BÍLÁ KNIHA

VNITŘNÍ ZÁLEŽITOSTI

TOP tým

poslanecký klub Čels v evropském parlamentu

Předmluva

Luděk Niedermayer
europoslanec

V současném světě plném rychlých změn a komplexních problémů či krizí se před naší zemí i naším kontinentem objevují další a další výzvy v klíčových oblastech, jako jsou hospodářství, zahraniční a evropská politika, energetika, ale i ve školství, sociální a zdravotní politice. Stále více se diskutuje o bezpečnosti v Evropě, o její energetické, technologické i surovinové soběstačnosti, o udržitelnosti či budoucí roli umělé inteligence v ekonomice i společnosti jako takové.

Odpověď na tyto výzvy stojí mimo jiné i v kvalitě a flexibilitě vzdělávacích systémů a třeba i přípravě společnosti na změny spojené s demografickým vývojem. A to jsou jen dvě z mnoha oblastí, ve kterých úspěch či neúspěch bude formovat naši budoucnost. Otvírá se před námi mnoho otázek a s nimi vzniká také prostor pro tvorbu nových odpovědí. Naše doba vyžaduje schopnost nejenom včas aktivně reagovat na nové výzvy, ale též schopnost je předvídat a aktivně přispívat k formování nových odpovědí na výzvy budoucí. A nejde jen o "abstraktní odpovědi", ale hlavně, v souladu s nimi, přijímání funkčních politik, které zajistí stabilitu, bezpečnost a prosperitu naší společnosti.

V proměnlivém prostředí světa, Evropy a České republiky ve 21. století budou získávat čím dál větší roli dnešní mladá generace, jejichž názory a pohledy jsou nositeli budoucí podoby naší společnosti. Velmi proto vítám angažovanost členů a členek mládežnické politické organizace TOP 09 TOP týmu, kteří projevují aktivní zájem o konstruktivní řešení výzev, jež ovlivňují a budou ovlivňovat nejen jejich generaci, ale i celou společnost, včetně generací budoucích. V postojích členů TOP týmu, reflektovaných v následujících bílých knihách můžeme vidět důkaz, že mladí lidé nejen sledují vývoj společnosti, ale také aktivně přispívají do veřejné diskuse. Není jim lhostejná budoucnost naší země ani Evropské unie a toho si velmi cením.

Právo

Novela volebního zákona

Podporujeme zavedení možnosti korespondenční volby. Je nutné zajistit, aby mohli volit i čeští občané nacházející se mimo republiku, a to nejjednodušším proveditelným způsobem. Jde o jejich právo. I z pozice kvality demokracie, by se na utváření politik ve státě mělo podílet co největší procento způsobilých občanů. Můžeme pohlédnout do mnoha zemí světa, kde korespondenční volba zdárně funguje, a to i v našem nejbližším okolí. Na Slovensku mají korespondenční volbu již více než 17 let a jde o zcela legitimní prostředek účasti u voleb, přičemž už se nad tím nikdo ani nezamyslí.

Podporujeme iniciativu změny aktivního volebního práva nejprve v rámci komunálních a krajských voleb, a to z 18 let na 16 let.

Jsme pro ratifikaci tzv. „Istanbulské úmluvy", Úmluvy Rady Evropy o prevenci a potírání násilí vůči ženám a domácího násilí. Jsme přesvědčeni, že tato Úmluva má svou materiální váhu a že nejde pouze o politickou proklamaci, ba zavádění pojmů závadné povahy, jak se snaží tuto Úmluvu zdiskreditovat určité spektrum politiků či veřejnosti. Pro TOP tým je zejména důležité, aby Česko patřilo k zemím, které vynakládají na preventivní část potírání násilí vůči ženám i jiným osobám a potírání domácího násilí maximální úsilí, neboť každý člověk je hoden veškeré dostupné ochrany své cti, zdraví a osobních práv a svobod.

Je nutné připravit český právní řád na výzvy související s umělou inteligencí. Zejména vyřešit otázky související s právem duševního vlastnictví a umělou inteligencí. Dále jsme také pro novelizaci trestního zákoníku a zákona o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů, která zohlední technologický pokrok vedoucí k možnostem pořizování obsahu, kterým mohou být zneužita práva na

ochranu osobnosti a cti zejména mladistvých fyzických osob a ohrožen také mravní vývoj mládeže a také celospolečenské hodnoty.

