Digital suverænitet: fra begreb til strategisk ramme

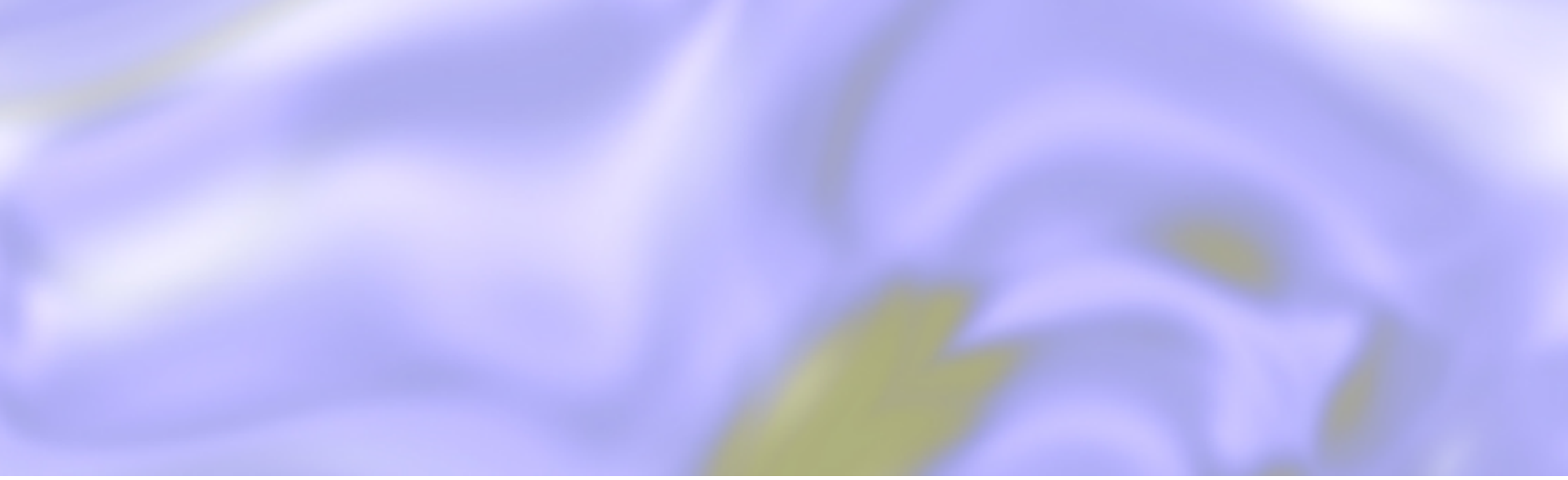
CAISA Forskningsbrief

Forfattere
Adler-Nissen, Rebecca; Eggeling, Kristin Anabel; Jurowetzki, Roman; Pedersen, Morten Axel

Redaktører
Søgaard, Anders; Feldt, Johannes N.

- Publikationsdato: 30. april 2026
- Publiceret af: CAISA, Det Nationale Center for AI I Samfundet, København og Aalborg, Danmark

- ISSN: 2795-0646
- Dokumentversion: Udgivers PDF, registreret version
- Citation for publiceret version (APA): Adler-Nissen, R., Eggeling, K. A., Jurowetzki, R., & Pedersen, M. A. (2026). Digital suverænitet: Fra begreb til strategisk ramme. *CAISA - Brief*. https://caisa.dk/forskning/digital-suveraenitet-fra-begreb-til-strategisk-ramme



Digital suverænitet: fra begreb til strategisk ramme

Af Rebecca Adler-Nissen, Kristin Anabel Eggeling, Roman Jurowetzki og Morten Axel Pedersen

Resumé: Digital suverænitet er flerdimensionel og kræver prioritering

I en tid med geopolitisk ustabilitet og hurtig AI-udvikling er kontrol over digital infrastruktur og data blevet afgørende. Selvom der er bred enighed om behovet for handling på nationalt, nordisk og EU-plan, mangler der et fælles sprog om digital suverænitet. Denne uenighed fører til enten handlingslammelse eller snævre tekniske løsninger uden strategisk retning.

Briefets **kerneargument** er, at digital suverænitet er et flerdimensionelt fænomen, der involverer både principiel stillingtagen og pragmatiske valg. Reducerer man det til tekniske løsninger, mister man synet for de værdier og valg, der bestemmer, hvem der kontrollerer og drager fordel af løsninger. Fokuserer man kun på værdier, ender man med tomme principper uden den nødvendige praktiske implementering og handlekraft. Digital suverænitet handler sjældent om et valg mellem fuld selvforsyning eller total afhængighed (Hoeffler & Mérand, 2024). I stedet drejer det sig om at balancere ofte modsatrettede krav om åbenhed, sikkerhed, konkurrenceevne, vækst, værdier og rettigheder i en verden med ujævnt fordelte kapaciteter.

