UNIVERZITA J. E. PURKYNĚ V ÚSTÍ NAD LABEM
Fakulta sociálně ekonomická

UNIVERZITA J. E. PURKYNĚ V ÚSTÍ NAD LABEM

Posouzení Zprávy o hodnocení dopadů regulace (RIA) k návrhu nového Zákona o kybernetické bezpečnosti

V Ústí nad Labem dne 9. března 2024

Obsah

Úvod 3
Použité materiály 3
Otázky zadavatele, dle kterých posuzujeme RIA k novému ZKB 4
Executive summary 5
Posouzení 6
1. Otázka 1: Odpovídá předložená RIA významu regulace? 6
2. Je RIA zpracovaná v souladu s doporučením vlády/NERVu ohledně vyhodnocení reálných dopadů regulace? 9
Zpráva neobsahuje adekvátně stanovené cíle ani parametry, dle kterých se bude vyhodnocovat úspěšnost regulace 11
3. Jak se RIA staví k průběžnému posuzovaní dopadů regulace? Má ambici například průběžně vyhodnocovat, zdali důvody regulace ještě trvají, anebo již pominuly a jak se změna takového stavu projeví na požadované administrativní zátěži směrem na podnikatele? 13
Úřad se nepokusil o průkazný odhad počtu dotčených subjektů 14
Úřad nevyhodnotil dostatečně dopady na výdajovou stranu veřejných rozpočtů 16
Úřad nebere v úvahu dopad na příjmovou stranu státního rozpočtu 18
4. Je z předložené RIA zřetelná vysoká úroveň analyticko-výzkumné odbornosti? 20
Úřad nevyužil dostupné metodiky pro stanovení nákladů regulace 20
Úřad nevyužil alternativní způsoby, jak kalkulovat náklady pro budoucí regulované subjekty 20
Úřad neplánuje podrobit prováděcí vyhlášky hodnocení dopadů regulace 22
5. Využívá RIA všechna relevantní dostupná ekonomicko-analytická data pro správné posouzení dopadů regulace? 24
Úřad reguluje nad rámec směrnice 25
6. Doporučuje hodnotitel dopracovat RIA v nějakých konkrétních oblastech a pokud ano, v jakých? 28
Závěr 29

Úvod

Výzkumné centrum Laboratoře behaviorálních studií (LABS) Fakulty sociálně-ekonomické Univerzity Jana Evangelisty Purkyně bylo požádáno zadavatelem, Asociací provozovatelů mobilních služeb sítí (APMS), o posouzení kvality a provedení Závěrečné zprávy o hodnocení dopadů regulace (RIA) (dále jen "Zpráva") k novému Zákonu o kybernetické bezpečnosti. Tento zákon je z hlediska dopadů na podnikatelské prostředí jednou z nejvýznamnějších norem, které by měl Parlament České republiky schvalovat v tomto volebním období, případně v příštím volebním období (pokud se nezdaří do voleb v roce 2025 či pokud dojde k volbám předčasným).

Hodnocení dopadů regulace (Regulatory Impact Assessment) je dokument, který analyzuje dopady navrhovaného právního předpisu nebo regulace na různé oblasti, jako jsou hospodářství, životní prostředí, zaměstnanost a další. Cílem těchto zpráv je poskytnout komplexní hodnocení možných důsledků a efektivity navrhovaného opatření před jeho přijetím. Tato analýza obvykle zahrnuje odhadované náklady a přínosy, možné alternativy řešení a konzultace s dotčenými stranami. Hodnocení dopadů regulace je navíc důležité pro kvalifikované rozhodnutí politické reprezentace, zda návrh zákona akceptovat či ne v podobě, ve které ho navrhovatel předkládá vládě a ve které jej poté vláda předkládá parlamentu pro schválení. Volení zástupci lidu musejí mít maximum informací o dopadu na jejich voliče, na ekonomiku a na společnost k tomu, aby mohli učinit kvalifikované rozhodnutí o tom, zda zákon schválit, změnit či odmítnout.

Dokument je koncipován jako odpovědi na zadavatelem formulované otázky – zhotovitel objektivně předkládá odpovědi vč. zdůvodnění a citací bez primárního záměru zasahovat do legislativního procesu.

Použité materiály

Tento posudek vychází z poslední dostupné verze Zprávy z 22. ledna 2024, která se nachází na Portále informačního systému ODok Úřadu vlády České republiky[1]. K posouzení, zda materiál odpovídá svou kvalitou a provedením požadavkům, které na něj kladou příslušná pravidla a zásady, jsme použili dostupné dokumenty a metodiky na stránkách Úřadu vlády ČR.[2]

[1] https://odok.cz/portal/veklep/material/ALBSCSSFKU7S/
[2] https://ria.vlada.cz/dokumenty/

Otázky zadavatele, dle kterých posuzujeme RIA k novému ZKB

Na základě formulovaného zadání měl zhotovitel za úkol za využití dostupných materiálů, dat a akademického know-how odpovědět na následujících šest otázek:

1. Odpovídá předložená RIA významu regulace?
2. Je RIA zpracovaná v souladu s doporučením vlády/NERVu ohledně vyhodnocení reálných dopadů regulace?
3. Jak se RIA staví k průběžnému posuzovaní dopadů regulace? Má ambici například průběžně vyhodnocovat, zdali důvody regulace ještě trvají, anebo již pominuly, a jak se změna takového stavu projeví na požadované administrativní zátěži směrem na podnikatele?
4. Je z předložené RIA zřetelná vysoká úroveň analyticko-výzkumné odbornosti?
5. Využívá RIA všechna relevantní dostupná ekonomicko-analytická data pro správné posouzení dopadů regulace?
6. Doporučuje hodnotitel dopracovat RIA v nějakých konkrétních oblastech a pokud ano, v jakých?

