

Suverénní AI

Když data nesmí opustit vaši organizaci

Kam směřuje AI a co z toho plyne pro veřejnou správu



Filip Dvořák, Ph.D.
zakladatel a CEO, Filuta AI



8. 9. 2026 · 15:00
Sekce kyberbezpečnost · zámek Mikulov

MIKULOV 2026

e-government 20:10



Filuta AI: tým, který za tím stojí



**Filip Dvořák,
Ph.D.**
zakladatel a CEO

- ✓ 15+ let staví autonomní AI systémy — plánování, optimalizace, usuzování
- ✓ 20+ mil. USD investic a výzkumných grantů (DARPA, ARPA-E, Horizon); exit 180 mil. USD s OQTON
- ✓ Patenty v USA i ve světě, 30+ publikací; ICAPS, IJCAI, ECAI



Slavomír Švancar

CTO

12+ let SW inženýrství;
provoz SaaS pro
300M+ uživatelů vč.
veřejné správy.



**Michael
Youngblood, Ph.D.**

Chief Scientist

Zakladatel a CEO
Geometric Analytics
(US/EU); výzkum v
PARC a SRI.



Helena Toušková

COO

10+ let v top-tier
poradenství
(technologie); strategie
a provozní modely.



Tomáš Plch, Ph.D.

CPO

15+ let výzkumu AI;
CD Projekt, Warhorse,
Activision; technický
ředitel v Pure Storage.



Petr Nádvořník

GTM & partnerství

10+ let v Google (US a
EU); globální
partnerství, portfolia
80–200 mil. USD.



**34 lidí · 5 profesorů
20 Ph.D. v AI a matematice**

250k+ citací (tým a poradní sbor); fellows
EurAI a AAAI

PORADNÍ SBOR



Tomáš Mikolov



Roman Barták



René Mořkos



Michal Trs

Gartner: poskytovatel kompozitní AI · prověrky NBÚ (Tajné) a EU SECRET · Filuta AI Labs — veřejná správa a bezpečnostní sbory

Nejcennější data státu nesmí opustit vaši organizaci. **Natož republiku.**



Vyšetřovací spisy

Miliony zpráv, dokumentů a záznamů na jeden případ. Čte je člověk — týdny.



Utajované informace

Vyhrazené, Důvěrné, Tajné — a přesně dané, kde a kým smějí být zpracovány.



Osobní údaje občanů

Správní spisy, registry, zdravotní a sociální data — pod GDPR i pod dohledem.



Kritická infrastruktura

Energetika, doprava, komunikační sítě — pro útočníka cíl, ne jen aktivum.

REALITA 2026

Nejsilnější AI je dnes služba v cizím datacentru, v cizí jurisdikci, za podmínek, které se mění v řádu týdnů. Pro většinu firem přijatelné. Pro stát ne.

**Suverénní AI = data zůstávají doma
a každé rozhodnutí umíte vysvětlit a obhájit.**

„Suverenita nezačíná u serveru. Začíná u otázky, kdo umí říct, proč systém rozhodl tak, jak rozhodl.“

Co se změnilo za posledních 12 měsíců



Od trénování k provozu

Náklady se stěhují z učení modelů do jejich provozu. Cena za odpověď klesá řádově, specializovaný hardware pro inferenci je standard.



Model už není produkt

Produktem je systém okolo něj: model + nástroje + paměť + vyhledávání + spouštění kódu + ověřování. Nástroje mají standard (MCP).



Otevřené modely stačí na většinu úřední práce

Open-weight modely lze provozovat ve vlastní infrastruktuře. Špička je dál — ale pro čtení spisů a hledání rozporů to není rozhodující.



Přístup ke špičce se řídí identitou zákazníka

Nejsilnější schopnosti (např. kybernetické) laboratoře uvolňují jen prověřeným zákazníkům v programech přístupu. Pravidla se mění v řádu týdnů.



Agenti obsluhují software jako lidé

Vývoj softwaru s asistencí AI je norma. Agenti začínají ovládat aplikace přes běžné uživatelské rozhraní — bez integrace. Odsud vede cesta k „agentickému státu“.



Ověření je nový úzký profil

AI zvládá úlohy, u nichž je ověření levnější než řešení (asymetrie ověření). Kde výsledek ověřit neumíme, nasadit ji nesmíme.

Shrnutí: inteligence zlevňuje, přístup k ní se politizuje — a úzkým profilem se stává ověření.

Symbolická, subsymbolická, neurosymbolická — a kam patří jazykový model



Symbolická AI

Logika, pravidla, omezení, plánování.