Det betyder, at man må definere, *hvem* eller *hvad* der præcist skal beskyttes eller fremmes – inden for domænerne sikkerhed, økonomisk vækst eller borgerrettigheder – og erkende, at valg i ét domæne kan styrke eller underminere et andet. Briefet fokuserer på AI som det område, hvor digital suverænitet aktualiseres skarpest, men begreberne gælder for digital infrastruktur og data bredere. Briefet giver beslutningstagere redskaber til at håndtere disse dilemmaer ved at præsentere:

- En **begrebslig ramme** til at identificere, hvem eller hvad der skal være digitalt suverænt
- Et **overblik** over hvordan man prioriteter digital suverænitet rundt om i verden
- En **forståelse** af, at suverænitet kan udøves gennem tre **kontrolregimer**: ejerskab, ekspertise eller regulering – men at ingen af disse kontrolregimer er tilstrækkelige alene.

Briefets **centrale implikation** er, at digital suverænitet kræver en **integreret strategi**, der kombinerer ejerskab, ekspertise og regulering og håndterer sammenhænge og afvejninger mellem sikkerhed, økonomisk vækst og borgerrettigheder gennem klare mål. Uden denne helhedsorienterede tilgang risikerer man ineffektiv regulering, ubrugelig infrastruktur eller manglende evne til at udvikle, vedligeholde og anvende løsninger i praksis samt - utilsigtet - at underminere sikkerhed, vækst eller rettigheder.

Digital suverænitets mange betydninger

Der florerer et væld af definitioner af digital suverænitet, hvilket besværliggør en fælles samtale. I en filosofisk-teoretisk litteratur behandles begrebet ofte som et *absolut* begreb, knyttet til normative aspirationer om autoritet eller frihed (Floridi, 2021; Pohle & Thiel, 2020). I dette brief anvender vi et *relativt* begreb: digital suverænitet beskriver en aktørs (f.eks. stats, virksomheds eller borgers) grad af kontrol med digital infrastruktur, databrug og teknologisk udvikling, og evne til at reducere ekstern indflydelse (Adler-Nissen & Eggeling, 2024; PA Consulting, 2026; Damsgaard, 2026). Inden for AI indebærer digital suverænitet kontrol over: indsamling, behandling og opbevaring af data; hardware (cloud, netværk) og software (modeller, platforme, apps); samt institutioner, der sikrer juridisk beskyttelse og fremme af specifikke rettigheder og

værdier (Jurowetzki et al., 2025).[1] Som Jan Damsgaard (2026: 19) skriver "[d]igital suverænitet er evnen til at bevare handlefrihed, når afhængigheder bliver politiske. Og netop derfor er det ikke et IT-tema. Det er strategi."

Hvad eller hvem skal beskyttes eller fremmes gennem digital suverænitet?

Når politikere, myndigheder, civilsamfund eller virksomheder taler om digital suverænitet, taler de ikke altid om det samme. Tidligere undersøgelser har identificeret, at der oftest tales om at sikre, fremme eller beskytte ét af tre centrale domæner, der overlapper og påvirker hinanden: *sikkerhed*, *økonomi* samt *borgere* (Adler-Nissen & Eggeling 2024; Jurowetzki et al., 2025).

Sikkerhed: Når man taler om digital suverænitet som sikkerhed, handler det typisk om at beskytte national digital infrastruktur, data og kritiske teknologier mod udenlandske trusler, spionage og cyberangreb, men også om handlefrihed og evne til at håndtere sikkerhedspolitiske udfordringer uden risiko for afpresning eller uhensigtsmæssige (geo)politiske afhængigheder.

Økonomi: Når digital suverænitet tænkes som økonomi, handler det ikke kun om at reducere afhængighed, men om at kapitalisere på lokale styrkepositioner. Den reelle økonomiske værdi af AI og digital innovation skabes f.eks. ofte i det domænespecifikke lag – der hvor f.eks. store sprogmodeller eller cloud-infrastruktur møder lokal viden om arbejdsgange, brancher, regulering og data. Denne type viden er kontekstafhængig, svær at importere og ofte umulig at replicere – og den kan oversættes til en fordelagtig økonomisk forhandlingsposition globalt.

Borgere: Endeligt når vi taler om digital suverænitet som noget, der skal beskytte eller fremme borgere, drejer det sig ofte om at sikre, at udviklingen og anvendelsen af digitale teknologier, herunder AI, er i overensstemmelse med bestemte samfundsværdier, dyder, individuelle eller kollektive rettigheder eller principper.

Strategiske beslutninger om digital suverænitet indebærer ofte en afvejning mellem de tre domæner - sikkerhed, økonomi og borgere - og en forståelse af, at fremskridt i ét område kan understøtte eller underminere et andet. For eksempel udgør dataudveksling en risiko for borgeres privatliv, men kan samtidig fremme innovation og værdiskabelse. GDPR og forskelle i national implementering kan vanskeliggøre deling af sundhedsdata på tværs af grænser, hvilket styrker beskyttelsen af privatlivet, men begrænser adgangen til de store datasæt, der er vigtige for tværnational sundhedsforskning og udvikling af AI-baseret diagnostik. Tilsvarende kan EUCS-certificeringskravene til cloud-tjenester øge datasikkerhed, transparens og tillid, men hvis sådanne krav i praksis udvikles eller anvendes i retning af lokaliserings-, jurisdiktions- eller suverænitetskrav, kan de skabe spændinger i forhold til europæiske virksomheders adgang til avancerede AI-tjenester, som ofte afhænger af globale cloud- og hyperscale-platforme (ENISA, 2020; Lehdonvirta et al., 2025).