Odpovědi na jednotlivé otázky tvoří jednotlivé kapitoly následujícího textu.

Executive summary

Tento posudek analyzuje Závěrečnou zprávu o hodnocení dopadů regulace (RIA) k návrhu nového Zákona o kybernetické bezpečnosti na základě otázek, které předložil Zadavatel posudku k zodpovězení. Zprávu hodnotíme oproti plnění příslušných manuálů, vodítek a pravidel pro provádění RIA, které jsou veřejně dostupné na stránkách Úřadu vlády ČR. Docházíme k závěru, že Zpráva vypracovaná Národním úřadem pro kybernetickou a informační bezpečnost neposkytuje dostatečný podklad dalším orgánům, které budou zákon projednávat, aby se dokázaly kvalifikovaně rozhodnout, zda jej schválit, či v některých ustanoveních měnit.

Zpráva především neobsahuje konkrétní přehled subjektů, které budou na základě nového zákona poskytovateli regulovaných služeb a budou tedy muset uvést své systémy a procesy do souladu s tímto zákonem, což pro ně bude znamenat náklady. Zpráva neobsahuje také odhad těchto nákladů a odhad (alespoň formou nějakého rozpětí) agregovaných nákladů, případně nákladů na jednotlivá regulovaná odvětví, aby bylo možné zhodnotit dopad na podnikatelské prostředí, sociální dopady a dopady na spotřebitele. Ve zprávě zcela absentuje vyhodnocení dopadu na malé a střední podniky, které pravidla pro hodnocení dopadů regulace vyžadují – většina subjektů, na které zákon dopadne, budou přitom z logiky věci malé a střední podniky (zákon je sice primárně jako implementace příslušné evropské směrnice zaměřený na střední a velké podniky, ale v odvětví poskytování služeb/sítí elektronických komunikací má ambici dopadnout na všechny podnikatele bez rozdílu velikosti, což v české realitě znamená bezmála šest tisíc převážně malých podniků a mikropodniků).

Předkladatel také nevyhodnotil dopady ani na výdajovou stranu státního rozpočtu (řada povinných subjektů budou nově regulované organizační složky státu, například státní zastupitelství či soudy, a přijetí nové právní úpravy bude navíc vyžadovat zavedení nových organizačních postupů a zavedení nových rolí v organizacích, což vyvolá personální požadavky), ani na příjmovou stránku rozpočtu, kdy především část zákona týkající se prověřování dodavatelského řetězce může ve finále znamenat významné dodatečné a nečekané investice u subjektů, které jsou zároveň významnými plátci daně z příjmu právnických osob. Pro rozhodnutí by bylo vhodné znát dopady nutných opatření požadovaných NIS2, ale i lokálních nepovinných požadavků nad rámec směrnice.

Předkladatel také zákon koncipuje jako „podvozek“, u kterého konkrétní regulované subjekty a konkrétní opatření, které budou muset plnit, bude definovat až formou vyhlášek. K nim ale dle Plánu vyhlášek na rok 2024 neplánuje už provádět hodnocení dopadů regulace, což fakticky znamená, že reálné dopady kroků státu v této oblasti na podnikatele, veřejnou sféru i spotřebitele nebudou vyhodnoceny nikde.

Posouzení

1. Odpovídá předložená RIA významu regulace?

Ne, předložená RIA svým rozsahem a obsahem (tj. svou kvalitou) neodpovídá významu, který navrhovaná regulace představuje pro veřejný i soukromý sektor. Kybernetická bezpečnost je v dnešním světě jedna z hlavních priorit vzhledem k rostoucí digitalizaci a propojenosti společnosti. Dnešní kybernetické hrozby dosahují bezprecedentní úrovně, což je úzce spojeno s rapidním rozvojem digitální společnosti. Pozorujeme trend, kdy se mnoho tradičních bezpečnostních hrozeb přesouvá či alespoň částečně transformuje do kyberprostoru, čímž vznikají nové specifické hrozby pro toto prostředí. Dochází také k prolínání různých typů hrozeb a jejich hybridizaci, kterou posiluje dynamika a rozsah kyberprostoru a moderní technologie. Všechny tyto hrozby sdílejí jedno společné – jsou natolik složité, že staví do zkoušky důvěru veřejnosti ve stát a jeho instituce. Dle Národní strategie kybernetické bezpečnosti České republiky na období 2015 až 2020 "*Kybernetická bezpečnost představuje souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v České republice, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost. Kybernetická bezpečnost pomáhá identifikovat, hodnotit a řešit hrozby v kyberprostoru, snižovat kybernetická rizika a eliminovat dopady kybernetických útoků, informační kriminality, kyberterorismu a kybernetické špionáže ve smyslu posilování důvěrnosti, integrity a dostupnosti dat, systémů a dalších prvků informační a komunikační infrastruktury*."[3]

