Parlamentet at stemme nej til forslaget af tre grunde.

For det første fordi den korte tidsramme for at fjerne eller blokere indhold vil tilskynde brug af indholdsfilter på trods af, at det ikke er påkrævet. Automatisk filtrering har blandt andet vist sig ikke at kunne skelne mellem propaganda og satire, og det har desuden ført til, at dokumentation af vold og overgreb i krigszoner som Syrien og Yemen automatisk er blevet taget ned fra hjemmesider.

For det andet er der i loven ingen krav om, eller regler for, at der skal foretages en uafhængig juridisk vurdering af det indhold, som fjernes. For det tredje mener de, at det er problematisk, at medlemslandene får ret at udvide deres jurisdiktion (retsområde) til andre lande uden retslig prøvelse, og uden respekt for den enkelte borgers rettigheder i det land, hvor indholdet fjernes.

De 68 organisationer fremførte, at loven alvorligt truer ytringsfriheden, ødelægger retten til adgang til oplysninger, svækker retten til privatliv og bryder mod retsstatsprincipper. De vandt ikke gehør for den kritik, og reglerne om terrorindhold er nu trådt i kraft.

PET som mellemled?

På et område har der været et enkelt dansk pip. Ifølge Justitsministeriets fortolkning af dansk statsret har danske myndigheder enekompetence til myndighedsudøvelse. Det kaldes for det uskrevne grundlovsforbud. En tysk anklager eller bulgarsk myndighed kan derfor ikke uden videre beordre en dansk udbyder til at fjerne eller blokere et uønsket indhold. Hvad gør man så? Det har Jan E. Jørgensen fra Venstre og Søren Søndergaard fra Enhedslisten spurgt om i Folketingets Europaudvalg.

Svaret fra justitsminister Nick Hækkerup (S) på de tos gentagne samrådsspørgsmål har været, at Danmark har valgt at hægte en såkaldt ensidig erklæring til Ministerrådets vedtagelse. I den erklæring står, at når en dansk udbyder får et påbud om at fjerne indhold fra et andet medlemsland, *"vil den danske myndighed underrette den danske udbyder om påbuddets retslige virkning i Danmark*."

Justitsministeriet forklarer i en skriftlig kommentar, at det uskrevne grundlovsforbud på denne måde undgås ved at indsætte en dansk myndighed som afsender af påbuddet:

"Denne ordning vil indebære, at det i praksis kan sikres, at reglerne i forordningen om fjernelse af terrorrelateret indhold inden for en time overholdes inden for rammerne af dansk ret, herunder det uskrevne grundlovsforbud."

Ministeriet understreger videre: "Påbuddet vil som følge af det uskrevne grundlovsforbud formelt først være bindende i Danmark, når det er videresendt fra en dansk myndighed. Påbuddet

vil dog allerede, når det kommer frem til den danske hosting-tjenesteudbyder, være bindende i alle andre medlemsstater."

Regeringen og det danske Folketing accepterer dermed, at udenlandske myndigheder kan fjerne terrorindhold på danske hjemmesider, hvis blot danske myndigheder fungerer som mellemled.

CYBERTRUSLER, KRIMINALITET OG DIGITAL SIKKERHED

Af Tina Mensel

Vores samfund er i stigende grad afhængigt af internettet og af digitale informationssystemer for at kunne fungere. Kritiske sektorer som transport, energi, sundhed og finansverden bliver stadig mere afhængige af digitale løsninger for at kunne udføre deres kerneaktiviteter. Digitaliseringen gør måske nogle ting nemmere, men skaber også en større risiko for hacking og cyberangreb, der kan få meget store konsekvenser.

Mere end en million mennesker bliver berørt af cyberkriminalitet hver dag og det koster den globale økonomi mere end 400 mia. dollars om året. Det er alle, fra enkeltpersoner til virksomheder og offentlige myndigheder, der kan blive ofre for svindel, identitetstyveri, falske bankhjemmesider eller industrispionage.