Tre globale tendenser for digital suverænitet

Den digitale suverænitets tre domæner og disses samspil bliver yderligere tydeliggjort, når vi ser på, hvordan forskellige stater og aktører arbejder med at balancere og prioritere disse for at reducere deres digitale afhængigheder. Vi kan i grove træk skelne mellem tre overordnede tendenser på globalt plan:[2]

Kontrol og autokratisk magtkonsolidering: Særligt i lande med forskellige slags og grader af autokratisk styre er digital suverænitet både et redskab til udvikling og til dominans. I Kina har WeChat og andre statsstøttede digitale platforme ikke kun muliggjort udviklingen af en kinesisk big tech-sektor og reduceret afhængigheden af amerikanske teknologivirksomheder, men også revolutioneret centrale samfundsfunktioner – fra forsikringer og betalinger til madlevering og social interaktion og statslig kontrol: Hvis myndighederne lukker din adgang til WeChat, bliver du i praksis udelukket fra det moderne samfund – uden adgang til betalinger, kommunikation eller offentlige tjenester. Her får digital suverænitet en dobbelt natur som både frihed og overvågning (Jurowetzki et al., 2025). Rusland kopierer Kina-modellen med MAX, en superapp der integrerer alt fra digitale ID'er til AI-chatbots. Målet er ikke bare kontrol, men regimeoverlevelse: at sikre, at vestlig teknologi ikke kan true det politiske system (Thumfart, 2025). Iran har udviklet et nationalt informationsnetværk (SHOMA/NIN) som led i en strategi for digital suverænitet, hvor vestlige platforme som Instagram og WhatsApp blokeres, mens lokale alternativer som Soroush og Rubika promoveres. Internationale sanktioner har accelereret Irans selvforsyningsstrategi, men har samtidig afskåret landet fra adgang til hardware og software. For Iran gælder det, at

[1] Grundmodeller, f.eks. GPT, Claude, Gemini, Llama, Mistral, Qwen og DeepSeek, er kapital- og regnetunge at træne og kontrolleres af et begrænset antal primært amerikanske og kinesiske aktører. Applikationssoftware, agenter og finetunede modeller bygges oven på dette lag og er tilgængelige for langt flere aktører.

[2] Dette afsnit opererer med inddelinger af lande, regioner og styreformer, der kan fremstå som generaliserende og med et vestligt/europæisk bias. Vi finder dog, at fordelene med denne kategorisering opvejer ulemperne i lyset af briefets overbliksskabende formål.

kontrollen styrkes, men samtidig begrænses landets teknologiske udvikling og globale integration.

Mere eller mindre liberal balancering: I lande, der ud fra diverse parametre betragtes som kernemedlemmer af den liberale internationale orden, der voksede frem efter Anden Verdenskrig, er suverænitet på det seneste blevet tænkt som et spørgsmål om *afvejninger* – mellem sikkerhed, individuelle rettigheder og økonomisk konkurrenceevne. EU har f.eks. traditionelt set sig selv som et åbent og liberalt marked på det digitale område, hvor de bedste spillere kan tilbyde sig på tværs af EU's medlemslande, så længe de overholder regler for fri konkurrence og grundlæggende rettigheder (f.eks. gennem GDPR), AI-forordningen (AI Act), *Digital Markets Act (DMA)* og *Digital Services Act (DSA)*. Denne tilgang er først for nyligt blevet justeret med et fokus på at reducere afhængigheder og fremme europæiske alternativer (gennem f.eks. European Cloud Framework) (Adler-Nissen & Eggeling, 2024). I USA er den grundlæggende strategi at sikre amerikansk global teknologisk overlegenhed gennem en blanding af statslig støtte (f.eks. CHIPS Act), eksportrestriktioner (særligt overfor Kina), markedsfrihed og afregulering. Under Trump-administrationen er USA's AI-strategi suppleret med en "antiwoke"-tilgang (The White House, 2025a) og et fortsat fokus på at begrænse kinesisk indflydelse, inklusive i multilateralt samarbejder (The White House, 2025b).

Japan har en længere tradition for tech-nationalisme inden for industrielle og kritiske teknologier og har siden 1980'erne haft til mål at styrke landets rolle i industrielle værdikæder, især inden for bilindustrien og den spirende halvlederindustri - kontrol bliver generelt tænkt som et spørgsmål om nationalt ejerskab og regulering. Således er et mål, at alle datacentre, netværkskabler og servere som håndterer følsomme oplysninger, forbliver i Japan (Hoshimi, 2025; JLL, n.d.). Sydkorea har hverken fulgt amerikanske markedsdrevne tilgange eller kinesiske statskontrolparadigmer, men har skabt et hybridt økosystem, der prioriterer nationale platforme og teknologisk kapacitet (Merrill, 2025). Man kombinerer statsstøttede tech-giganter som Naver og Kakao med en Digital Bill of Rights, der skal beskytte borgerne mod algoritmisk diskrimination (Merrill, 2025; Ministry of Science and ICT, Republic of Korea, 2023). Resultatet er et kompromis mellem rettigheder, vækst og sikkerhed.