Z vlastních strategických dokumentů předkladatele vyplývá, a sám předkladatel si zcela jistě uvědomuje, že řešení kybernetické bezpečnosti není jen o vypracování legislativního znění, ale o celé řadě dílčích kroků, které jsou naprosto podstatné k zajištění co nejbezpečnějšího prostředí v rámci kyberprostoru. K tomu, aby bylo dosaženo cíle co nejvíce bezpečného kyberprostoru, je nutné mít nejen připravený zákon, ale zároveň s ním mít i připravenou brilantní analýzu očekávaného dopadu, ale především také náklady na tato opatření.

Od 1. 11. 2007 vznikla v ČR povinnost provádět hodnocení dopadů regulace tzv. Metodou RIA (Regulatory Impact Assessment nebo Regulatory Impact Analysis). Byly též schváleny tzv. Obecné zásady pro hodnocení dopadů regulace, což je soubor pravidel a metodik, které

[3] https://nukib.gov.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2015-2020.pdf, str. 5

stanovují postup ústředních orgánů státní správy při vypracování analýzy dopadů regulace (RIA). Tyto zásady jsou navrženy tak, aby poskytovaly strukturovaný rámec a usnadnily hodnocení dopadů navrhovaných právních předpisů či politik. Jedním z klíčových aspektů RIA je přezkum alternativních možností, které jsou k dispozici pro dosažení cílů navrhované regulace. To zahrnuje zkoumání nejen přínosů, ale také nákladů a rizik spojených s každou možností. RIA se také zabývá otázkami efektivity a účinnosti navrhovaných opatření, přičemž se snaží najít rovnováhu mezi dosažením požadovaných cílů a minimalizací nežádoucích vedlejších účinků.

Další důležitou součástí RIA je zapojení zúčastněných stran a veřejnosti do procesu. To zahrnuje konzultace s dotčenými subjekty, jako jsou podniky, nevládní organizace, odborníci a občané, aby se získaly různé perspektivy a informace. Tento dialog může pomoci identifikovat potenciální problémy a možnosti zlepšení navrhované regulace.

RIA také zahrnuje hodnocení dopadů na různé skupiny obyvatelstva, včetně zranitelných skupin, a zkoumání možných nerovností nebo nespravedlností, které by mohly vzniknout v důsledku přijetí nových pravidel. Tento proces pomáhá zajistit, že regulace bude spravedlivá a přínosná pro celou společnost.

Jak uvádí Vzdělávací manuál pro hodnocení dopadů regulace (RIA), jednou ze základních součástí procesu RIA je správné definování problému. Cílem je identifikace záležitostí, které mají být vyřešeny návrhem právního předpisu. Proto je zapotřebí jasně analyzovat současný stav a zdůvodnit, co a proč by se mělo změnit. Lze uvést, zda se jedná o problém jednorázový nebo opakující se. Nutné je také zvážit, zda se k problému nevážou i další problémy související, které je potřeba rovněž analyzovat.

Hodnocení dopadů metodou RIA lze posuzovat z tří perspektiv. První perspektivou je hodnocení navrhované regulace, známé jako hodnocení **Ex ante**, druhou je hodnocení již platné nebo zavedené regulace, označované jako hodnocení **Ex post**. Některé analýzy nákladů a přínosů provádějí také hodnocení během procesu. V našem případě v ex ante hodnocení měl Úřad disponovat již řadou vstupních dat, protože nejde o úplně novou regulaci, ale fakticky o rozšíření dnes platného zákona o kybernetické bezpečnosti, který je implementací směrnice NIS. Zpracovatelé uvádí, že “odhady hovoří o minimálně 6 000 povinných orgánech a osobách, což je skoro desetinásobný nárůst regulovaných subjektů. V takovém případě je naprostou nutností, aby RIA obsahovala nejen informace o počtech a druhu subjektů, ale i především ekonomické dopady pro nově regulované subjekty. Z navrhovaných tezí vyhlášek je totiž patrné, že řada z nich spadá mezi ty podniky, které patří

mezi odvětví, která se dají označit za sociálně citlivé (výrobci potravin, výrobci a dodavatelé energií atd.).

