Úřad vlády České republiky
Legislativní rada vlády České republiky
Pracovní komise pro hodnocení dopadů regulace (RIA)

V Praze 1. března 2024
Čj.: OVA 68 + 69/24

Stanovisko

k

Návrhu zákona o kybernetické bezpečnosti + Návrhu zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti

I. Úvod

Návrh předkládá na základě plánu legislativních prací vlády na rok 2023 Národní úřad pro kybernetickou a informační bezpečnost (dále jen „Předkladatel“). Předkladatel vykonává na základě § 22 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, státní správu v oblasti kybernetické bezpečnosti. Z tohoto důvodu je i mimo jiné gestorem řádné transpozice směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2), která je provedena předloženým návrhem nového znění zákona o kybernetické bezpečnosti (dále jen „návrh zákona“), kterým se ruší a nahrazuje zákon o kybernetické bezpečnosti. Cílem návrhu zákona je především zajistit řádnou transpozici směrnice NIS 2.
Předkladatel se tedy rozhodnul do předloženého zákona zpracovat také mechanismus prověřování bezpečnosti dodavatelského řetězce.

Jako důvody pro navržení nové právní úpravy uvádí tedy Předkladatel následující:

- transpozice směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (dále jen „směrnice NIS2“),

- legislativní úkol Předkladatele zpracovat a předložit vládě návrh zákona, zpracovaný na základě Bezpečnostní radou státu zvoleného přístupu A – Prověřování dodavatelů, podle aktuální bezpečnostní situace, uvedeného v materiálu „Bezpečnost dodavatelských řetězců strategické infrastruktury státu“, č. j. 28261/2022-UVCR“ (dále také jen „mechanismus prověřování bezpečnosti dodavatelského řetězce“ nebo „mechanismus“) zařazený v Plánu legislativních prací vlády na rok 2023.
- reflektování připomínek z praktické aplikace zákona o kybernetické bezpečnosti.

Cílem návrhu zákona pak má být na základě všech tří výše uvedených skutečností vytvořit ucelený právní předpis reagující na tyto nové požadavky a prostřednictvím něj dosáhnout vysoké společné úrovně (kybernetické) bezpečnosti služeb v České republice.

Kromě zprávy RIA k *Návrhu zákona o kybernetické bezpečnosti* byla Předkladatelem vypracována i zpráva RIA k *Návrhu zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti.* Je otázkou, zda by nebylo vhodnější sloučit obě zprávy do jedné, jelikož RIA ke změnovému zákonu nepřináší podstatné dodatečné informace.

V návaznosti na výše uvedené se stanovisko Komise RIA věnuje Závěrečné zprávě RIA k Návrhu zákona o kybernetické bezpečnosti.

II. Připomínky a návrhy změn

Závěrečná zpráva RIA je rozdělena na 7 částí. První část se věnuje obecnému rámci změn a popisu současného stavu, následných 6 částí se zabývají jednotlivými problematikami nového zákona o kyberbezpečnosti, jejich definicí, návrhem variant a jejich vyhodnocením.

Zpráva RIA bohužel obsahuje značné nedostatky, zejména pokud jde o nedostatečné odůvodnění výběru varianty řešení nové legislativy, tak i o dopady, které návrh zákona o kybernetické bezpečnosti provází.

Problematickým aspektem provázejícím návrh zákona o kybernetické bezpečnosti i zprávu RIA je také rozsáhlé využití prováděcích vyhlášek, v nichž Předkladatel zamýšlí definovat řadu důležitých institutů. Toto řešení může být problematické jak z hlediska a kontroly implementace směrnice NIS2, tak i z hlediska posouzení nákladů a finančních dopadů připravované legislativy, když zásadní instrumenty spojené s návrhem zákona mají být upraveny až prováděcími právními předpisy. To lze považovat za velký nedostatek zprávy RIA.

Předkladatel dále popisuje obecně známá rizika spojená s dodavatelským řetězcem (zejm. strategická rizika spočívající v zemi původu dodavatele) a uvádí, že v současnosti neexistuje v ČR komplexní mechanismus, který by umožnil rizika plynoucí z těchto strategických hrozeb pro strategicky významnou infrastrukturu cíleně, účinně a flexibilně vyhodnocovat a mitigovat. Současně uvádí, že napříč státy EU jsou mechanismy pro posuzování a omezení/vynětí rizikových dodavatelů běžné a ČR by v tomto ohledu neměla být pozadu. Ovšem i přes vylíčení důvodů pro zavedení mechanismu není nikde ve zprávě RIA ani důvodové zprávě uvedeno, proč je mechanismus navržen právě v uvedené podobě.