Global opstigen: I den store og heterogene gruppe af lande fra det Globale Syd, hvoraf flere, såsom Brasilien og Indien, udgør stadig vigtige geopolitiske spillere og morgendagens centrale globale aktører, italesættes digital suverænitet ofte som en del af kampen for national opstigen og selvstændighed samt international anerkendelse (Adler-Nissen & Liebetrau, 2026). Indien bygger sin egen digitale infrastruktur (IndiaStack) for at undgå at blive styret af Google og Facebook (Pandey, 2025), men bruger samtidig internetnedlukninger til at slå ned på oppositionen (Thumfart, 2025). Brasilien ønsker national kontrol over betalingssystemer (Pix) og sociale medier, men samarbejder alligevel med Amazon Web Services (AWS) – en inkonsistens, der afslører at fuld uafhængighed er svær at opnå (Belli, 2024). I Nigeria er der i stigende grad fokus på digital inklusion og lokal lagring af data, men manglende infrastruktur og svag lovhåndhævelse gør visionen svær at opnå (Beyleveld, 2022). Nigeria har i stedet fokuseret på at give flere borgere adgang til digitale tjenester og internet - også uden for større byer (Federal Ministry of Communications, Innovation and Digital Economy, 2026). Resultatet er, at økonomisk vækst ofte vægtes over ejerskab, sikkerhed og rettigheder (Banya, 2025).

Tværgående tendenser: På trods af landenes og aktørers forskellige udgangspunkter og prioriteter, kan der også identificeres tværgående globale tendenser: stort set alle fokuserer i stigende grad på datalokalisering (Pandey, 2025), mindskning af afhængighed af udenlandske aktører (Liebetrau & Kristensen, 2021) samt cybersikkerhed (Muller, 2025). Her bliver *stiafhængighed* afgørende: Afhængigheden er kumulativ – jo længere et land undlader at træffe beslutninger om digital suverænitet, desto dyrere og sværere bliver det at ændre kurs. Lock-in-effekter betyder, at tidlige valg ikke bare former muligheder nu og her, men også fastlåser fremtidige beslutningsrum (Lambach & Monsees, 2025).

Hvordan udøves digital suverænitet?

Den anden dimension af digital suverænitet handler om, *hvordan* det udøves i praksis. For overskuelighedens skyld kan vi skelne mellem tre kontrolregimer.[3]

Kontrol gennem ejerskab: Dette kontrolregime handler om at opnå digital suverænitet ved at eje de tekniske komponenter, der udgør den digitale stack. Ejerskab kan

[3] Alle lande kombinerer kontrolregimer: EU fremmer europæisk-kontrolleret cloud-infrastruktur for at reducere afhængighed af USA og Kina, mens Rusland, Indien og Indonesien kræver lokal datalagring for at beskytte privatliv og styrke national vækst. Kina ("Made in China 2025") og USA ("Winning the AI Race") bygger økosystemer, der udnytter lokale data, ekspertise og infrastruktur for at cementere deres globale dominans. Draghi-rapporten (Draghi, 2024) følger en lignende strategi, men med fokus på Europas styrker – nicheindustrier, offentlig digitalisering og regulering – for at sætte en europæisk standard for AI og dataøkonomi.

være offentligt, privat, hybridt eller, i tilfældet af brugergenererede data, brugernes eget.

- **Hardware og infrastruktur**: datacentre, cloud-platforme, netværk, halvledere (f.eks. Amazon Web Services, Gefion, DelC, ASML).
- **Foundation models**: de store generelle AI-modeller, hvis træning kræver enorm regne- og kapitalkapacitet (f.eks. OpenAI, Anthropic, Meta, Mistral, DeepSeek).[4]
- **Applikationer og brugerflader**: de systemer hvorigennem borgere, virksomheder og myndigheder konkret anvender modellerne (f.eks. ChatGPT, Microsoft Copilot, Palantir AIP, danske vertikale løsninger).
- **Data og dataflows**: det indhold modellerne trænes på, og det input/output der genereres i brug; her er brugere og borgere selv reelle "ejere" i form af det indhold de bidrager med.

Den kinesiske stat kræver medejerskab i kritiske teknologivirksomheder, men for de fleste aktører er det ikke realistisk at skulle eje *hele* tech-stacken. På kort sigt vurderer mange lande, at de ikke har kapacitet eller råd til at bygge og udvikle egen hardware eller grundlæggende AI-modeller. I stedet fokuserer de på strategiske kontrolpunkter - f.eks. orkestreringslaget i tech-stacken.[5] På den måde øger de kontrollen, mens mange lande - ikke mindst i en EU-sammenhæng sætter strategiske og mellemsigtede mål hele tech-stacken, som f.eks. med EuroStack-initiativet (Bria et al., 2025).