Jak ukazujeme níže, Zpráva z tohoto hlediska neposkytuje odpovědi na základní otázky, na které by měla odpovídat, tedy především na to, jaké dopady bude mít nový zákon o kybernetické bezpečnosti na povinné subjekty a na které subjekty vlastně dopadne a s jakou intenzitou. Je to důležité, protože **dopady navrhovaných variant musí být vždy prezentovány transparentně a srozumitelně tak, aby mohly sloužit jako základ pro politická rozhodnutí o přijetí nebo nepřijetí návrhu právního předpisu či jeho přijetí v jiné podobě.**

2. Je RIA zpracovaná v souladu s doporučením vlády/NERVu ohledně vyhodnocení reálných dopadů regulace?

Ne, RIA svým zpracováním neodpovídá ani doporučením NERV, ani legislativním pravidlům vlády. Zpráva má významné nedostatky, zejména v nedostatečném zdůvodnění výběru řešení nové legislativy a dopadů navrhovaného zákona o kybernetické bezpečnosti. Formální chyby jsou patrné již od začátku samotného dokumentu. V souhrnu závěrečné zprávy například není jasně uvedeno, že návrh přesahuje požadavky stanovené předpisem EU, jak je obvyklé. Je důležité toto explicitně uvést, protože některé části navrhované právní úpravy jdou nad rámec předpisu EU, což není v zprávě RIA ani patřičně zdůrazněno, ani připuštěno.

Vhodné je také porovnat Zprávu s tím, jaké pokyny pro její zpracování dává Vzdělávací manuál pro hodnocení dopadů regulace (RIA)[4]. Ten uvádí k transpozici směrnice následující:

> *Povinnost transponovat do národního právního řádu směrnici EU však nesmíme zaměňovat s problémem, který je třeba řešit. I definice problému musí odpovídat tomu, že daná směrnice reaguje na nějaký skutkový a právní stav, respektive že řeší nějaký problém a přináší jeho úplná nebo postupná řešení.* ***Proto je nutno si položit několik otázek****: Jaký veřejný zájem směrnice v praktickém životě prosazuje? Jaké předpisy u nás tento zájem, v situaci, která je ve směrnici popsána, řeší? Odpovídají tyto předpisy a postupy u nás dané směrnici? Lze se od nějakých požadavků směrnice odchýlit a za jakých podmínek a s jakým cílem? S kým bylo konzultováno, jaký dopad na něj směrnice bude mít?*

V oddílu “Důvod předložení a cíle” přitom předkladatel činí přesně to, co vzdělávací manuál říká, že by dělat neměl – tedy zaměňuje povinnost a řešený problém. Důvodem je podle Úřadu povinnost transponovat směrnici, splnit legislativní úkol předložit návrh zákona, který zpracovává "mechanismus prověřování bezpečnosti dodavatelského řetězce” a reflektovat připomínky z praktické aplikace zákona o kybernetické bezpečnosti.

Vzdělávací manuál dále uvádí, že je zapotřebí *“jasně analyzovat současný stav a zdůvodnit, co a proč by se mělo změnit.”*[5] Předkladatel ovšem žádnou počáteční analýzu nepředložil, a to především v části, která se týká “mechanismu prověřování bezpečnosti dodavatelského řetězce”. Součástí takové analýzy by mělo být, kteří dodavatelé jsou v současnosti přítomní

[4] https://ria.vlada.cz/wp-content/uploads/Vzdelavaci-manual-pro-RIA-UV-2017.pdf
[5] Vzdělávací manuál pro RIA, str. 18

v infrastruktuře, kterou chce Úřad podrobit regulaci, a zároveň jasná definice "strategické závislosti", které chce stát přijetím zákonné úpravy předcházet či ji, pokud již nastala, řešit. Z RIA není například jasné, zda "strategická závislost" je vytvořena pouhou přítomností některých dodavatelů v určité (či jakékoli) části strategicky významné infrastruktury bez ohledu na to, jakou část dodávek do strategicky významné infrastruktury určitého regulovaného subjektu tvoří, nebo zda je problémem, že určitý dodavatel má významný podíl (čemuž by napovídala poznámka pod čarou 16, ve kterém jako příklad strategické závislosti předkladatel uvádí 75-100% závislost ČR na ruském plynu v prvním pololetí roku 2021).

Z jasné definice toho, jakému problému chce stát předcházet, a zároveň z analýzy současného stavu lze totiž posoudit rozsah problému, určit jeho příčiny a vyhodnotit jejich důležitost, jak to opět uvádí Vzdělávací manuál pro hodnocení dopadů regulace (RIA). Pokud například z analýzy současného stavu plyne fakt, že povinné subjekty většinou zohledňují technická i netechnická rizika v souladu s doporučením NÚKIB pro hodnocení důvěryhodnosti dodavatelů technologií 5G sítí v České republice, jak to NÚKIB uvádí ve Zprávě o stavu kybernetické bezpečnosti České republiky za rok 2022[6], pak je na místě mezi varianty zařadit i možnost nelegislativního řešení či alternativy k tvrdé regulaci (jak to doporučuje Vzdělávací manuál pro hodnocení dopadů regulace (RIA)[7], jako povinnost náhrady škody, odpovědnost, pojištění a podobně. Nezahrnutí těchto variant zřejmě souvisí s chybně nastaveným důvodem předložení, tedy "splněním zadání od Bezpečnostní rady státu předložit zákon".