Under Covid-19-pandemien er antallet af hackerangreb for eksempel steget med over 4000 pct. i hele verden, hvilket svarer til et succesfuldt angreb hvert 39. sekund. I Danmark bliver danske myndigheder, virksomheder og borgere udsat for cyberangreb eller forsøg på angreb fra hackere, der forsøger at stjæle forskningsresultater, forretningsplaner og innovative idéer hver eneste dag.

Derfor står cybersikkerhed også højt på dagsordenen hos organisationer, virksomheder og myndigheder i alle EU's medlemslande. EU har en vedtaget strategi mod cyberangreb, der går ud på at skabe en "robusthed" (resiliens) til at modstå angreb på de fire centrale, digitale områder: Det indre marked, forsvaret, diplomatiet og ordensmagten.

Kinesere i 5G-netværket

En af de helt store debatter de seneste år har handlet om, hvilke netværksvirksomheder der skal have lov til at udbygge medlemslandes teleinfrastruktur. Alle lande og de nationale teleselskaber, har hver haft deres overvejelser om, hvilken udbyder de ville bruge til at udrulle 5G-netværket.

En af de virksomheder som har budt ind på at udrulle 5G-netværk i verdens lande er den kinesiske netværks- og mobilgigant Huawei, som nåede at indgå aftaler med flere EU-lande før den kinesiske løsning kom i kraftig modvind. Vinden kom fra USA, hvor den amerikanske regering i 2020 advarede alle sine allierede mod at indgå aftaler med Huawei af cybersikkerhedsmæssige årsager. Anklagen lød på, at Huawei arbejder for tæt sammen med den kinesiske regering, der vil kunne få adgang til alle slags data, når de først er inde i teleinfrastrukturen. Det kan for eksempel omfatte sundhedsoplysninger, bankoptegnelser, indlæg på sociale medier og i det hele taget bare alle oplysninger om enkelte borgere.

Canada, Tyskland og en række andre lande har fået meget håndfaste advarsler om, at USA ikke vil fortsætte det tætte samarbejde med landenes efterretningstjenester, hvis de tillader, at Huawei stiller nye mobilmaster i forbindelse med overgangen til 5G-netværk. Flere EU-lande har på den baggrund skrinlagt deres aftale med Huawei og i stedet indgået aftale med svenske Ericsson som leverandør af teleselskabernes kommende 5G-netværk.

EU-Kommissionen har indtil videre ikke forholdt sig lige så stringent til Huawei, som USA ellers har opfordret til, og har ikke nedlagt et forbud mod, at EU-lande kan benytte Huawei i deres udrulning af 5G-netværk. I stedet har EU's tilgang til Huawei været at se på, hvordan man kan håndtere de sikkerhedsmæssige risici. EU har med input fra medlemslandene lavet en værktøjskasse og en risikovurderingsrapport for cybersikkerhed i 5G-netværk.

Selvom dokumenterne ikke direkte nævner Huawei, så står det meget klart, at en af de største sikkerhedsrisici ved 5G-udrulningen er mulig indblanding af tredjestater, som især er sandsynlig, hvis 5G-leverandøren har stærke forbindelser til regeringen, eller hvis regeringen er i stand til at udøve nogen form for pres på leverandøren. Og i betragtning af at den kinesiske nationale efterretningslov pålægger kinesiske virksomheder at samarbejde med den nationale efterretningstjeneste, er der i EU's dokumenter klare referencer til Huawei.

Spredt fægtning i EU

Uden en fælles EU-politik på området, har medlemslandene valgt ret forskellige tilgange til den kinesiske telegigant. I Tyskland valgte man at give grønt lys til Huaweis deltagelse i det tyske 5G-netværk efter forsigtige overvejelser om, hvorvidt en fravælgelse af Huawei ville skade handelsrelationerne og særligt bilproducenternes adgang til det kinesiske marked. I stedet for et forbud mod Huawei har Tyskland skærpet de generelle sikkerhedskrav til netværksleverandører og gjort det muligt at nedlægge veto mod indkøb fra upålidelige leverandører og har dermed i høj grad fuldt EU's vejledninger. Så selvom loven ikke i sig selv udpeger Huawei direkte, så står budskabet med at virksomheder, der er i kontrol af autoritære stater, anses for at være upålidelige, klokkeklart.