Kontrol gennem ekspertise og evne til drift: Digital suverænitet afhænger ikke alene af ejerskab eller regulering, men i høj grad af evnen til at forstå, styre, anvende og reparere teknologien i praksis. Den afgørende kompetence ligger ikke nødvendigvis i at udvikle grundmodeller, men i at:

- specificere problemer præcist nok til, at teknologien kan løse dem,
- vurdere output kritisk (f.eks. AI-modellers nøjagtighed, bias eller sikkerhedsrisici),
- integrere løsninger i eksisterende arbejdsgange og systemer.

Denne kapacitet opbygges ved at arbejde med teknologien. Uden "absorptionskapacitet" (Cohen & Levinthal, 1990) – evnen til at optage, tilpasse og udnytte ny viden – kan hverken ejerskab eller regulering alene sikre reel kontrol. Det er en afgørende flaskehals: Uden kompetence til at forstå og styre teknologien risikerer man at blive afhængig af eksterne aktørers ekspertise, selvom man formelt ejer infrastrukturen eller sætter reglerne.

For europæiske virksomheder og myndigheder betyder det, at investeringer i ekspertise, håndgribelig implementering og brugerdrevet læring kan være mere værdifulde end at jagte teknologisk selvforsyning på alle niveauer. Den afgørende viden og ekspertise er f.eks.:

- STEM-kompetencer til udvikling af modeller, chips og datacentre
- Organisatorisk, samfundsvidenskabelig, humanistisk, juridisk, cybersikkerheds- og implementeringsekspertise til at skabe løsninger og applikationer, der imødekommer samfundsmæssige og økonomiske behov
- Operationel kontrol over kritisk infrastruktur (f.eks. datacentre, kabler, energi) samt centrale AI-platforme, der kan styre adgangen til modeller og tjenester

Ejerskab af teknologi er ikke nok alene. Ekspertise kan være en lige så begrænset og kritisk ressource som de sjældne jordartsmetaller, der indgår i produktionen af GPUer. Uden tilstrækkelig viden og driftskapacitet kan man hverken fuldt ud udnytte det, man ejer, eller forstå og håndhæve det, man regulerer. Uden viden og kompetencer blandt forskere, myndigheder, virksomheder og civilsamfund risikerer man at sidde med teknologiske aktiver eller lovgivningsmæssige rammer, som man ikke kan anvende strategisk eller tilpasse til lokale behov.

Kontrol gennem regulering. Digital suverænitet gennem regulering og lovgivning udøves primært af statslige aktører og internationale organisationer, men i nogle tilfælde (f.eks. Starlink) også af virksomheder med tilstrækkelig skala, magtmidler eller legitimitet til at påvirke både ejerskabs- og kapacitetsregimerne. Lovgivning kan sætte rammer for teknologiudvikling (som EU's DMA, DSA eller AI Act, der fastlægger regler for modeltræning, databeskyttelse og indholdsmoderation) og forbyde visse anvendelser, kræve transparens eller pålægge lokal datalagring. Men selv strenge regler kan undergraves af platformvirksomheders "arkitekturfordele" (Jacobides et al., 2006): store tech-selskaber designer deres systemer til at gøre sig selv uundværlige og partnere udskiftelige. Hvis man ikke ejer de afgørende knudepunkter (cloud-platforme, API'er, orkestreringssystemer) eller forstår de tekniske og operationelle detaljer, risikerer man at regulere i blinde, f.eks. kan en lov om europæisk datalokalisering være værdiløs, hvis en udbyder som Starlink eller

[4] Open weight-modeller (som Llama, Gemma, Mistral, Qwen) giver mulighed for at køre AI lokalt uden at sende data ud af landet eller organisationen, men det er vigtigt at understrege, at hardware-afhængigheden forbliver.
[5] Dette lag fungerer som et "operativsystem", der forbinder modeller med data, konkrete opgaver og brugere, sikrer overholdelse af lokale regler for datahåndtering og muliggør fleksibilitet, så man kan skifte udbydere uden at være låst fast.

Microsoft Azure kontrollerer de underliggende netværk eller softwarelag.

De tre kontrolregimer er værdiløse alene

De tre kontrolregimer – regulering, ejerskab og ekspertise – er gensidigt afhængige på en måde, der gør dem værdiløse i isolation:

- Regulering uden teknisk indsigt bliver til symbolpolitik – love og forbud, der ser strenge ud på papiret, men som mangler tænder, fordi man ikke forstår, hvad man regulerer, eller hvordan magt faktisk udøves i teknologiske systemer. Et eksempel er datalokaliseringskrav, der let omgås, når platforme som AWS eller Palantir kontrollerer de underliggende arkitekturer.
- Ejerskab uden kompetence til drift ender som katedraler i ørkenen – kostbare infrastrukturer eller teknologiske aktiver, der står ubrugte, fordi ingen ved, hvordan man udnytter dem strategisk.
- Ekspertise uden ejerskab eller regulatorisk magt reducerer et land til en talentfabrik for andre – en kilde til dygtige ingeniører, ledere, jurister og dataloger, der ender med at skabe værdi uden for landets grænser, fordi man ikke kontrollerer de systemer, de arbejder med, eller de regler, der styrer dem.

