



V Praze 18. září 2024

Čj.: OVA 634/24

Stanovisko

k

Návrh zákona o odolnosti subjektů kritické infrastruktury a o změně dalších zákonů (zákon o kritické infrastruktuře)

I. Úvod

Hlavním důvodem pro zpracování návrhu zákona je nutnost zapracovat do právního řádu České republiky požadavky směrnice CER, přičemž v souladu s právem EU musí být směrnice CER zapracována do českého právního řádu ve stanovené transpoziční lhůtě, která činí 21 měsíců od nabytí platnosti této směrnice (tj. do 17. října 2024). Nové požadavky, vyplývající především ze směrnice CER, vedou k tomu, že návrh nového zákona musí zohlednit především tyto náležitosti:

- změnu přístupu od určování fyzických prvků kritické infrastruktury k určování subjektů kritické infrastruktury poskytujících základní služby,
- požadavky na zpracování dokumentace na národní úrovni (posouzení rizik, strategie),
- další požadavky na subjekty kritické infrastruktury,
- zpracování posouzení rizik,
- zavedení opatření k zajištění jejich odolnosti a jejich promítnutí do plánu odolnosti,
- požadavky na hlášení incidentů,
- intenzivnější sdílení informací mezi státní správou a soukromým sektorem,
- systém ověřování spolehlivosti kritických pracovníků subjektů kritické infrastruktury,
- provázání povinností se sankcemi,
- zohlednění problematiky dodavatelských řetězců,
- provázání s návrhem nového zákona o kybernetické bezpečnosti a nařízením Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011 (dále jen „nařízení DORA“),
- vznik nového informačního nástroje v podobě Portálu kritické infrastruktury.

II. Připomínky a návrhy změn

Definice problému

Definice problému jsou v ZZ RIA uváděny velmi obecně, formou nijak nepodložených a bezobsažných výroků („některé nedostatky“, „určitá negativa“...). Definovaný problém nemá

žádnou strukturu, pojmenované příčiny, a není kvantifikován. V kapitole také dochází ke zmatení toho, co je problém (neuspokojivý stav, který je potřeba řešit) s navrhovanými řešeními.

Na str. 11 ZZ RIA: *“Dalším nedostatkem souvisejícím s decentralizací současného systému kritické infrastruktury je výrazná disproporcionalita odvětvových kritérií v rámci jednotlivých odvětví. Nejmarkantněji je tento nedostatek patrný v odvětví zdravotnictví a v odvětví potravinářství a zemědělství, kde od roku 2010 nedošlo vlivem nevhodně nastavených kritérií k určení žádného prvku kritické infrastruktury.”*

Proč jsou právě tato odvětví problémem a proč zde nedošlo k žádnému určení prvků kritické infrastruktury? Jak byla tato kritéria vůbec vyhodnocena? Opravdu se jedná jen o tato tři odvětví?

“Stávající systém kritické infrastruktury je také příliš zaměřený na významnost jednotlivých prvků kritické infrastruktury, čímž jsou upozadřovány méně významné prvky, které však spolu mohou vytvářet významné systémy tvořené z více prvků.”

Zde doporučujeme přepsat do srozumitelnější formy, aby bylo jasné i pro člověka, který není odborníkem na kybernetickou bezpečnost

Na str. 12. ZZ RIA: *„Z důvodu zakotvení oficiální změny názvů operačních a informačních středisek IZS je nutná změna znění § 5 odst. 1 předmětného ustanovení upravujícího problematiku stálých orgánů pro koordinaci složek IZS. Jedná se toliko o změnu názvosloví bez dopadu na fungování IZS.”*

Od této části stále v bodě definice problému jsou popisovány specifické změny současného právního stavu, což do této části není vhodné.

Popis existujícího právního stavu v dané oblasti

Popis na str. 13. ZZ RIA je dostačující, ovšem na následující straně se z popisu existujícího právního stavu dostáváme spíše do definice problému a popisu cílového stavu. Proto doporučujeme tuto část vyjmout a přepsat do patřičných částí.

Identifikace dotčených subjektů

Na str. 15 ZZ RIA: *„Pozitivně dotčenými subjekty z hlediska povinností, které právní úprava zavádí mohou reálně být všechny subjekty kritické infrastruktury. Důvodem k tomuto tvrzení je fakt, že díky nutnosti zajistit svou odolnost plynoucí z návrhu zákona, subjekty kritické infrastruktury obecně sníží pravděpodobnost vzniku incidentu v rámci své organizace a stejně tak zmírní dopady případných incidentů. Tato skutečnost se vztahuje rovněž na subjekty kritické infrastruktury, které budou určeny v odvětví Veřejná správa.”*

Návrh zákona nepředpokládá negativní vliv na subjekty, neboť primárním cílem je posílení odolnosti, které má jasně pozitivní charakter. Negativitu tak lze spatřovat například ve finančních či personálních nákladech na opatření k zajištění odolnosti, v jejichž zavedení lze ale spatřovat jasné benefity pro dotčené subjekty a v této rovině i pro fungování státu, a to v podobě zajištění poskytování základních služeb. Zajištění kontinuálního poskytování základních služeb je hlavním cílem při aplikaci návrhu zákona.”