Flere EU-lande er fulgt efter USA med at fravælge Huawei, og det er i høj grad de skandinaviske og østeuropæiske lande, der har taget mest afstand til Huawei. I Sverige har man lavet et forbud mod at bruge Huawei i 5G-udrulningen efter krav fra forsvaret og har givet teleselskaber besked på at fjerne alt mobiludstyr fra kinesiske producenter fra infrastrukturen inden 2025 og i Danmark har man fulgt en lignende vej.

Slovenien, Polen, Tjekkiet, Rumænien, Estland, Letland, Slovakiet og Bulgarien underskrev en aftale med den daværende

Trump-administration om at lukke Huawei ude af deres 5G-udrulning. Lande som Tyskland og Frankrig forbyder ikke direkte Huawei, men besværliggør deres adgang til deres telesektorer. Andre lande har haft en blødere tilgang til Huawei og deres 5G-udrulning, hvor de ikke har haft specifikke love til at forbyde Huaweis deltagelse i 5G-udrulningen, men i stedet lagt vægt på, at man kan fravælge 5G-udstyr, hvis man tænker, at det kan være en trussel for den nationale sikkerhed i landet.

Dermed har flere lande i EU valgt at sætte den kinesiske mobilgigant Huawei på porten og overlade 5G-udrulningen i deres lande til Nokia og Ericsson. Ifølge en rapport fra den danske teleanalysevirksomhed Strand Consult i 2020 var Belgien sammen med Cypern og Færøerne de eneste i Europa, hvor samtlige teleselskaber brugte Huawei eller ZTE (også en kinesisk IT-virksomhed) som leverandører af selve maste- og antennenettet.

Forbud mod og forhindringer af Huaweis indtog i Europa er ikke blevet vel modtaget i Kina, der har truet flere lande i spillet om de store netværkskontrakter. Forud for TDC's forhandlinger med Huawei om etableringen af 5G-netværket fik daværende statsminister Lars Løkke Rasmussen i 2019 besked om, at andre kinesiske virksomheders lyst til at investere i Danmark ville blive alvorligt påvirket, hvis Huawei skulle støde ind i problemer i Danmark. Og i december 2019 lød det i en lækket optagelse mellem den kinesiske ambassadør i Danmark, Feng Tie, og den færøske lagmand, Bárður á Steig Nielsen, at det ville få alvorlige konsekvenser for Færøernes handel med Kina, hvis Færøerne fravalgte Huawei.

Der har været kritik mod forbuddet mod Huawei fra flere kanter, blandt andet fordi der ikke har været konkrete beviser på, at Huawei ville udgøre nogen sikkerhedstrussel mod landene. Men med eller uden håndfaste beviser, mener man stadig, at der er grund til at være bekymret for Kinas intentioner i cyberspace og Huaweis indtog i Europa og verden.

USA aflytter toppolitikere

I 2014 igangsatte daværende chef for Forsvarets Efterretningstjeneste (FE), Thomas Ahrenkiel, *Operation Dunhammer*, der frem til 2015 undersøgte om den amerikanske Efterretningstjeneste (NSA) havde misbrugt et samarbejde med FE om at tappe data fra danske internetkabler til at aflytte toppolitikere i Danmarks nabolande. En sag, der i august 2020 sendte rystelser gennem FE og Forsvarsministeriet og som førte til hjemsendelsen af FE's ledelse. Operationen blev udført af en gruppe IT-eksperter og analytikere fra FE, der i al hemmelighed skulle analysere, hvem NSA spionerede mod gennem det dansk-amerikanske samarbejde.