Identifikace dotčených subjektů

Návrh zákona o kybernetické bezpečnosti má dopadnout přinejmenším na 6000 subjektů ze soukromé (především) i veřejné sféry. V mnoha částech textu ZZ RIA chybí detailní identifikace dotčených subjektů. Na str. 28 se se píše o minimálně patnáctinásobném navýšení počtu povinných osob (z dnešních 400), nicméně dle Předkladatele toto číslo není konečné!

Návrh variant řešení

Předkladatel v rámci zprávy RIA předložil návrh <u>následujících variant řešení nové právní úpravy</u>:

- **Varianta I:** Nulová varianta – zachování současného stavu
- **Varianta II**: Transpozice směrnice bez zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce a bez odstranění zjištěných nedostatků a reflexe dosavadních zkušeností (minimální transpozice směrnice)
- **Varianta III:** Transpozice směrnice bez zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce, ovšem při odstranění zjištěných nedostatků a reflexe dosavadních zkušeností
- **Varianta IV:** Transpozice směrnice zároveň zohledňující mechanismus prověřování bezpečnosti dodavatelského řetězce, ovšem bez odstranění zjištěných nedostatků a reflexe dosavadních zkušeností
    - **Podvarianta IVa**: Mechanismus cíleného prověřování bezpečnosti dodavatelského řetězce ve strategicky významné infrastruktuře
    - **Podvarianta IVb**: Mechanismus cíleného prověřování bezpečnosti dodavatelského řetězce ve strategicky významné infrastruktuře se zapojením vlády České republiky
    - **Podvarianta IVc**: Mechanismus plošného prověřování bezpečnosti dodavatelského řetězce ve strategicky významné infrastruktuře

    - **Podvarianta IVd**: Mechanismus cíleného prověřování bezpečnosti dodavatelského řetězce pouze v sektoru elektronických komunikací
- **Varianta V:** Transpozice směrnice, zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce a odstranění zjištěných nedostatků a reflexe dosavadních zkušeností
    - **Podvarianta Va**: Mechanismus prověřování bezpečnosti dodavatelského řetězce ve strategicky významné infrastruktuře
    - **Podvarianta Vb:** Mechanismus cíleného prověřování bezpečnosti dodavatelského řetězce ve strategicky významné infrastruktuře se zapojením vlády České republiky
    - **Podvarianta Vc**: Mechanismus plošného prověřování bezpečnosti dodavatelského řetězce ve strategicky významné infrastruktuře
    - **Podvarianta Vd:** Mechanismus prověřování bezpečnosti dodavatelského řetězce pouze v sektoru elektronických komunikací

Předkladatel z výše uvedených variant navrhuje přijmout variantu V (jejíž realizace si z důvodu rozsahu změn vyžádá zrušení stávajícího zákona o kybernetické bezpečnosti a schválení nového zákona o kybernetické bezpečnosti) **– resp. podvarianty Va či Vb**

Pokud jde o podvarianty Vc a Vd, ty shledal Předkladatel nevhodnými z důvodu neproporčního zvýšení nákladů na straně státu (podvarianta Vc) nebo nedosažení požadovaného cíle (vzhledem k omezení jen na elektronické komunikace – podvarianta Vd).

Vyhodnocení z hlediska dopadů

Dopady na mezinárodní konkurenceschopnost.

Metodika RIA vyžaduje vyhodnotit dopady a faktory ovlivňující mezinárodní hospodářskou konkurenceschopnost České republiky v kontextu hospodářského růstu, dopadů na inovační a investiční činnost a na zaměstnanost.

Předkladatel přitom nijak nevyhodnotil právě dopady související s růstem počtu potřebných zaměstnanců, ačkoli návrh zákona (pokud jej čteme spolu s návrhem prováděcích právních předpisů) předpokládá nejen významný nárůst pracovníků Předkladatele i dalších resortů, ale především s vysokou mírou pravděpodobnosti i u povinných subjektů. Povinné osoby, které budou předmětem “vyšších povinností” budou muset zavést v rámci své organizační struktury nové role (manažer kybernetické bezpečnosti, architekt kybernetické bezpečnosti, auditor kybernetické bezpečnosti a podobně). Předkladatel se nijak nevypořádal s tím, zda povinnosti, které navrhuje uvalit na povinné osoby budou vůbec splnitelné vzhledem k napjaté situaci na trhu práce a zda i on sám bude mít dostatek pracovníků na efektivní vymáhání regulace.