Zároveň minimálně v jednom místě v důvodové zprávě předkladatel tento vlastní analytický podklad popírá, když tvrdí, že "*k reflexi 5G Doporučení jeho adresáty po jeho vydání prakticky nedošlo*" (ve výše zmíněné Zprávě o stavu kybernetické bezpečnosti České republiky za rok 2022 říká, že "*povinné subjekty většinou zohledňují technická i netechnická rizika v souladu s doporučením*"). Není tak jasné, jaké tvrzení je pravdivé, protože obě pravdivá být nemohou. Druhé tvrzení navíc může být potvrzené kontrolou předkladatele, které v části Varování z roku 2018 žádná pochybení u regulovaných subjektů nenašel. Zároveň předkladatel sám vnímá mitigaci rizika v důvodové zprávě binárně (tedy pouze jako daného dodavatele v infrastruktuře používat, či nepoužívat), nikoli např. řídit riziko jinými prostředky.

6 https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2022.pdf, strana 29
7 Vzdělávací manuál pro RIA, str. 22

Zpráva neobsahuje adekvátně stanovené cíle ani parametry, dle kterých se bude vyhodnocovat úspěšnost regulace

Vzdělávací manuál stanovuje, že cíle je třeba vymezit věcně:

> *"Cíle je třeba vztáhnout k dosažení určité hodnoty či reálné změny v postavení dotčených subjektů, nelze se omezit výlučně na cíle formální (například řádná transpozice evropské směrnice, naplnění závazku z programového prohlášení vlády)."*[8]

Předkladatel k zpracování Zprávy přistoupil přesně tak, jak vzdělávací manuál říká, že se postupovat nemá, když napsal:

> *"Cílem návrhu zákona je úplná a správně provedená transpozice směrnice NIS 2, zavedení funkčního a efektivního mechanismu prověřování bezpečnosti dodavatelského řetězce a reflexe dosavadních zkušeností s fungováním a praktickou použitelností zákona o kybernetické bezpečnosti tak, aby vznikl jednotící předpis, který bude srozumitelný pro adresáty a povede k zajištění bezpečného fungování informační společnosti ČR, tj. zajištění bezpečné realizace základního práva na informační sebeurčení prostřednictvím informačních systémů, služeb a sítí elektronických komunikací. Cílem návrhu zákona je též ochrana nedistributivních práv státu, tj. zajištění veřejného zájmu na bezpečnosti regulovaných služeb."*

Zároveň vyjmenované cíle ve Zprávě nesměřují k dosažení určité hodnoty nebo reálné změny v postavení dotčených subjektů. Ty, které nejsou formální (tedy transpozice, plnění strategií a podobně), jsou definované neměřitelně, například jako *"významné omezení přítomnosti rizikových a potenciálně rizikových dodavatelů, jež mohou představovat bezpečnostní hrozbu pro ČR."* Není-li jasné, kdo tito dodavatelé jsou, nebo mohou být kdykoli v budoucnu, a jaký je jejich podíl na dodávkách ve strategicky významné infrastruktuře, je jen těžké vyhodnotit, zda k naplnění tohoto cíle došlo (nebo proč je potřeba zákon jako takový).

Předkladatel zákona také uvedl, že cílem předložení zákona je *"prostřednictvím intenzivnějšího informování poskytovatelů strategicky významné služby o hrozbách spojených*

[8] Vzdělávací manuál pro hodnocení dopadů regulace (RIA), str. 20

s rizikovými dodavateli přispívat k tomu, že i poskytovatelé strategicky významné služby začnou sami klást větší důraz na bezpečnost, včetně aspektů rizikovosti, které posuzuje stát." Cílem předložení zákona ale nemůže být informovat určité subjekty o hrozbách či rizicích, protože k informování Úřad zákon v zásadě nepotřebuje.

Parametry vyhodnocení regulace také neodpovídají Vzdělávacímu manuálu. Ten uvádí, že přezkum by měl odpovědět na následující dotazy:

- S jakým časovým odstupem bude přezkoumána účinnost navrhované úpravy, tedy dosažení jejích cílů, popřípadě její nezamýšlené důsledky?
- Na základě jakých ukazatelů?
- Jak budou shromážděna data potřebná pro tento přezkum?

Úřad ve Zprávě neuvedl žádnou lhůtu, ve které k přezkumu dojde. U konkrétních ukazatelů uvedl, že relevantní budou např. počet a druh kybernetických bezpečnostních incidentů, které byly detekovány a nahlášeny Úřadu, úroveň kybernetické bezpečnosti informačních systémů hodnocená na základě výsledků kontrol zavádění a provádění bezpečnostních opatření a protiopatření Úřadu, procento orgánů a osob, které jsou v souladu se zákonnými požadavky, úroveň osvěty a povědomí veřejnosti a dotčených osob v regulovaných organizacích v oblasti kybernetické bezpečnosti. Ovšem není vůbec jasné, na základě čeho bude efektivitu měřit, tedy např. o jaké procento by se měl snížit počet a druh kybernetických bezpečnostních incidentů, jak hodnotit úroveň kybernetické bezpečnosti systémů a podobně. Úřad také neuvedl, jak shromáždí data, která budou pro přezkum potřebná. Efektivita regulace je tak v zásadě neměřitelná, protože není ve Zprávě nijak zakotvena.