Den rapport og de efterretningsdata, som ligger til grund for Operation Dunhammer, afslørede, at USA udnyttede samarbejdet med FE til aflytning af danske internetkabler til at spionere mod statsledere, toppolitikere og højtplacerede embedsmænd i Tyskland, Sverige, Norge og Frankrig. På den måde har NSA målrettet indhentet data gennem det dansk-amerikanske samarbejde.

Den hemmelige, interne arbejdsgruppe i FE afslørede blandt andet, at NSA har brugt de pågældende politikeres og embedsmænds telefonnumre som såkaldte selektorer. Det vil sige, at NSA har brugt telefonnumrene som søgeparametre for at trække politikernes, embedsmændenes og statsledernes kommunikation ud af de omfangsrige datastrømme, der løber gennem internetkabler til og fra Danmark. NSA fik dermed alt lige fra sms-beskeder til telefonopkald, der passerede gennem kablerne på vej til og fra politikernes og embedsmændenes telefoner.

Lovligt men pinligt

Tysklands forbundskansler Angela Merkel, den daværende tyske udenrigsminister Frank-Walter Steinmeier, og den daværende oppositionsleder Peer Steinbrück, er blot et udpluk af flere nav-

ne i Danmarks nabolande, som NSA har brugt det dansk-amerikanske samarbejde til at spionere mod.

Det er ikke ulovligt for FE at hjælpe en samarbejdspartner med at spionere mod andre lande. Men det er politisk betændt, at FE tilsyneladende har givet NSA adgang til at spionere mod politikere i vores nabolande ved at aflytte kabler ind og ud af Danmark. I Sverige og Norge har man også udtrykt, at situationen har været et dybt, alvorligt og urovækkende tillidsbrud.

I Tyskland derimod var forbundsmedlemmet Patrick Sensburg fra CDU ikke helt så overrasket, da han var formand for en undersøgelseskommission, der undersøgte udenlandske efterretningstjenesters aflytning i Tyskland fra 2014 til 2017 og han betegner det som gængs praksis, at selv EU-lande spionerer mod hinanden. Det spørgsmål der rejser sig, er så hvor bevidst det er sket.

Dunhammer-operationen blev planlagt helt tilbage i 2013, hvor den amerikanske whistleblower Edward Snowden lækkede dokumenter om NSA's arbejdsmetoder, herunder en global masseovervågning, hvor de havde spioneret mod folkevalgte ledere i allierede lande, blandt andet gennem samarbejder med de allierede landes efterretningstjenester.

Cybersikkerhed i EU

Antallet af cyberangreb mod europæiske virksomheder og myndigheder stiger fortsat og angrebene bliver stadig mere sofistikerede. Militært forsvar og sikkerhedspolitik er primært medlemslandenes kompetence og det gælder også cybersikkerhed. Derfor er der kun et enkelt EU-direktiv på området og ellers de mindre forpligtende tiltag som rådskonklusioner, handleplaner, strategier og koordinering.

Direktivet om sikkerhed for net- og informationssystemer (NIS) blev indført i 2016 som det første EU-direktiv om cybersikker-

hed nogensinde. NIS har til formål at harmonisere love om cybersikkerhed i hele Europa og forbedre samarbejdet mellem EU-landene. I december 2020 foreslog Europa-Kommissionen et revideret NIS-direktiv til at erstatte direktivet fra 2016 som en reaktion på det nye trusselsbillede og vores samfunds digitale transformation, som er blevet fremskyndet på covid-19-krisen. Forslaget er lige nu i behandling i Rådet. Det pålægger blandt andet medlemslandene at have en relevant cyber-sikkerhedsautoritet på plads, og at de med det samme udveksler relevante informationer om trusler og angreb med de øvrige EU-lande.

