



Pozice Digital Council k evropské technologické suverenitě

Úvod

Digital Council vítá snahu Evropské unie posílit své technologické kapacity, odolnost a konkurenceschopnost. Vznikající evropský rámec technologické suverenity, včetně zejména Aktu o čipech 2.0, Aktu o rozvoji cloudu a umělé inteligence (CADA), Strategie EU pro open source a propojení digitalizace, AI a energetické politiky, může přispět ke snížení kritických závislostí a vytvořit nové příležitosti pro evropské firmy.

Pro Českou republiku jako otevřenou a exportně orientovanou ekonomiku je však zásadní, aby **technologická suverenita nebyla ztotožňována s technologickou soběstačností, lokalizací nebo izolací.**

Podle Digital Council by česká pozice měla vycházet z principu **otevřené technologické suverenity**: Evropa by měla posilovat vlastní technologické kapacity a schopnost řídit kritické závislosti, zároveň však zachovat otevřený trh, hospodářskou soutěž a spolupráci s důvěryhodnými mezinárodními partnery.

1. Suverenita by měla být založena na ověřitelných zárukách, kontrole a odolnosti

Česká republika by měla podporovat takové pojetí technologické suverenity, které je založeno především na **efektivní kontrole, ověřitelných bezpečnostních zárukách, interoperabilitě a možnosti volby.**

Původ společnosti, vlastnická struktura, národnost personálu nebo geografické umístění dat mohou být relevantní v úzce vymezených vysoce rizikových případech, neměly by však automaticky nahrazovat posouzení skutečných právních, technických a provozních rizik.

Bezpečnost, ochrana soukromí a odolnost závisí především na tom, **jak jsou data a systémy chráněny**, včetně silného šifrování, principů privacy and security by design, robustního řízení, přísné kontroly přístupu, auditovatelnosti a důvěryhodných mechanismů přeshraničního přenosu dat.

Česká republika by proto měla odmítat **diskriminační nebo zbytečně restriktivní požadavky na suverenitu u běžných cloudových a AI služeb**, včetně požadavků založených na lokální vlastnické struktuře, původu společnosti, národnosti personálu nebo plošném požadavku na imunitu vůči působení práva třetích zemí. Takové



podmínky mohou vést k vyloučení špičkových globálních poskytovatelů z evropského trhu, omezit možnost volby a zpomalit digitální transformaci, aniž by nutně přinášely odpovídající bezpečnostní přínos.

Přísnější požadavky mohou být odůvodněné u skutečně kritických workloadů, měly by však vycházet z konkrétního posouzení rizik a být přiměřené sledovanému zájmu veřejného pořádku nebo bezpečnosti.

Pokud jsou omezení založená na suverenitě uplatňována, měla by se proto vztahovat pouze na systémy nebo workloady, které splní **konkrétní a jasně definovaný test veřejného pořádku, bezpečnosti nebo obdobné kritičnosti**. Česká republika by měla rovněž podporovat vhodné výjimky pro zahrnuté či důvěryhodné obchodní partnery z mechanismů country screening, včetně čl. 18, pokud jsou zajištěny srovnatelné ochranné záruky.

2. Požadavky na suverenitu musí zůstat přiměřené

Česká republika by měla podporovat rozvoj evropské cloudové, AI a datacentrové infrastruktury a vznik společného evropského rámce, který omezí fragmentaci mezi členskými státy.

Současně by požadavky na dosažení jednotlivých stupňů Union Assurance Levels podle hlavy IV měly být přiměřené skutečným rizikům. Plošné uplatnění širokých požadavků na suverenitu u základních veřejných zakázek by mohlo zbytečně zužovat okruh dodavatelů, zvyšovat náklady veřejných institucí a daňových poplatníků a zpomalovat adopci cloudových a AI služeb.

Přísnější požadavky mohou být odůvodněné u skutečně kritických systémů, včetně některých funkcí v oblasti obrany, bezpečnosti nebo kritické infrastruktury. Neměly by se však plošně vztahovat na běžnou veřejnou správu nebo standardní komerční služby.