Digital suverænitet er dilemmafyldt

Tilbage står beslutningstagere altså med en perlerække af svære valg og tilsyneladende uløselige dilemmaer: Når forsvars- og sikkerhedsmyndigheder får adgang til avancerede analyseværktøjer – som dem den amerikanske virksomhed Palantir tilbyder – styrkes deres umiddelbare evne til at håndtere sikkerhedstrusler, som f.eks. terrorisme. Men afhængigheden af udenlandske teknologier giver sårbarheder ift. politisk pres: Når europæiske lande ikke kontrollerer den underliggende infrastruktur og arkitektur, kan selv strenge databeskyttelseslovgivninger som GDPR ikke forhindre, at europæiske analyser, data og operationer i sidste ende bliver underlagt udenlandsk indflydelse. Dermed kan gevinsten ved at bruge avancerede værktøjer gå på kompromis med den langsigtede sikkerhed, demokrati og suverænitet. Palantir afviser selv, at virksomheden ejer, lagrer eller anvender kundernes data til egne formål, og i f.eks. NHS-sammenhæng fremhæver både Palantir og NHS England, at Palantir fungerer som databehandler, mens kunden bevarer ansvar og kontrol over data. Dette ændrer dog ikke suverænitetsspørgsmålet: dataejerskab er ikke i sig selv tilstrækkeligt. Digitale suverænitet afhænger også af kontrol med softwarearkitektur, integrationslag, adgangsstyring, driftsmodel, opdateringscyklus og muligheden for at skifte leverandør. Afhængighed af en udenlandsk platform kan derfor skabe sårbarheder, selvom data formelt forbliver hos kunden - især hvis den tekniske infrastruktur og strategiske kontrol ligger uden for

Figur 1: Digital suverænitet, domæner og kontrolregimer.

Hvordan? – kontrolregimer

Hvad/hvem? – domæner

	Ejerskab Hardware • Sofware • Modeller	**Ekspertise** Viden • Drift • Kapacitet	**Regulering** Love • Standarder • Håndh.
Sikkerhed Infrastruktur Data Cybersikkerhed	Kritisk infrastruktur (datacentre, netværk, hardware)	Detektere, afværge, og håndtere cybertrusler; adgangskontrol	Cybersikkerhed, databeskyttelse, overvågning
Økonomi Vækst Konkurrence Domæneviden	Teknologiske aktiver (cloud, AI-modeller, patenter)	Udvikle, tilpasse og kommercialisere teknologi	Markedsadgang, konkurrence og lokal værdiskabelse
Borgere Rettigheder Værdier Transparens	Platforme og data der påvirker borgeres rettigheder	Designe, implementere og overvåge rettigheds-beskyttende systemer	Privatliv, ytringsfrihed og ikke-diskrimination

Hvert kontrolregime er virkningsløst alene. Regulering uden indsigt → symbolpolitik | Ejerskab uden drift → katedraler i ørkenen | Ekspertise alene → talentfabrik for andre

europæisk jurisdiktion (Palantir, 2023; NHS England, n.d.; UK Parliament, 2026; The Guardian, 2026).[6]

Hovedpunkter

- Rundt omkring i verden forsøger aktører at øge deres kontrol med digital infrastruktur og data med forskellige mål og metoder - nogle for at styrke autoritær kontrol eller økonomisk vækst, andre for at sikre bestemte samfundsværdier eller borgernes rettigheder og dyder.
- Kernen i digital suverænitet er afvejningen mellem **domænerne sikkerhed**, **økonomi** og **rettigheder** – både på kort og lang sigt. Disse afvejninger kræver anerkendelse af de gensidige afhængigheder mellem domænerne. For at en sådan afvejning skal finde sted og være gennemførlig og demokratisk forankret, vil det kræve strategier med klare mål og tæt samarbejde mellem offentlige og private aktører og civilsamfund.
- Digital suverænitet kan ikke opnås ved at vælge ét **kontrolregime**, men ved at integrere alle tre: **Regulering** skal være teknisk informeret til at modvirke strukturelle magtasymmetrier (f.eks. de store tech-platformes arkitekturfordele). **Ejerskab** må følges op med operationel kapacitet – ellers bliver det til dyre, tomme skaller. **Ekspertise** er **en afgørende faktor**, der bestemmer, om man kan realisere værdien af både ejerskab og regulering. Uden denne treenighed risikerer man at ende i en af tre fælder: ineffektiv regulering, dyr og ubrugelig infrastruktur eller *brain drain* til dem, der kan udnytte teknologien. Det betyder, at investeringer i tekniske løsninger skal gå hånd i hånd med investeringer i uddannelse og forskning samt i operationel drift og organisering både hos virksomheder og i det offentlige.

Om forfatterne

Rebecca Adler-Nissen er professor i international politik ved Institut for Statskundskab på Københavns Universitet og centerleder i CAISA, Det Nationale Center for AI i Samfundet.