EU har derudover taget en række tiltag på området. I december 2020 fremlagde Europa-Kommissionen og Tjenesten for EU's Optræden Udadtil (EU-Udenrigstjenesten) blandt andet en ny strategi for cybersikkerhed i EU. Strategien indeholder EU's indsats for at beskytte sine borgere og virksomheder mod cybertrusler, fremme sikre informationssystemer og beskytte et globalt, åbent, frit og sikkert cyberspace.

Den 22. marts 2021 vedtog Rådet konklusioner om strategien for cybersikkerhed, hvor centrale mål som at opnå strategisk autonomi og samtidig bevare en åben økonomi var helt central. Under indsatsområderne i de kommende år fremhæver Rådet i sine konklusioner blandt andet planerne om at oprette et netværk af sikkerhedscentre i hele EU samt en fælles cyberenhed, der skal sætte klart fokus på EU's ramme for håndtering af cybersikkerhedstrusler, og en EU's 5G-værktøjskasse, der skal garantere 5G-nettets sikkerhed og en styrkelse af samarbejdet med internationale organisationer og partnerlande for at fremme en fælles forståelse af trusselsbilledet.

Derudover fastlagde Rådet tilbage i maj 2019 en ramme, så EU kan indføre målrettede sanktioner for at afskrække fra og reagere på cyberangreb, der udgør en ekstern trussel mod EU eller EU-medlemslandene. Denne ramme giver for første gang EU

mulighed for at indføre sanktioner mod personer eller enheder, der er ansvarlige for cyberangreb eller forsøg på samme, yder finansiel, teknisk eller materiel støtte til cyberangreb, eller på anden vis er involveret. Sanktionerne omfatter forbud mod indrejse i EU for personer og en indefrysning af aktiver for personer og enheder. De første sanktioner blev anvendt mod "seks personer og tre enheder", som der står i en pressemeddelelse fra Rådet den 30. juli 2020.

Cybersikkerhed er en af EU's prioriteter i forbindelse med den milliardstore genopretningspakke. I maj 2020 gav EU blandt andet tilsagn om, at 49 mio. euro herfra skal bruges til at fremme innovation inden for cybersikkerhed og systemer til beskyttelse af privatlivet. EU har ydermere forpligtet sig til at investere 1,6 mia. euro i cybersikkerhedskapacitet og en bred udrulning af cybersikkerhedsinfrastrukturer og værktøjer i hele EU til offentlige forvaltninger, virksomheder og borgere inden for rammerne af programmet for et digitalt Europa for perioden 2021-2027.

DIGITAL INDUSTRI: EUROPA LØBER MARATON I HJEMMESKO

Af Rasmus Nørlem Sørensen

"Vi er trådt ind i et globalt kapløb, hvor det at beherske teknologier er helt centralt. Det er først og fremmest ved at udvikle banebrydende teknologier, at Europa kan blive i stand til at påbegynde sin dobbelte grønne og digitale transition, mens vi fortsat garanterer modstandsdygtighed og autonomi."

Sådan sagde EU's franske kommissær, Thierry Breton, i juli i år i en tale på Menéndez Pelayo International University.

At Breton som kommissær for det indre marked blander sig i den digitale kommissær, Margrethe Vestagers, ressortområde er helt naturligt, for EU's digitale strategi handler i høj grad også om industripolitik, vækst og fremtidige indtægtsmuligheder. EU er i dag ikke meget andet end et marked for handel med hardware fra Kina og software fra USA. Kommissærens ambition er, at EU skal være førende på en række nye teknologier, hvis det dødvande skal brydes.

Det er også oplagt, at Breton som franskmand slår til lyd for, at EU skal opnå strategisk og teknologisk suverænitet, for det har altid været grundholdningen i Frankrig, at EU skal fokusere meget mere på at varetage egne økonomiske interesser. Det vil konkret sige, at EU skal være villig til at lave store offentlige investeringer i europæisk drevet forskning og udvikling. De skal følges op med det, der for få år siden, hvor Storbritannien var med i EU, ville have været stort set umuligt: Protektionisme og favorisering af europæiske virksomheder.