Česká pozice by proto měla podporovat **rizikově orientovaný a proporcionální přístup**, vzájemné uznávání auditů a certifikací a omezení duplicitních či překrývajících se regulatorních požadavků.



3. Lokalizace dat by neměla být výchozím pravidlem

Česká republika by měla odmítat plošné požadavky na lokalizaci dat jako základní nástroj technologické suverenity.

Fyzické umístění dat samo o sobě neurčuje úroveň bezpečnosti, ochrany soukromí ani odolnosti. Silné šifrování, zákaznická kontrola nad šifrovacími klíči, řízení přístupů, robustní governance, auditovatelnost a důvěryhodné mechanismy přeshraničního přenosu dat mohou poskytovat silnější ochranu než samotná geografická omezení.

Povinná lokalizace může rovněž snižovat odolnost tím, že omezuje geografickou redundanci, možnosti disaster recovery a přístup ke globálně distribuované kyberbezpečnostní infrastruktuře a odborným kapacitám. Může také zvyšovat náklady a omezovat přístup k pokročilým cloudovým a AI službám, aniž by nutně přinášela odpovídající bezpečnostní přínos.

Požadavky na lokalizaci by proto měly být vyhrazeny pouze pro **úzce vymezené případy, kdy je odůvodňuje konkrétní bezpečnostní riziko, riziko pro veřejný pořádek nebo kritičnost daného systému**, nikoli systematicky uplatňovány na běžné veřejné zakázky či komerční služby.

4. Silnější evropské kapacity bez protekcionismu

Česká republika by měla podporovat investice do evropských kapacit v oblasti polovodičů, cloudu, AI, softwaru, výzkumu a digitální infrastruktury.

Evropská technologická politika by však neměla být založena na plošném zvýhodňování podle původu poskytovatele ani na vylučování důvěryhodných neevropských technologií.

To je zvláště důležité ve vztahu k pojmu „**Union added value**“. Česká republika by měla podporovat jeho vymezení na základě objektivních, transparentních a nediskriminačních ukazatelů.

Posouzení by mělo komplexně zohledňovat skutečný přínos poskytovatele pro evropskou ekonomiku a technologický ekosystém, a to jak:



- **přímé přínosy**, například investice do infrastruktury, výzkumu a vývoje, tvorbu duševního vlastnictví, kvalifikovaná pracovní místa nebo zapojení evropských startupů a SME;
- **nepřímé přínosy**, včetně technologických platforem a služeb, které umožňují evropským firmám inovovat, růst a soutěžit na globálních trzích.

Sídlo poskytovatele, jeho vlastnická struktura nebo národnost by samy o sobě neměly určovat, zda vytváří hodnotu pro Evropu.

Evropská politika by měla usilovat o **posílení pozice Evropy v globálních technologických hodnotových řetězcích**, nikoli o její oddělování od nich.

5. Open source jako nástroj, nikoli povinný model

Česká republika by měla podporovat širší využívání open source, otevřených standardů a interoperabilních technologií jako nástrojů ke snižování vendor lock-inu a posilování technologické kontroly.

Digital Council podporuje princip:

Open source first, nikoli open source only.

Open source by neměl být automaticky preferován bez ohledu na bezpečnost, funkčnost, údržbu nebo celkové náklady vlastnictví.

Současně platí, že **open-source software není sám o sobě bezpečnější než proprietární software**. Jeho bezpečnost závisí na kvalitě vývoje a governance, včasném řízení zranitelností, bezpečnosti závislostí, robustním řízení přístupů a efektivním zajištění bezpečnosti softwarového dodavatelského řetězce.

Česká pozice by proto měla zdůrazňovat, že Evropa potřebuje nejen podporu vývoje open-source projektů, ale také jejich **dlouhodobou profesionální údržbu, bezpečnostní audity, řízení zranitelností, software supply-chain security a udržitelnou governance**.

Pro technologickou suverenitu jsou otevřené standardy, interoperabilita, přenositelnost a možnost změnit dodavatele v konečném důsledku důležitější než konkrétní licenční model.