3. Jak se RIA staví k průběžnému posuzovaní dopadů regulace? Má ambici například průběžně vyhodnocovat, zdali důvody regulace ještě trvají, anebo již pominuly a jak se změna takového stavu projeví na požadované administrativní zátěži směrem na podnikatele?

Ne, RIA adekvátně nevyhodnocuje dopady regulace na povinné subjekty. Jak se píše ve vzdělávacím manuálu, obecně platí, že aby mohly být dopady správně identifikovány, musí být správně definován problém a cíl navrhovaného právního předpisu (cílový stav). Výše jsme ukázali, že problém a cíle považujeme za definované nedostatečně. Z toho pramení i další nedostatky ve vyhodnocení dopadů regulace na povinné subjekty. To je přitom jeden ze základních parametrů, podle kterých lze měřit efektivitu.

Hodnocení dopadů na podnikatelské prostředí je však zcela nedostatečné. Zpráva sice uznává, že náklady pro regulované subjekty porostou, avšak tvrdí, že přesnou výši finančních dopadů nelze předem stanovit. Všechny předchozí snahy o jejich vyčíslení vedly pouze k odhadům s nízkou mírou vypovídající hodnoty (viz s. 7 zprávy RIA). Dle zprávy RIA má návrh zákona dopad na přinejmenším 6 000 subjektů především ze soukromé sféry. Za takové konstelace je potřeba popsat finanční dopad na subjekty s nějakou akceptovatelnou odchylkou. Tyto informace zpráva RIA bohužel vůbec neobsahuje a celkově je v ní naprostý nedostatek jakýchkoliv dat, díky kterým má legislativa právě vznikat.

Úřad také tvrdí, že administrativní zátěž je zanedbatelná, avšak pouze pokud jde o subjekty, na něž se již vztahují administrativní povinnosti související s kybernetickou bezpečností. Avšak není zřejmé, jak k tomuto závěru předkladatel došel, neboť předkladatel byl informován, že významný administrativní dopad bude i na subjekty, na něž se regulace již vztahuje. Vedle toho se však předkladatel vůbec nezmiňuje o nově povinných subjektech. Dále se v podkladu vůbec nemluví o počtu regulovaných služeb či velikosti firem, jichž se bude nová regulace týkat, což je další signál toho, že administrativní zátěž spíše poroste. Obecně Úřad nijak nevyhodnotil administrativní zátěž subjektů, ačkoli má k dispozici několik metodik, včetně metodiky Ministerstva průmyslu a obchodu z července 2017 nebo Metodické pomůcky pro prevenci nadbytečné regulatorní zátěže při implementaci práva EU, která je dostupná na webových stránkách Úřadu vlády. Obě tyto metodiky byly plně využitelné při zpracování zprávy RIA, avšak Úřad je zjevně ignoroval.

V rámci zprávy RIA rovněž chybí posouzení dopadu na OSVČ a malé a střední podniky, což jsou aspekty, na něž zásady hodnocení RIA explicitně upozorňují. **Hodnocení dopadu na podnikatelské prostředí je tedy nedostatečné a nepřispívá ke splnění zásad hodnocení RIA**.

Zásady hodnocení RIA – Metodika pro hodnocení dopadů regulace (RIA), část A, bod 10.7., vyžadují, aby zpráva RIA obsahovala informace o dopadech na ceny, které platí spotřebitelé, a o dopadech na kvalitu a dostupnost zboží a služeb, včetně zajištění informovanosti a ochrany spotřebitelů. Úřad uvádí, že nepředpokládá žádné přímé dopady na spotřebitele, ale zároveň uznává, že může dojít k tlaku regulovaných subjektů na promítnutí nákladů na zavedení bezpečnostních opatření do cen služeb. Toto by mělo negativní dopad na spotřebitele, což by mělo být alespoň odhadem vyčísleno, zejména v oblastech, které ovlivňují širokou veřejnost, jako jsou telekomunikace či energetika. V oblasti energetiky by mohlo přenášení nákladů na spotřebitele mít zásadní dopad, který by mohl mít sociální důsledky, což v zprávě RIA není dostatečně reflektováno.

Zhodnocení dopadů na spotřebitele, jak je prezentováno ve zprávě RIA, není dostačující a neodpovídá zásadám hodnocení RIA.