Opgør om industri-strategi

EU-samarbejdet er født ud af drømmen om frihandel og fri bevægelighed. Ikke blot indenfor grænserne af det indre marked, men i hele verden. Tankegangen har siden Kul- og Stålunionen været, at det frie, globale marked er en ubetinget fordel for alle og dermed også for de europæiske lande. Med Storbritannien som et toneangivende medlem, der fik støtte af Danmark og resten af Nordeuropa Tyskland inklusive, var det i mange år ikke muligt for den franske tilgang at slå igennem. I dag ser vi en bevægelse væk fra den naive markedsoptimisme, selvom det er med små, langsomme skridt.

Det sker blandt andet fordi franskmændene, der i økonomiske og handelspolitiske spørgsmål som regel har de sydeuropæiske lande i ryggen, har fået mere spillerum i EU efter brexit. De er ikke længere alene om ambitionerne om et EU, der har militær, strategisk, teknologisk og i dag også digital suverænitet. Tyskerne er kommet helhjertet med på den vogn, og de fleste andre EU-lande kan også godt se, at der er et behov for at gentænke EU's placering i verden.

For det første fordi grundfornemmelsen af, at hvad der er godt for verden, også er godt for Europa, har lidt et knæk. Den konkurrence, man ser fra især Kina i dag, har fået EU-toppen til at bekymre sig om, at Europa er ved at blive marginaliseret i verden og særligt i verdenshandlen. Hvordan får man vendt dén udvikling i en situation, hvor europæerne er nede på at udgøre seks procent af verdens befolkning og EU's skrumpende andel af verdensøkonomien i dag udgør omkring 15 procent?

For det andet har de flaskehalse, der har vist sig i mikrochip-industrien de sidste par år, afsløret at et EU, der er afhængigt af leverance-kæder over hele verden, også er sårbart over for kriser. Her er kommissær Bretons ønske, at EU skal finde en model for at beskytte egne markeder og forsyningskæder uden at lukke sig af mod verden.

For det tredje har corona-pandemien demonstreret, at det ikke er lige meget, hvem der kontrollerer produktionen af livsnødvendigheder. Medicinsk udstyr som ansigtsmasker blev pludselig en slags strategisk ressource, men også andre ressourcer til at klare krisen blev pludselig politiske og ikke kun handelsmæssige spørgsmål. Det understreges blot af det længevarende globale kapløb om sjældne jordarter og særlige metaller til produktion af batterier, elektronik, vindmøllekomponenter etc. Her har Kina i høj grad formået at sætte sig på de strategiske ressourcer. Europa halter efter med en naturlig fattigdom på eget territorium på disse råstoffer.

Endelig er der i de europæiske hovedstæder en stigende bekymring for, om man kan regne USA som en stabil og varig allieret. Trump-æraen satte for alvor panderynker i ansigtet på regeringslederne, men Biden-administrationen har langt fra entydigt glattet bekymringssporene ud.

Små hjul kan vælte store læs

Der sidder mikrochips og såkaldte halvledere i rigtig mange produkter i dag. Igennem de sidste par år har der været store forsinkelser på produktionen af varer som biler, computere og telefoner, fordi der er en flaskehals i produktionsleddet. Problemet skyldes tre forhold: En kraftigt stigende efterspørgsel på mikrochips, enorme investeringsbehov hvis ny produktion skal opstartes og endelig et nærmonopol på de mest avancerede halvledere.

Næsten hele verden er afhængig af én enkelt producent af de mest avancerede mikrochips. Det taiwanesiske TSMC (Taiwan Semiconductor Manufactoring Company) står for omkring halvdelen af verdensproduktionen i den specifikke niche. Og deres produktion har simpelthen ikke kunnet følge med den stigende efterspørgslen.