Podporujeme implementaci online soudnictví ADR (Alternative Dispute Resolution)

V rámci justice navrhujeme zavedení přezkoušení pro soudce (např. každých 10 let) a navrhujeme zrušení institutu přísedících. Zasadíme se o odklon od retributivní justice směrem k restorativní justici

Narovnání výše srážek v rámci exekučního a insolvenčního řízení

Státní správa

Podporujeme zachování systému hodnocení státních zaměstnanců. Možnost podílet se na svém vlastním ohodnocení, čímž by se zamezuje začátku možných problémů na pracovišti. Nutné je lépe podporovat schopné kvalitní zaměstnance a jejich kariérní růst, stejně tak propojit pracovníky ministerstev a samotné úřady. Optimalizace počtu úředníků je žádoucí, tak jako se snížily počty úředníků na ministerstvu zdravotnictví a ministerstvu financí, stejným příkladem by se měla řídit i zbylá ministerstva a zbylé úřady. Revize počtu roztříštěných agend, které by se daly sloučit v rámci jednoho, ne pěti úřadů. Digitalizace nejen státní správy je jednou z největších výzev, kterou bychom měli řešit.

Podporujeme větší zapojení soukromého sektoru do činností státu; výstavby soukromých dálničních úseků, nebo privatizace České pošty, je jedním z možných kroků. V rámci řešení nutných záležitosti se státem podporujeme mobilitu poboček úřadů, např. v rámci menších obcí, kde by úřad mohl fungovat jen omezenou dobu v týdnu a v dalším čase působit v blízkém okolí, v jiných obcích.

Chceme zavést systém AI (zejména generativní) do veřejné správy a to za účelem zeštíhlení státní správy (snížení počtu státních úředníků) a její zefektivnění.

Chceme zefektivnit státní správu a samosprávy (slučování obcí a krajů) a podpořit legislativu a zjednodušení pravidel pro slučování

Digitalizace a Kybernetická bezpečnost v České Republice

Digitální identita nabízí celé množství výhod, například efektivnější a rychlejší komunikaci občana se státem, dále díky bezpečnostním prvkům (například dvoufaktorové ověření) také zlepšení bezpečnosti a lepší ochranu soukromí. Zároveň by také díky digitální identitě by mohlo dojít k růstu Českého HDP až o 3,7 %.

Současně je digitální identita upravena nařízením eIDAS a zákonem č. 250/2017 Sb., o elektronické identifikaci.

Základním prvkem elektronické (digitální) identity jsou prostředky pro elektronickou identifikaci, prostřednictvím těchto prostředků je možné se skrze národní bod přihlásit k online službám (např. k elektronickým službám Finanční správy – MOJE daně).

Prostředků pro elektronickou identifikaci je v současně době dostupná celá řada, lze je rozdělit na prostředky elektronické identifikace spravované státními orgány a prostředky elektronické identifikace spravované soukromými (akreditovanými) osobami

Prostředky elektronické identifikace spravované státními orgány:

- Mobilní klíč eGovernmentu
- NIA ID
- eObčanku

Prostředky elektronické identifikace spravované soukromými (akreditovanými) osobami:

- I.CA identita
- MojeID
- Bankovní identita

Tento velký počet je zapříčen různými technickými řešeními, které je možné použít pro prostředky pro elektronickou identifikaci, některé tak například využívají karetní princip (eObčanky) a jiné například používají mobilní aplikace (Mobilní klíč eGovernmentu).

V současné době probíhá na úrovni EU legislativní proces revize nařízení nařízením eIDAS, který představil koncept nového nástroje digitální identity – evropskou peněženku digitální identity (EUDI Wallet). EUDI Wallet budu nad rámec přístupu k online službám sloužit také k elektronickému podepisování, ukládání el atributů (vysokoškolský diplom, řidičský průkaz apod.) apod.

EU si pro oblast digitální identity vytyčila cíl, aby alespoň 80 % občanů Evropské unie využívalo prostředky elektronické identifikace do roku 2030

V současné době je v ČR možné identifikovat tyto problematické aspekty digitální identity:

1. Vysoký počet prostředků pro elektronickou identifikaci
2. Nízká míra informovanosti společnosti o digitální identitě

Nízká míra využívání vydaných prostředků pro elektronickou identifikaci

Kyberbezpečnost

Každým rokem rostou kybernetické útoky zaměřené na Českou republiku. V srpnu 2023 bylo evidováno dvojnásobek kybernetických incidentů oproti červenci 2023. Je nezbytné vzhledem k vzrůstajícím útokům nejen zvyšovat povědomí o kybernetických hrozbách, ale i navýšit rozpočet na bezpečnost. Za hlavní problémy v této oblasti mohu jmenovat vedle nedostatku financí, nedostatek odborníků, který je klíčový. Bohužel současný stav a ohodnocení ve státní správě je nedostatečné a nedokáže konkurovat nabídkám ze soukromého sektoru. Pokud chceme posílit státní složky je nezbytné najít takové řešení, které naopak přiláká specialisty a odborníky v oblasti kybernetické bezpečnosti. Musíme si uvědomit, že tato oblast se velice rychle vyvíjí a mění, mohu ji označit za tzv. živou a bez odborníků, informací - osvěty v rámci kyberbezpečnosti je nemožné v budoucnu zabránit nebo zmírnit dopady nečekaných kybernetických útoků. Nezbytná je informovanost a edukace nejen v státních institucích jako jsou nemocnice, školy, ministerstva ale i veřejnost, která se může nevědomky stát cílem a obětí nějaké kybernetické hrozby.