Zde předkladatel v textu implikuje, že by měl být dopad na všechny aktéry stejný, což je velmi nerealistické (jak sám předkladatel zmiňuje u různých odvětví: *„Nejmarkantněji je tento*

nedostatek patrný v odvětví zdravotnictví a v odvětví potravinářství a zemědělství, kde od roku 2010 nedošlo vlivem nevhodně nastavených kritérií k určení žádného prvku kritické infrastruktury“.)

Dopad se bude také zásadně lišit v závislosti na velikosti subjektů a na současné míře přípravy – zda budou subjekty ochranu budovat zcela nově na zelené louce, nebo zda ji již mají zajištěnou v dostatečně (nebo vyšší) míře.

Rizika

Zmiňují se pouze rizika nepřijetí a to opět pouze ve velmi obecné rovině.

Zcela se opomíjí rizika spojená s přijetím úpravy, nebo rizika, která mohou ohrozit implementaci návrhu – jako je například personální zajištění pro všechny dotčené subjekty v situaci, kdy je na trhu extrémní nedostatek odborníků, zabývajících se kybernetickou bezpečností. Logicky potom také chybí návrhy opatření, která mají rizika maximálně snížit.

Návrh variant řešení

Návrh variant řešení je nejen zcela formalistický, bez věcné logiky a obsahu, ale navíc neodpovídá ani tomu, co sám předkladatel ve shrnutí ZZ RIA uvádí. Ve shrnutí je uvedeno (a je to asi pravda), že návrh jde nad rámec požadavků směrnice. Varianty nabízí možnost směrnici neimplementovat, implementovat ji částečně, nebo úplně. Navrhovaný předpis tedy ve vyhodnocení variant úplně chybí.

Varianty jsou popsány naprosto obecně, není zřejmé, co se má v rámci které stát. Návrh variant je proto nefunkční z hlediska využití jako podkladového materiálu pro rozhodování.

V textu není nikde uvedeno, jaké konkrétní návrhy řešení jsou dány potřebou implementace směrnice a kde jde návrh nad rámec jejích požadavků.

Vyhodnocení nákladů a přínosů

Náklady a přínosy všech variant je třeba popsat, rozdělit podle typu subjektů, kterých se budou týkat, a kvantifikovat.

U dopadů na soukromý sektor je třeba rozlišit subjekty dle odvětví, velikosti a míry připravenosti na změny. Dále odhadnout míru nutných investic (kvantifikovat náklady pro subjekty kritické infrastruktury) a odhad zátěže a reakce subjektů na takové náklady.

Identifikované dopady je třeba vyhodnotit pro všechny uvažované varianty na základě společných kritérií. Jedině tak je možné mezi sebou varianty řešení porovnávat a vyhodnocovat jejich vhodnost.

Všechny odhady dopadů je třeba podložit o metodě výpočtu a zdrojích dat. Pokud někde udáváme například navýšení o procentuální část, je třeba říci, co to znamená Viz např. následující, ničím nepodložené údaje:

“Náklady na zavedení Portálu kritické infrastruktury, včetně pořízení potřebného hardwaru v rámci Ministerstva vnitra, byly vyčísleny na částku 6 000 000 Kč. Tato částka bude z 90 % financována

z operačního programu EU Fondu pro vnitřní bezpečnost. Organizační a personální kapacity na jeho provoz budou pokryty z aktuálních zdrojů.”

“Finanční náklady na Informační systém krizového řízení nepřesáhnou částku 197 000 000 Kč. Tato částka bude financována z operačního programu EMAS/AMIF a rozpočtu Ministerstva vnitra – generálního ředitelství hasičského záchranného sboru České republiky.”

“Náklady spojené s přijímáním opatření na zvyšování odolnosti se budou odvíjet od již existujících opatření, obecně jsou v průměru odhadovány v řádech statisíců až jednotek milionů korun”

“Vzhledem k této skutečnosti je odhad finančních nákladů značně obtížný, nicméně za reálný lze považovat požadavek na navýšení ročního rozpočtu kapitoly Správa státních hmotných rezerv, konkrétně části určené k pořízování věcných zdrojů v systému hospodářských opatření pro krizové stavy o 20 %.”

“V případě přijetí nových, dosud nezavedených, opatření bude finanční částka odpovídat typu a rozsahu opatření, obecně lze kalkulovat s průměrnou částkou v řádech statisíců či jednotek milionů korun.”