6. Polovodiče: odolnost namísto autarkie

Česká republika by měla podporovat posilování evropského polovodičového ekosystému, nikoli však prostřednictvím snahy o úplnou evropskou soběstačnost ve všech částech hodnotového řetězce.

Prioritou by měla být **diverzifikace kritických dodávek a investice do oblastí, ve kterých mohou Evropa a Česká republika vytvářet skutečnou konkurenční výhodu.**

Pro Českou republiku jde zejména o vazby na automobilový průmysl, průmyslové aplikace, výzkum, návrh čipů, pokročilou výrobu a kvalifikovaná pracovní místa.

Důvěryhodná mezinárodní partnerství by měla zůstat nedílnou součástí evropské polovodičové politiky. **Diverzifikace je zpravidla odolnější než autarkie.**

Veřejná podpora by měla být zaměřena na jasně prokazatelnou technologickou a ekonomickou přidanou hodnotu a neměla by vytvářet trvalou dotační soutěž mezi členskými státy.

7. Energie a infrastruktura jsou podmínkou digitální konkurenceschopnosti

Rozvoj AI, cloudu a datových center nelze oddělit od energetické a infrastrukturní politiky.

Česká republika by proto měla podporovat užší propojení technologické a energetické politiky se zaměřením na:

- rozvoj elektrických sítí;
- dostupnost a transparentnost připojovací kapacity;
- rychlejší a předvídatelnější povolovací procesy;
- flexibilitu spotřeby a ukládání energie;
- efektivní využívání odpadního tepla;
- vysokokapacitní konektivitu;
- využívání digitálních technologií a AI ke zvyšování efektivity energetického systému.



Dostatečná energetická a síťová kapacita se stává jednou ze základních podmínek evropské i české digitální konkurenceschopnosti.

Hlavní priority pro českou pozici

Digital Council doporučuje, aby Česká republika prosazovala:

1. **technologickou suverenitu založenou na ověřitelných zárukách, efektivní kontrole, odolnosti a možnosti volby, nikoli na původu poskytovatele, vlastnické struktuře nebo lokalizaci;**
2. **odmítnutí diskriminačních nebo zbytečně restriktivních požadavků na suverenitu u běžných cloudových a AI služeb;**
3. **přísnější požadavky na suverenitu pouze tam, kde jsou odůvodněny konkrétním rizikem pro veřejný pořádek, bezpečnost nebo kritičnost systému;**
4. **proporcionální přístup k Union Assurance Levels, který zachová možnost volby dodavatele a zabrání zbytečnému růstu nákladů veřejných zadavatelů;**
5. **lokalizaci dat pouze tam, kde ji odůvodňuje konkrétní riziko, nikoli jako výchozí požadavek ve veřejných zakázkách;**
6. **objektivní, transparentní a nediskriminační kritéria pro Union added value, která zohlední přímé i nepřímé přínosy pro evropskou ekonomiku;**
7. **interoperabilitu, přenositelnost, otevřené standardy a možnost změnit poskytovatele;**
8. **princip „open source first, nikoli open source only“, doplněný robustní kybernetickou bezpečností, zabezpečením softwarového dodavatelského řetězce a dlouhodobou profesionální údržbou;**
9. **silnější evropské polovodičové a technologické kapacity při zachování spolupráce s důvěryhodnými mezinárodními partnery;**
10. **omezení regulatorní duplicity a nepřiměřené zátěže, zejména pro startupy a SME;**
11. **propojení technologické strategie s energetikou, konektivitou a fyzickou infrastrukturou.**



Závěr

Česká republika má jasný zájem na silnější a odolnější Evropě, která dokáže lépe řídit své kritické technologické závislosti a vytvářet globálně konkurenceschopné technologie.

Evropská technologická suverenita by proto měla posilovat **schopnost Evropy jednat a její svobodu volby**, nikoli vytvářet nové závislosti prostřednictvím lokalizace, protekcionismu nebo zbytečného zužování okruhu dodavatelů.

Evropa nepotřebuje technologickou izolaci. Potřebuje silnější vlastní kapacity, ověřitelné bezpečnostní záruky, skutečnou možnost volby a otevřený ekosystém důvěryhodných partnerů.