Úřad se nepokusil o průkazný odhad počtu dotčených subjektů

Ve zprávě RIA je identifikace dotčených subjektů velmi nedostatečná. Úřad pouze píše (na str. 14 a dále), že “odhady hovoří o minimálně 6 000 povinných orgánech a osobách, aniž by doložil, jak k tomuto číslu došel. V Pracovním dokumentu útvarů Komise ([9] (str. 71) odhaduje Evropská komise, že směrnice pokryje v celé EU 110 000 subjektů, z toho 67 tisíc bude “základních” (tedy s vyšší mírou důležitosti) a 43 tisíc bude “důležitých” (tedy s nižší mírou důležitosti). Státní správa má přitom k dispozici řadu zdrojů dat, díky kterým může odhadnout množství regulovaných subjektů s poměrně vysokou mírou přesnosti (počet zaměstnanců, obrat, data z registru ekonomických subjektů podle klasifikace ekonomických činností a řadu dalších), zároveň jsou k dispozici různé registry, rejstříky a podobně. Je tedy možné dospět k lepšímu stanovení množství povinných subjektů. Úřad také nijak neuvádí, proč odhaduje pro ČR poměr režimů povinnosti 1:5 ve prospěch režimu s nižšími povinnostmi,

[9] COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020SC0345

zatímco v Pracovním dokumentu útvarů Komise k návrhu evropské směrnice NIS 2 je to naopak, přibližně 3:2 ve prospěch režimu s vyššími povinnostmi. Protože z návrhů vyhlášek vyplývá poměrně dramatický rozdíl v míře povinností, které má úřad vyžadovat, jde o zásadní číslo. Úřad v části 7 "Konzultace a zdroje dat" sice uvádí, které subjekty oslovil se žádostmi o konzultace a vyjádření, ale zároveň neuvádí, v jaké podobě je žádal o data a zda data dostal. Zároveň neuvádí, jak konzultace dopadly. Jak uvádí Vzdělávací manuál:

> *Vyhodnocení konzultačního procesu musí být součástí ZZ RIA (tedy průběhu a výsledku konzultací s dotčenými subjekty). Je nutno uvést všechny dotčené subjekty a orgány státní správy, s nimiž konzultace probíhaly. Výsledek by měl zahrnovat nejen výčet konzultovaných subjektů, ale i všechny jejich připomínky a podněty. Také by měl obsahovat informace o tom, jak byly jejich podněty zapracovány, případně zdůvodnění, proč podněty zohledněny nebyly.*[10]

Nic z toho bohužel ve Zprávě obsažené není. Není tak naprosto jasné, z jakých dat Úřad vycházel při odhadech o počtu budoucích povinných subjektů.

S ohledem na význam regulačního dopadu této legislativy by bylo vhodné využít všechny dostupné prostředky k přesnějšímu odhadu a následnému kvantifikování potenciálního dopadu. Právě při hodnocení dopadů mimo veřejnou správu je zásadní oslovit široký okruh dotčených subjektů. Tento proces zahrnuje konzultace s různými organizacemi a pečlivé zohlednění jejich relevantních komentářů a podnětů, což výrazně přispívá k vyšší kvalitě navrhované regulace.

Jednou z možností je samozřejmě přes mezirezortní připomínkové řízení, ale pro usnadnění tohoto procesu byla pro zpracovatele hodnocení dopadů vytvořena Databáze konzultujících organizací (DataKO). Tato databáze obsahuje seznam organizací z různých oblastí, včetně odborného, profesního a zájmového spektra, které vyjádřily zájem o aktivní účast v přípravě materiálů určených pro jednání vlády a pro strategické a konzultační dokumenty pro další rozhodování veřejných orgánů.

Dále je nutné upozornit, že ve Zprávě nejsou nijak reflektované požadavky na dodavatele vyplývající z § 10 (Řízení dodavatelů) a z přílohy č. 7 k návrhu Vyhlášky o regulovaných službách v režimu vyšších povinností (Řízení dodavatelů – bezpečnostní opatření pro smluvní vztahy) a přílohy č. 3 k návrhu Vyhlášky o regulovaných službách v režimu nižších povinností

[10] Vzdělávací manuál, str 34

(Požadavky na smluvní ujednání s dodavateli) Dodavatelé poskytovatelů regulovaných služeb budou nuceni k zavádění některých bezpečnostních opatření i přes to, že nejsou povinné osoby podle tohoto zákona. Totéž platí i v případě mechanismu bezpečnosti dodavatelského řetězce – je velmi pravděpodobné, že pokud Úřad rozhodne o omezení či zákazu některých dodavatelů, bude totéž platit i pro ty dodavatele, kteří tyto zakázané či omezené dodavatele používají (tito jsou tedy jejich poddodavateli, na které se mechanismus vztahuje také). Nepřímé (sekundární) náklady ostatně požaduje vyčíslit i Vzdělávací manuál pro hodnocení dopadů regulace (RIA).

Úřad nevyhodnotil dostatečně dopady na výdajovou stranu veřejných rozpočtů

Pro dopady na státní rozpočet a ostatní veřejné rozpočty existuje Metodika pro stanovení plánovaných nákladů na výkon státní správy[11] a Metodika pro měření celkových nákladů na plnění povinností vyplývajících z regulace[12]. Ze Zprávy není patrné, zda vůbec a jak počítal NÚKIB nutnost navýšení počtu zaměstnanců s ohledem na zjevně nutné zásadní navýšení počtu zaměstnanců.