Kristin Anabel Eggeling er seniorforsker ved Norsk Utenrikspolitisk Institutt og adjunkt ved Institut for Statskundskab på Københavns Universitet.

Roman Jurowetzki er lektor i innovationsøkonomi og anvendt datavidenskab ved Aalborg University Business School og chefforsker i CAISA, Det Nationale Center for AI i Samfundet.

Morten Axel Pedersen er professor i antropologi og social data science ved Institut for Antropologi og Copenhagen Center for Social Data Science (SODAS) og Chair for UCPH AI på Københavns Universitet og chefforsker i CAISA, Det Nationale Center for AI i Samfundet.

Om CAISA

Det Nationale Center for Kunstig Intelligens i Samfundet (CAISA) er et nationalt konsortium, der samler forskere fra Københavns Universitet, Aalborg Universitet, Aarhus Universitet, IT-Universitetet og DTU i tæt samarbejde med Pioneer Centre for AI (P1).

Som Danmarks uafhængige forskningscenter for kunstig intelligens i samfundet sætter CAISA borgerne i centrum. Vi udfører banebrydende tværfaglig forskning og skaber overblik over nye videnskabelige gennembrud. Funderet i ny og tværfaglig forskning rådgiver vi beslutningstagere i den offentlige og private sektor i, hvordan de bedst udvikler og anvender kunstig intelligens i praksis, så den bidrager til vækst, understøtter demokratiet og styrker digital selvbestemmelse.

Om CAISAs briefs

CAISAs briefs er en del af CAISAs indsats for at sikre, at viden og nye indsigter fra forskningsverdenen styrker beslutningstagere i offentlige myndigheder og private virksomheder – og dermed samfundet som helhed – når det står overfor de muligheder og risici, som hastig teknologisk forandring medfører. CAISA udgiver to slags briefs:

Forskningsbriefs præsenterer forsknings- og evidensbaseret viden inden for AI og samfund i en tilgængelig form.

Positionsbriefs udtrykker forfatternes forskningsbaserede og informerede vurdering af vigtige problemstillinger relateret til AI og samfund.

CAISAs briefs udgives under redaktion af Anders Søgaard, der er professor ved Datalogisk Institut, Københavns Universitet og chefforsker i CAISA, samt Johannes N. Feldt, der er videnskabelig assistent i CAISA. Alle briefs læses af og modtager kommentarer fra mindst én ekstern uafhængig forsker inden udgivelse.

Forfatterne er ansvarlige for indholdet i et CAISA-brief

[6] USA's CLOUD Act giver amerikanske myndigheder ret til at kræve adgang til data opbevaret hos amerikanske virksomheder – uanset hvor i verden data fysisk befinder sig. Det betyder, at europæiske virksomheder, myndigheder og organisationer, der bruger tjenester som Microsoft Azure eller Amazon Web Services (AWS) de facto opererer under amerikansk jurisdiktion, selvom data lagres i EU.