Rozsah regulace musí zohledňovat i tento faktor, tedy zda ji bude mít kdo provádět. Zohlednění by mělo být součástí vyhodnocení jednotlivých variant, a to včetně stanovení většího množství variant "mechanismu bezpečnosti dodavatelského řetězce", kde předkladatel počítá fakticky jen s jednou variantou, která postihuje různá odvětví, ale nikoli s variantami širšího či užšího zacílení mechanismu.

Dopady na státní rozpočet a ostatní veřejné rozpočty

Předkladatel uvádí, že **nově navýšené náklady** budou muset být promítnuty do budoucích rozpočtů povinných subjektů (a to i těch, které jsou již nyní povinnými osobami dle zákona o kybernetické bezpečnosti). Současně však uvádí, že v zásadě není schopen finanční dopady odhadnout, výši finančních dopadů není možné předem stanovit a vytvořené odhady tak mají nízkou vypovídající hodnotu.

Hrubý odhad stavějící výlučně na nákladech implementace předchozích právních předpisů činí 800.000 – 1.500.000 Kč vůči jednomu zabezpečovacímu systému (výpočet sám není ze zprávy RIA zcela srozumitelný). Dotčené subjekty poskytující veřejnosti srovnatelné služby (Předkladatel zde nesděluje které, ani typově) v rámci dotazníkového řízení sdělily rozptyl nákladů přinejmenším od 6.000.000 Kč do 11.000.000 Kč za organizaci (viz s. 4 zprávy RIA). I z uvedeného je zřejmé, že hrubé odhady (kde se o ně alespoň pokouší) se zcela míjí s realitou.

Dopady na státní rozpočet pak samozřejmě může (a zřejmě bude) mít i zvýšení nákladů poskytovatelů strategicky významné služby z řad veřejné správy – tyto náklady však Předkladatel nijak blíže nekomentuje, ani je nevyčísluje (ani odhadem).

Dopady na podnikatelské prostředí

Vyhodnocení dopadů na podnikatelské prostředí je zcela nedostatečné. Byť Předkladatel přiznává, že náklady regulovaných subjektů se zvýší, opět tvrdí, že výši finančních dopadů není možné předem stanovit a veškeré předchozí požadavky na jejich vyčíslení vedly k vytvoření odhadů s nízkou vypovídající hodnotou (viz s. 7 zprávy RIA). Překladatel měl k dispozici mnoho možností, jak přistoupit ke zjištění reprezentativních dat týkajících se (finančních) dopadů na podnikatelské prostředí, včetně provedení vlastního reprezentativního průzkumu mezi potenciálními povinnými subjekty, či studie od externího dodavatele, která by pomohla vyčíslit předpokládané náklady připravované legislativy. Předkladatel mohl také využít jako vhodné přiblížení povinností, které budou plynout z plnění povinností ze směrnice NIS 2, například soulad s normou ISO/IEC 27001 a data z registru smluv subjektů, které jsou podle této normy certifikované. Tím mohl zhodnotit dopad nejen v samotném zavedení povinností, ale i k jejich udržování, což bude představovat také nemalý náklad.

Návrh zákona o kybernetické bezpečnosti má dopadnout přinejmenším na 6000 subjektů ze soukromé (především) i veřejné sféry. Za takové konstelace není zcela jistě vhodné, aby Překladatel tyto subjekty zhodnotil pouze větou že „*není z pohledu regulátora možné vyčíslit dopady na rozpočty v podobě absolutního čísla, které by bylo dostatečně přesné. Z obdržených vyplněných dotazníků vyplýval extrémní rozptyl těchto předpokládaných nákladů*." (viz s. 4 zprávy RIA) Pokud z dotazníků vyplýval extrémní rozdíl, proč nebyl ve zprávě RIA uveden? Závěrem této analýzy totiž klidně může být, že část subjektů je na implementaci připravena a část nikoliv.

V rámci zprávy RIA také zcela absentuje posouzení dopadu na OSVČ a malé a střední podniky, které zásady hodnocení RIA výslovně požadují.

Hodnocení dopadu na podnikatelské prostředí je tedy zcela nedostatečné a není v souladu se zásadami hodnocení RIA.