- Vysvětlitelná, auditovatelná, čitelná člověkem
- Model navrhuje expert; učí se z malých dat
- Škáluje na tisíce kroků rozhodování
- Slabina: svět se musí umět zapsat



Subsymbolická AI

Neuronové sítě, jazykové modely.

- Učí se z dat; skvělá na jazyk, obraz a vzory
- Statistická černá skříňka: slučuje korelaci s kauzalitou
- Spolehlivá na desítky kroků, ne tisíce
- Slabina: neumí doložit, proč



Neurosymbolická (kompozitní) AI

Symbolické jádro rozhoduje a dokládá, neuronové modely čtou a navrhuji.

- Čísla a logika deterministicky, jazyk generativně
- Každý závěr dohledatelný ke zdroji
- Stejný vstup → stejný výstup
- AI píše příběh, nikdy rozsudek.

Jazykový model patří na okraj procesu — tam, kde se čte a formuluje. Ne do středu, kde se rozhoduje.

Čtyři vlastnosti AI, kterou úřad podepíše



1

Data zůstávají doma

Provoz on-premise nebo zcela bez internetu. Jurisdikce ČR/EU. Žádné učení dodavatelova modelu na vašich datech.



2

Vysvětlitelnost

Každý závěr dohledatelný ke zdroji: ke spisu, paragrafu, záznamu. Úředník deleguje práci, ne odpovědnost.



3

Auditovatelnost a reprodukovatelnost

Stejný vstup → stejný výstup. Číslo bez AI, auditní stopa pro interní kontrolu, NKÚ i soud.



4

Nezávislost na dodavateli

Vyměnitelné modely, otevřené formáty, znalost zůstává úřadu. Zeptejte se dodavatele, jak vydělává.



Rámec, který to bude vyžadovat

Zákon o kybernetické bezpečnosti (NIS2)

Řízení rizik a dodavatelů zahrnuje i AI systémy a jejich modely.

AI Act, příloha III

Bezpečnostní sbory, migrace, justice, veřejné služby = vysoké riziko. Povinnosti od 2. 12. 2027 (nař. (EU) 2026/1744).

GDPR

Zpracování ve vlastní infrastruktuře = méně předávání a zpracovatelů.

Správní řád

Rozhoduje úřad, ne model. Odůvodnění musí existovat i tam, kde radila AI.

„Úředník může delegovat práci, nikdy odpovědnost. AI proto musí umět ukázat, odkud každý závěr vzala.“

Suverénní není server. Je to celý řetězec.



LIDÉ A PROCES

Kdo zadává, kdo ověřuje, kdo podepisuje · role, oprávnění, prověrky



SYSTÉM

Analytická AI: propojuje důkazy, ověřuje hypotézy, dokládá zdroje · řízení přístupu (deny-by-default) · auditní log

Filuta AI



MODELY

Otevřené jazykové modely · malé specializované modely · symbolická jádra (logika, plánování, omezení)

Filuta AI



VÝPOČETNÍ INFRASTRUKTURA

GPU servery v ČR · modulární datacentra · energie a chlazení · fyzická bezpečnost

Jiří Fiala, COLLAPO

Kde suverenita vzniká



Jurisdikce

kde data fyzicky leží a kdo k nim smí



Kontrola

kdo může měnit model, pravidla a přístupy



Vysvětlení

kdo umí říct, proč systém rozhodl



Kontinuita

co se stane, když dodavatel zmizí

Suverénní AI = železo + model + rozhodnutí + audit – a schopnost kteroukoli část vyměnit.

Co funguje, co ne — a co to stojí



Funguje

- Hybrid: klasické vyhledávání + několik menších specializovaných modelů místo jednoho obřího
- Symbolické jádro pro čísla, logiku a plánování; jazykový model jen na okraji
- Jeden GPU server unese model se stovkami miliard parametrů — pro úřad velikosti ministerstva to stačí
- Plná izolace (jednosměrné prostředí) je proveditelná i provozně zvládnutelná



Nefunguje

- Dotrénování na citlivých datech — model si je pamatuje a může je vyzradit
- Jazykový model jako zdroj čísel, citací a lhůt
- „AI všude“ bez otázky na návratnost
- Nákup modelu bez nákupu ověření



Co to stojí

- Pořízení: GPU server pro velký model řádově jednotky milionů Kč; menší modely běží i na běžných serverech
- Provoz: elektřina, chlazení — a hlavně lidé, kteří systému rozumějí
- Skrytý náklad: lidé, kteří po špatně nasazené AI uklízejí
- Pravidlo zastavení: investujte, dokud další koruna vrací víc než korunu