Referencer

- Adler-Nissen, R., & Eggeling, K. A. (2024). The discursive struggle for digital sovereignty: Security, economy, rights and the cloud project Gaia-X. *Journal of Common Market Studies*, 62(4), 993–1011. https://doi.org/10.1111/jcms.13594
- Adler-Nissen, R., & Liebetrau, T. (2026). Big Tech as world makers: A research agenda for international political sociology. *International Political Sociology*. Accepted manuscript.
- Banya, R. M. (2025). Africa's digital sovereignty trap: The data center dilemma. New America. http://newamerica.org/planetary-politics/briefs/africas-digital-sovereignty-trap/
- Belli, L. (2024). 'Building Good Digital Sovereignty Through Digital Public Infrastructures And Digital Commons In India And Brazil'. https://doi.org/10.2139/ssrn.4966348
- Beyleveld, A. (2022). Data localisation in Kenya, Nigeria and South Africa: Regulatory frameworks, economic implications and foreign direct investment. Policy Brief 7. Mandela Institute. https://www.wits.ac.za/media/wits-university/faculties-and-schools/commerce-law-and-management/research-entities/mandela-institute/documents/research-publications/PB7%20Data%20localisation%20and%20FDI.pdf
- Bria, F., Timmers, P., & Gernone, F. (2025). EuroStack: A European alternative for digital sovereignty. Bertelsmann Stiftung. https://doi.org/10.11586/2025006
- Cohen, W. M., & Levinthal, D. A. (1990). Absorptive capacity: A new perspective on learning and innovation. *Administrative Science Quarterly*, 35(1), 128–152. https://doi.org/10.2307/2393553
- Damsgaard, J. (2026). *Digital suverænitet*. København: Djøf Forlag.
- Draghi, M. (2024). The Draghi report on EU competitiveness. https://commission.europa.eu/topics/competitiveness/draghi-report_en
- ENISA. (2020). EUCS – Cloud Services Scheme: A candidate cybersecurity certification scheme for cloud services. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme
- Federal Ministry of Communications, Innovation and Digital Economy. (2026). *Nigeria Advances Digital Inclusion through Integrated Electrification and Connectivity Convening | The Federal Ministry of Communications, Innovation and Digital Economy*. https://fmcide.gov.ng/nigeria-advances-digital-inclusion-through-integrated-electrification-and-connectivity-convening/
- Floridi, L. (2021). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *SSRN*. https://doi.org/10.2139/ssrn.3827089
- Hoeffler, C., & Mérand, F. (2024). Digital sovereignty, economic ideas, and the struggle over the digital markets act: A political-cultural approach. *Journal of European Public Policy*, 31(8), 2121–2146. https://doi.org/10.1080/13501763.2023.2294144
- Hoshimi, A. (2025, October 15). Japan's sovereign cloud strategy: Innovation meets security. Itbusinesstoday. https://itbusinesstoday.com/tech/cloud/japans-sovereign-cloud-strategy-balancing-innovation-with-national-security/
- Jacobides, M. G., Knudsen, T., & Augier, M. (2006). Benefiting from innovation: Value creation, value appropriation and the role of industry architectures. *Research Policy*, 35(8), 1200–1221. https://doi.org/10.1016/j.respol.2006.09.005
- JLL. (n.d.). Japan's data centre market expands beyond Tokyo and Osaka. Retrieved 18 February 2026. https://www.jll.com/en-in/insights/japan-s-data-centre-market-expands-beyond-tokyo-and-osaka
- Jurowetzki, R., Adler-Nissen, R., & Pedersen, M. A. (2025). En modulær tilgang til digital suverænitet: Fra ambition til handling med et nationalt AI-orkestreringslag. *CAISA Brief*. https://caisa.dk/forskning/en-modulaer-tilgang-til-digital-suveraenitet
- Lambach, D., & Monsees, L. (2025). Beyond sovereignty as authority: The multiplicity of European approaches to digital sovereignty. *Global Political Economy*, 4(1), 71–88. https://doi.org/10.1332/26352257Y2024D000000007
- Lehdonvirta, V., Wu, B., Hawkins, Z. J., Caira, C., & Russo, L. (2025). Measuring domestic public cloud compute availability for artificial intelligence. *OECD Artificial Intelligence Papers*, No. 49. OECD Publishing. https://doi.org/10.1787/8602a322-en
- Liebetrau, T., & Christensen, K. K. (2021). The ontological politics of cyber security: Emerging agencies, actors, sites, and spaces. *European Journal of International Security*, 6(1), 25–43. https://doi.org/10.1017/eis.2020.25
- Merrill, N. (2025). The South Korean digital paradox: How South Korea's internet development model creates unique cybersecurity vulnerabilities. CLTC White Paper Series. https://cltc.berkeley.edu/wp-content/uploads/2025/04/South_Korean_Digital_Paradox_Report.pdf
- Ministry of Science and ICT, Republic of Korea. (2023, August). Digital Bill of Rights. https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=10&mPid=9&pageIndex=&bbsSeqNo=46&nttSeqNo=19
- Muller, L. P. (2025). Cybersecurity in practice: The vigilant logic of kill chains and threat construction. *European Journal of International Security*, 10(2), 231–251. https://doi.org/10.1017/eis.2024.27
- NHS England. (n.d.). Federated Data Platform: Frequently asked questions. https://www.england.nhs.uk/digitaltechnology/nhs-federated-data-platform/fdp-faqs/
- PA Consulting. (2026). Digital suverænitet i den offentlige sektor: Sammenfattende analyse af erfaringer og indsigter fra ind- og udland. https://www.kl.dk/nyheder/digitalisering-og-teknologi/2026/ny-rapport-kortlaegger-digital-suveraenitet-i-den-offentlige-sektor
- Palantir. (2023, November 21). Palantir and the NHS. https://blog.palantir.com/palantir-and-the-nhs-dd1362982fa9
- Pandey, P. (2025). Digital sovereignty and AI: Developing India's national AI stack for strategic autonomy. *Procedia Computer Science*, 254, 250–259. https://doi.org/10.1016/j.procs.2025.02.084
- Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4). https://doi.org/10.14763/2020.4.1532
- The Guardian. (2026, April 16). Labour and Lib Dem MPs demand 'shameful' Palantir NHS contract be scrapped. https://www.theguardian.com/technology/2026/apr/16/labour-and-lib-dem-mps-demand-shameful-palantir-nhs-contract-be-scrapped
- The White House. (2025a). Fact sheet: President Donald J. Trump prevents woke AI in the federal government. https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-president-donald-j-trump-prevents-woke-ai-in-the-federal-government/
- The White House. (2025b). Winning the AI race: America's AI Action Plan. https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf
- Thumfart, J. (2025). Digital Sovereignty in China, Russia, and India: From NWICO to SCO and BRICS. In M. Jiang & L. Belli (Eds.), *Digital Sovereignty in the BRICS Countries* (pp. 41–62). Cambridge University Press.
- UK Parliament. (2026, April 16). NHS Federated Data Platform. Hansard. https://hansard.parliament.uk/commons/2026-04-16/debates/2FDCA71C-D0C1-4738-BEE8-A4BDA311DB99/NHSFederatedDataPlatform