Dopady na spotřebitele

Předkladatel uvádí, že nepředpokládá žádné přímé dopady na spotřebitele, ale zároveň uvádí, že lze očekávat tlak regulovaných orgánů na promítnutí nákladů na zavádění bezpečnostních opatření do cen služeb. Toto jednoznačně představuje negativní vliv na spotřebitele, který se promítne ve zvýšení cen, které by ze strany Předkladatele měly být alespoň odhadem vyčísleny i proto, že regulované služby se dotýkají i odvětví, která zasahují prakticky celou společnost (jde např. telekomunikace, energetika, potravinářství).

Zhodnocení dopadů na spotřebitele v podobě předložené zprávou RIA nelze považovat za dostatečné a v souladu se zásadami hodnocení RIA.

Přezkum účinnosti regulace je stručný, chybí podrobnější popis sledovaných ukazatelů a zcela chybí sledování indukovaných nákladů na povinné subjekty.

Konzultace a zdroje dat

Dle ZZ RIA se konzultace a zdroje dat zdají být dostatečné, a kromě výčtu úřadů a organizací předkladatel dokonce konstatuje, že opakovaně vyzýval odbornou i širokou veřejnost k zasílání podnětů týkajících se budoucí regulace – ať už formou obecné výzvy na svých internetových stránkách, tak zřízením speciální internetové stránky zaměřené na transpozici směrnice do českého právního řádu.

III. Shrnutí připomínek

Potřeba transpozice směrnice NIS2 je neoddiskutovatelná, předložená zpráva RIA však nedává jasnou odpověď na otázkou, zda je celková koncepce navržené právní úpravy proporcionální a zda navržená varianta a znění mechanismu je opravdu odůvodněné.

Kromě výše uvedených nedostatků je zásadním problém této ZZ RIA samotné pojetí metodického zpracování, kdy není zohledněno, že faktické dopady jsou velmi závislé na tom, jak předkladatel přistoupí k zpracování vyhlášek. Není možné vyloučit, že tyto vyhlášky mohou mít podstatný dopad na regulační potenciál připravovaného zákona.

Zpráva RIA je zpracována nedostatečným způsobem. Doporučujeme se zaměřit zejména na tyto nedostatky:

- Dopad na povinné subjekty, a to i finanční dopad dle rozdělení vyšších a nižších povinností.
- Zdůvodnění návrhu mechanismu bezpečnosti dodavatelského řetězce, především v porovnání s ostatními podobnými "mechanismy" v ostatních zemích EU.
- Lépe a detailněji zpracovat dopady na jednotlivé zasažené subjekty – na malé a střední podniky (především v oblasti telekomunikací), sociální dopady (promítnutí zvýšených nákladů do cen u sociálně citlivých komodit jako energie, telekomunikace nebo potraviny).
- Legislativní rada vlády by se pak měla zabývat otázkou, zda je možné zákon naplnit prostřednictvím vyhlášek (které stanoví kdo je regulovaný subjekt a jak, jaké budou jejich povinnosti a podobně). Je nutné upozornit na to, že předkladatel v předběžném přehledu dopadu vyhlášek požaduje výjimku z analýzy dopadů regulace (RIA) s tvrzením, že dopady jsou již dostatečně postižené v RIA k samotnému zákonu – což jak uvádíme i v tomto stanovisku není zcela pravda.
- Doporučujeme v rámci nulových variant, tedy zachování současného stavu, doplnit kvantifikaci, jaká rizika mohou nastat, pokud by skutečně současný stav přetrvával. Využít lze např. odhady dopadů rizika realizace sankcí vůči zemím, které jsou v dodavatelském řetězci a co by znamenaly škody způsobené absencí vstupů ze zemí pod sankcemi (např. určitou analogií může být kvantifikace dopadů stávajících balíků sankcí vůči RF).
- Dopracovat Přezkum účinnosti regulace v souladu s doporučeními výše.

IV. Závěr

Pracovní komise Legislativní rady vlády pro hodnocení dopadů regulace **doporučuje** Legislativní radě vlády, **aby byl Návrh zákona o kybernetické bezpečnosti a Návrh zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti, doporučen vládě ke schválení** za předpokladu zohlednění výše uvedených **připomínek.**

Vypracoval:

Marek Ondroušek

Mgr. et Mgr. Marek Havrda, MA, MPA, Ph.D.

předseda komise