Det er enormt dyrt og tidskrævende at få gang i en udvikling og produktion, der kan matche TSMC. Et billede på udfordringen er, at Europas førende halvlederproducent Intel i Irland arbejder med produktionsprocesser med en præcision på 20 nanometer. TSMC arbejder med processer ned til 3 nanometer, der giver mulighed for at lave mikrochips, der er langt kraftigere, hurtigere, mindre og bruger mindre energi. Egenskaber der er i høj kurs hos kunderne i teknologibranchen.

Tid er tid og penge er penge

EU-landene stod for 30 år siden for omkring 35 procent af verdensproduktionen af halvleder-chips, men er i dag nede på under 9 procent. Den udvikling forsøger EU gennem erhvervs- og forskningsstøtte at vende. Helt aktuelt har den tyske regering meldt ud, at den blandt andet med EU-midler som finansiering vil skyde 3 milliarder euro (mere end 22 milliarder kroner) ind i at generhverve kontrollen med alle produktionsled i forsyningskæden og derudover tiltrække 2-3 gange det offentlige støttebeløb i private investeringer. Målet er, at tyske producenter kan levere processer ned til 2 nanometer og dermed effektivt konkurrere med de asiatiske producenter.

Det er et åbent spørgsmål, om det er muligt for EU-landene på kort sigt at stige på udviklingstoget. Det er ikke let, for det tog kører allerede i meget høj fart. Chip-producenten TSMC i Taiwan har siden slutningen af 1980'erne satset benhårdt på at blive den førende producent af mikrochips i verden, og deres succes kan blive svær at kopiere.

De tyske forsøg i genren er oppe mod mere end 40 års erfaring, avancerede produktionsanlæg på 160.000 m2 (32 fodboldbaner eller en mindre dansk provinsby), investeringer på tocifrede milliardbeløb og opbygning af et ekspertmiljø og teknisk ekspertise. At det er en svær konkurrencesituation, viser det fler-

årige forløb med mangel på microchips også. Hvis det var let at starte en konkurrerende produktion, var det nok allerede sket.

De nærmeste konkurrenter til TSMC er fra Kina. Det betyder også, at verdensmarkedet er afhængigt af en produktion i Kina og en produktion i Taiwan, som Kina for øvrigt mener, rettelig er en del af Kina.

Europæisk kvantecomputer

Kvantecomputere er ikke længere kun en våd fysiker-drøm. Det er en mulig nyskabelse, som flere regeringer og forskere er begyndt at tro på, kan være en realitet om et årti. Kvantecomputere kan i teorien lave mange parallelle udregninger i ekstremt højt tempo og dermed slå traditionelle supercomputere med flere længder. Ifølge en rapport fra konsulentfirmaet Boston Consulting Group ligger værdien af kvantecomputermarkedet i de kommende to til tre årtier på mellem 450 og 850 milliarder euro.

I juni lancerede Tyskland sit første kvantecomputerprojekt. I juli fulgte Frankrig og Nederlandene op med en fælles satsning på udvikling af fremtidsteknologien. Kvantecomputere kan ifølge en artikel i Science Magazine foretage udregninger på 200 sekunder, der ville tage vore dages supercomputere omkring 10.000 år at gennemføre.

Netop på dette udviklingsområde ligger EU på linje med både USA og Kina i kapløbet. Viljen til offentlige milliardinvesteringer i en endnu usikker teknologi er en forudsætning for at vinde.

Hvad så med software?

Det er lidt sværere at se for sig, hvordan EU-Kommissionens ambitioner om nye, europæiske tech-giganter på software og platformsområdet skal lykkes. Hvem i Europa kan tage kampen op mod Facebook, LinkedIn eller Twitter? Kender man overhovedet et europæisk udviklet socialt medie? Er der andre europæi-

ske tech-virksomheder end Spotify, du kan finde på din smartphone?