Přínosy

Přínosy jsou definovány zcela obecně bez kvantifikace. Tuto část doporučujeme rozepsat více do detailu a ke každé variantě i uvést jasně definované přínosy. Je třeba si uvědomit, že i varianta 1 – nulová varianta má svůj jasný přínos a to, že nedojde k nákladům, které jsou popsány v ostatních variantách. Tento je třeba porovnávat s přínosy schválení a implementace navrhovaných opatření

Vyhodnocení nákladů a přínosů variant

Vyhodnocení dopadů je třeba provádět pomocí srovnatelných kritérií jednotlivých přínosů a nákladů.

Uvádění ničím nepodložených výroků typu *“Investice do odolnosti subjektů kritické infrastruktury budou mít pozitivní dopad na společnost a státní rozpočet jako celek. Z teorie řízení bezpečnosti lze uvést pravidlo, že 1 EUR vynaložené na prevenci má přínos 5 EUR vynaložených na řešení krizové situace a jejích dopadů.”* kvalitu textu ZZ RIA nepřispívá. Doporučujeme uvést zdroj a jak se tento model aplikuje na tuto navrhovanou regulaci. Dále pak jestli toto obecné pravidlo platí pro všechny regulované subjekty (například podle míry již existujícího zabezpečení).

Zavádění nebo zlepšování jakýchkoliv prvků bezpečnosti, jak kybernetické, tak fyzické je potřeba analyticky vždy velmi dobře podložit v datech, a to především v přínosech a nákladech pro dané subjekty/stát. Dosáhnout 100 % ochrany nikdy nelze, a proto je velmi podstatné najít přiměřený náklad k dostatečnému přínosu. Čím více se totiž v rámci ochrany budeme blížit číslu 100 %, tím náklady budou vzrůstat ne lineárně, ale exponenciálně.

Předkladatel píše, že: *„S variantou I a II nejsou spojeny žádné přínosy...”* (str. 21) Jak již bylo řečeno výše, přínosy varianty 1 jsou například ty, že subjekty nebudou čelit zvýšeným nákladům. Pokud již totiž předkladatel ví, že jim definovaná varianta 1 a 2 nemají žádná přínosy, proč si vůbec takové varianty vytvořil?

Stanovení pořadí variant a výběr nejvhodnějšího řešení

Čistě formální, vhodné řešení by mělo být nalezeno pomocí reálného srovnání dopadů jednotlivých variant, podle společných kritérií. Doporučí uvést na základě jaké metody bylo výběru varianty III dosaženo (například multikriteriální analýza či CBA).

U vybrané varianty je napsáno, že *“obsahuje přijatelný poměr nezbytných nákladů a očekávaných přínosů”*. Jak vysoké jsou ty náklady, jak velké jsou přínosy, jaký poměr je přijatelný a jaký už nepřijatelný, jaký je poměr nákladů a přínosů u dalších dvou variant?!

Implementace

Jakým způsobem byla zvolena pokuta “do výše zlomku z čistého obratu”? Jak bude dopadat na různé typy subjektů?

Přezkum účinnosti regulace

Popis přezkum účinnosti regulace je velmi obecný, navrhované indikátory jsou uvedeny bez bližší časové specifikace a určení minimální hranice, která bude chápána jako efektivně zavedená regulace.

Konzultace a zdroje dat

Doporučujeme podložit a uvést zdroje k obecným proklamacím v textu a uvést, v čem konkrétně se promítla konzultace s jednotlivými zájmovými stranami.

III. Shrnutí připomínek ke zprávě z hodnocení dopadů regulace (zpráva RIA)

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

- Konkrétně a podloženě definovat řešený problém a na základě toho navrhovat reálné, konkrétní a smysluplné varianty řešení.
- Zřetelně a jasně popsat, jaká navrhovaná opatření jsou výsledkem čisté implementace směrnice a co jde nad její rámec
- V ZZ RIA se věnovat všem dopadovým ustanovením, která jsou v zákoně (např. paragraf 14, který může mít zásadní dopady a není v ZZ RIA nijak reflektován)
- Dopady navrhovaných variant řešení kvantifikovat, podložit daty a srovnat na základě společných, konkrétních kritérií. Rozlišovat dopady na různé typy aktérů.
- Dále doporučujeme detailněji vyhodnotit rizika, která by nastala v případě nepřijetí této legislativní úpravy mimo argument možného infringementu

IV. Závěr

Pracovní komise Legislativní rady vlády pro hodnocení dopadů regulace **doporučuje** Legislativní radě vlády, **aby projednávání návrhu zákona o odolnosti subjektů kritické**

infrastruktury a o změně souvisejících zákonů, přerušila za účelem přepracování návrhu předkladatelem ve smyslu výše uvedených zásadních připomínek

Vypracoval:
Marek Ondroušek

Mgr. Ing. Lucie Zapletalová, M.A.
předsedkyně komise