„Úřad platí dvě faktury a vidí jen jednu: tu za AI — a tu za lidi, kteří po ní uklízejí.“

Analytická AI, která každý závěr doloží zdrojem



Vstup

Forenzní export z jednoho zařízení: miliony zpráv, více messengerů, více jazyků



Deterministické jádro

Statistika, síť kontaktů, časové osy — čísla bez AI, pokaždé stejná



Jazykové modely

Čtou, překládají, navrhnou hypotézy — lokálně, bez internetu



Ověření proti zdroji

Každá citace dohledána; co nelze doložit, je označeno



Výstup

Zpravodajský obraz s odkazy na zdroj — během minut, ne týdnů



Proč se pod to dá podepsat

Běží u vás

Jediný instalační balík, zcela bez internetu, s lokálními modely.

Vysvětlitelné

Každý závěr → zdroj. Co zdroj nemá, je viditelně označeno.

Reprodukovatelné

Stejná data, stejná čísla — dnes, za rok, u soudu.

Stejný princip jinde

Spis ve správním řízení, zadávací dokumentace, dvě verze vyhlášky.

„Úzkým hrdlem nejsou data. Je to člověk, který je musí všechna přečíst.“

Jak začít: pět pravidel

1

Začněte od dat, která nesmí ven.

Klasifikace dat určí architekturu (cloud / vlastní / izolované prostředí) — ne naopak.

2

Vybírejte úlohy, kde je ověření levnější než řešení.

Úplnost podání, rozpory ve spisu, porovnání verzí: AI navrhne, člověk rychle zkontroluje.

3

Oddělte čísla od příběhu.

Čísla, lhůty a logika deterministicky. Jazykový model jen na shrnutí a formulaci.

4

Kupujte auditní stopu, ne „inteligenci“.

Zdroj u každého závěru, výměna modelu bez přepisu systému — a otázka, jak dodavatel vydělává.

5

Měřte návratnost a umějte přestat.

Pilot na jedné úloze s měřitelným ověřením. Investujte, dokud další koruna vrátí víc než korunu.



Prvních 90 dní

1 úloha

ohraničená, opakovaná, s jasným výstupem

1 klasifikace dat

která rozhodne o místě provozu

1 metrika ověření

kolik závěrů člověk potvrdil / opravil

1 rozhodnutí

pokračovat, rozšířit — nebo skončit

„Neptejte se, co AI umí. Ptejte se, co u vás umíte ověřit.“

Tři věci, na které se připravit



1

„Agentický stát“ v praxi

Agenti obsluhují stávající agendové systémy přes jejich uživatelské rozhraní — bez integrace a přepisu. Nejdřív rutina: podání, lhůty, úplnost. Podepisuje člověk.

Připravte se: inventura agend, kde je ověření levné



2

Cena inteligence padá, cena důvěry roste

Provoz modelů zlevňuje řádově. Drahé bude ověření, audit a odpovědnost. Vzniká nová kategorie: ověřená AI (verified AI).

Připravte se: metriky ověření v každé zakázce



3

Suverénní provoz jako výchozí volba pro citlivá data

Otevřené modely + výpočetní kapacity v ČR + sdílená státní platforma místo desítek izolovaných projektů.

Připravte se: klasifikace dat jako první krok

„Nejdražší otázka roku 2028 nebude „co AI umí“. Bude to: „kdo ověřil, že to udělala správně“.“

Tři věty na závěr

1

Nejlepší AI pro stát není ta nejchytřejší, ale ta, kterou umíte vysvětlit, auditovat a vyměnit.

2

Jazykový model patří na okraj procesu. Rozhodnutí a čísla patří tam, kde je lze doložit.

3

Suverénní AI je proveditelná dnes — u vás, i zcela bez internetu. Nejdražší části nejsou grafické karty, ale lidé, kteří ji umějí ověřit.

→ Kde to poběží: suverénní výpočetní infrastruktura v ČR — Jiří Fiala, COLLAPO



Neurosymbolická AI · Analytická AI

Děkuji.

Otázky?

✉ filip@filuta.ai

filuta.ai

„Ani bajt přitom neopustí vaši budovu.“

✓ Data zůstávají doma

✓ Vysvětlitelná

✓ Auditovatelná a reprodukovatelná

✓ Nezávislá na dodavateli

Filuta AI · poskytovatel kompozitní AI uznaný Gartnerem · tým s prověrkou NBÚ (Tajné) a EU SECRET

Veřejná správa · Bezpečnostní sbory · Zpravodajské služby · Průmysl