En del af formålet med EU's Digital Services Act og Digital Market Act er ganske vist at bryde de amerikanske tech-giganters nær-monopol på databehandling, sociale medier og online-platforme. Hvis de to lovforslag vedtages, er det muligt, at der bliver lidt bedre plads på markedet til nye europæiske online-virksomheder. Udfordringen er klar. I dag er det kun omkring 10 procent af behandlingen af europæiske data, der sker i europæiske virksomheder. Langt størstedelen foregår hos virksomheder fra Silicon Valley.

De relativt få eksisterende europæiske software-virksomheder er tilmed sårbare. I løbet af 2021 har den kinesiske tech-gigant Tencent købt store andele i nogle af verdens stærkeste computerspilsfirmaer i Sverige, Tyskland, Finland, Frankrig og Tjekkiet. Det sker, selvom EU's konkurrencelovgivning er blevet strammet og overvågningen af udenlandske investeringer – særligt dem, hvor der er mistanke om statsstøtte til opkøb – er intensiveret.

Strategiske investeringer

EU-samarbejdet har aldrig været gearet til offentlige investeringer, der er store nok til at have strategisk betydning. Det skyldes, at EU's samlede budget altid har ligget på under en procent af EU-landenes BNP, og dermed har det ikke været muligt virkelig at rykke på udviklingen. Men EU har også traditionelt modarbejdet store offentlige investeringer i medlemslandene. Både direkte ved at forbyde mange former for statsstøtte med henvisning til, at den frie konkurrence på markedet er den bedste allokeringsmekanisme for investeringer. Men også mere indirekte ved at sætte snævre grænser for, hvor meget gæld medlemslandene i eurosamarbejdet må stifte – uanset om gælden omsættes direkte til investeringer.

De bremser og begrænsninger er i en vis udstrækning suspenderet for at give EU-landene bedre mulighed for at komme ud af den økonomiske krise efter pandemien. Med den økonomiske genopretningspakke, der har leveret de første milliarder til gennemførsel af de nationale genopretningsplaner, bliver der over de næste fire år skudt ekstra 5.565 milliarder kroner ud i europæisk økonomi. 20 procent af de midler – det vil sige lige over 1.110 milliarder kroner – er øremærket investeringer i det digitale Europa.

Teknologisk magt

Den digitale virkelighed er en udfordring, men også en mulighed for demokratisering og cementering af menneskerettigheder. De enorme erhvervsinteresser, som sætter deres tydelige spor i lovgivning gennem lobbyindsatsen i Bruxelles, er nødt til at blive imødegået af forsvarere af borgernes, mediernes og civilsamfundets interesser.

Men et hvilket som helst forsøg på demokratisk eller borgerdrevet styring med udviklingen må også gøre sig klart, at man er oppe imod strategiske kerneinteresser. Et forhold som kommissæren for det indre marked, Thierry Bretons, indrammede retorisk skarpt i en tale på den digitale messe i Hannover i juli 2020:

"For mig står det klart, hvor vi er nødt til at gøre vores indsats: I det globale kapløb om teknologisk magt vil Europa føre an, hvis vi griber mulighederne i data, micro-elektronik og dataforbindelser."

Hvilke regler skal Facebook følge, når EU-borgere deler deres data i cyberspace? Skal vi være nervøse, hvis et kinesisk firma leverer 5G-netværk? Må kunstig intelligens overvåge vores færden og aktiviteter? Er det censur, hvis terrorrelateret indhold slettes?

Det digitale er blevet en del af vores hverdag og samfund. Butikker, myndigheder, medier og banker har vi i årevis forholdt os til på nettet. Nedlukningerne under pandemien har vist os, at venner, familie og kolleger også kan være digitale relationer.

I EU er ambitionen, at det digitale liv skal følge de sammen love, som vi kender fra det analoge liv. Demokrati og borgerrettigheder skal beskyttes, konkurrencelovgivning håndhæves og forbrugerne bør kunne færdes lige så sikkert på hjemmesider som i fysiske butikker.

Læs mere om EU's digitale strategi og de politiske dilemmaer lovgivningen rejser.

DEO

ISBN 978-87-94125-10-9

9 788794 125109