Souhrn kyberbezpečnosti v ČR podle NÚKIB

Podle statistik NUKIBu z roku 2022 je ČR vystavena neustálými útoky, které mají za cíl ochromit její významné služby. Patří sem i skupiny operující v rámci celé EU, a které jsou i podporované cizími státy, nejčastěji Ruskem.
Nejčastějším typem útoku zůstává tzv. DDos útok, který má za cíl vyřadit z provozu konkrétní službu nebo celou infrastrukturu. Navzdory minimálním dopadům byly DDoS útoky v tuzemsku často silně medializovány, přičemž skupiny jako Killnet či Anonymous Russia posléze tyto články přebíraly a propagovaly je svému domácímu publiku na sociální síti Telegram se snahou zveličovat jejich reálné dopady. Přílišná medializace útoků v napadených zemích tak paradoxně podporovala cíle útočníků.

Podle dat Policie ČR se kybernetická kriminalita zvýšila meziročně o 95 %. Z dotazovaných organizací 68 % zaznamenalo pokus o kybernetický útok, ať už s cílem vyřadit některou jejich službu nebo se jednalo o snahu získat nějaké citlivé informace. Jako pozitivum můžeme brát informaci, že roste počet společností, které začali brát kybernetickou bezpečnost vážně a začali do ni investovat. Bohužel v průměru se jedná o 0–5 % svého rozpočtu.

Novou bezpečnostní hrozbou pomalu začnou být tzv. smartmetery. Ty musí být do roku 2027 nasazeny na odběrných místech se spotřebou nad 6 MWh. Jejich hlavním účelem je zajistit aktuální informace o zatížení soustavy, zajištění lepší kontroly, bezpečnosti a stability rozvodných sítí, ale také zpětnou vazbu o spotřebě energie koncovým zákazníkům. NÚKIB proto upozorňuje na bezpečnostní rizika spojená hlavně se společnostmi, jejichž politicko-právní prostředí zavazuje tyto společnosti spolupracovat s tamními bezpečnostními nebo státními orgány na úkor soukromí či bezpečnosti zákazníků dané společnosti.

NIS 2

Jedná se o směrnici k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, která byla schválena při našem předsednictví. Tato směrnice musí být do 16.10.2024 převedena do našeho práva a být schválena.

Toto nařízení se bude týkat subjektů tzv. poskytovatelů regulované služby. Jedná se o jakýkoliv subjekt, který poskytuje alespoň jednu regulovanou službu, tedy službu, jejíž narušení by mohlo mít významný dopad na zabezpečení důležitých společenských nebo ekonomických činností. Těmto subjektům ukládá určité povinnosti např. hlásit bezpečnostní hrozby, zavádět určitá opatření atd. Dále novela rozšiřuje způsob prověřování dodavatelů strategické infrastruktury státu v oblasti informačních a komunikačních technologií. Samotné prověřování bude stát moci provádět jak se zaměřením na dodavatele, kteří již svá plnění do infrastruktury pro poskytování strategicky významných služeb dodávají, tak na jejich poddodavatele či potenciální dodavatele. Prověřování dodavatelů a subdodavatelů se bude týkat i států, ze kterých dodavatelé pocházejí, a které mohou mít na dodavatele vliv.

Vize

- Posílení odborníků v oblasti kyberbezpečnosti pro zajištění lepší obranyschopnosti ve státní správě
- Dotace na předmět rozvíjející edukaci v online světě (kyberbezpečnosti) pro základní/střední školy
- Nezveřejňovat identitu útočníků a nedávat jim mediální prostor, zvláště pokud jejich akce neměla velký dopad
- Umožnit příjem dotací na kyberbezpečnost i společnostem, které nepatří do veřejné správy, ale jsou dle NIS 2 poskytovatelé regulované služby
- Zvýšit všeobecné povědomí o důležitosti kybernetické bezpečnosti
- Připravit úspěšný projekt evropské peněženky digitální identity (v kooperaci se soukromým sektorem)
- Dosáhnout cíle, aby alespoň 80 % občanů ČR aktivně využívalo prostředky elektronické identifikace do roku 2030
- Zvýšit informovanost občanů ČR o možnostech digitální identity