Pracovní dokument útvarů Komise doprovázející návrh směrnice NIS 2 uvádí, že "možnost č. 3", kterou nakonec vybral jako nejvhodnější pro rozpracování do podoby návrhu směrnice, bude vyžadovat významný růst zdrojů pro kyberbezpečnostní úřady v národních státech:

> *Balancing all the above-mentioned factors, in option 3 these new tasks are expected to require an overall increase of about 20-30% of resources (including staff) of the relevant authorities per Member State at central level needed mainly for performing supervisory actions on a larger number of entities (i.e. on-site and off-site checks, udits, requests for and assessment of compliance evidence, etc) and interactions with industry (including sector-specific)*

Úřad přitom píše (v kapitole 3.1. shrnutí Zprávy), že

> *Primárně budou veškeré výdaje a zvýšená potřeba v personální a platové oblasti, jež jsou spojeny s implementací návrhu zákona o kybernetické bezpečnosti včetně*

[11] http://www.vlada.cz/assets/ppov/lrv/ria/metodiky/Naklady-na-vykon-statni-spravy.pdf
[12] http://www.vlada.cz/assets/ppov/lrv/ria/metodiky/Nakladova-metodika-_UV-2016-05-10_-finalni-verze.pdf

prováděcích předpisů ve všech dotčených rozpočtových kapitolách, pokryty v rámci schválených rozpočtových limitů a stanovených limitů počtu míst a objemu prostředků na platy.

Pokud správci jednotlivých dotčených kapitol identifikují potřebu navýšení své kapitoly rozpočtu nad rámec schválených rozpočtových limitů nebo stanovených limitů počtu míst a objemu prostředků na platy, bude taková potřeba předmětem standardního vyjednávání o podobě relevantní kapitoly státního rozpočtu.

Zároveň ale ve Zprávě Úřad píše, že *"v souvislosti se zavedením mechanismu bude pro relevantní státní orgány třeba přijmout jednotky až nízké desítky nových pracovníků pro posuzování rizikovosti a prověřování rizikových dodavatelů"* (str. 57) a *"Náklady na straně Úřadu budou v personálních otázkách vyšší desítky tabulkových míst oproti aktuální Koncepci rozvoje Úřadu"* (str. 4) NÚKIB má dle své zprávy o činnosti za rok 2022 rozpočtováno 269,5 pracovních míst[13]. Pokud bychom vzali v úvahu odhady ze SWD zpracovaného EK a jako základ současný stav, znamenalo by to nutný nárůst počtu pracovníků o 54–81 zaměstnanců. Pokud bychom odhady promítli oproti aktuální koncepci rozvoje NÚKIB, ke které se vztahuje Zpráva, pak ta pro rok 2025, kdy mají účinky nového zákona nabíhat, prognózuje 365 pracovních míst. To by znamenalo nárůst o 73–110 zaměstnanců Úřadu.

Dle návrhu Vyhlášky o regulovaných službách bude řada subjektů veřejné správy poskytovatelem regulované služby v režimu vyšších povinností. Tento režim ukládá subjektům přidělit řadu formálních rolí, jako je manažer kybernetické bezpečnosti, architekt kybernetické bezpečnosti nebo auditor kybernetické bezpečnosti. Lze předpokládat, že tyto role jsou formalizované v případě ústředních orgánů státní správy, ale řada orgánů je přidělené mít pravděpodobně nebude (soustava státní zastupitelství, orgány soudní moci, útvary policie s celonárodní působností) nebo je nebude mít v potřebné dekoncentrované podobě na úrovni jednotlivých okresů. S tímto nárůstem potřeby kvalifikovaných zaměstnanců (úřad např. pro manažera kybernetické bezpečnosti předpokládá alespoň 3 roky praxe v oboru informační nebo kybernetické bezpečnosti, nebo absolvování studia na vysoké škole a alespoň 1 rok praxe v oboru informační nebo kybernetické bezpečnosti, příslušné certifikáty a znalosti) se Zpráva rovněž nijak nevypořádává.

Úřad v oblasti personálního zabezpečení kontroly souladu s regulací a vymáháním nových povinností jak v rámci sebe sama, tak v rámci povinných subjektů v oblasti státní a veřejné

13 https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zpr%C3%A1va%20o%20%C4%8Dinnosti%20N%C3%9AKIB%20-%202021.pdf

správy nijak nereflektuje poměry na trhu práce. Z materiálu předloženého vládě místopředsedou vlády pro digitalizaci s názvem "Kritický nedostatek ICT pracovníků ve veřejné správě"[14] vyplývá, že obor služby „Informační a telekomunikační technologie" mělo 1 926 pracovníků (2,81 %). Jejich počet navíc vytrvale klesá – oproti roku 2018 o 344 míst. Státu se nedaří nové pracovníky tohoto typu zaplatit. Jakkoli jsme si vědomi toho, že průnik mezi ICT pracovníky a potřebnými rolemi pro soulad se zákonem o kybernetické bezpečnosti je částečný, je z tohoto údaje (a z obrovského rozdílu mezi mediánovou mzdou a mediánovým platem u tohoto typu pracovníků) patrné, že při návrhu zákona je nutné brát v úvahu i tento aspekt. Navrhovat novou regulaci, kterou nebude mít kdo zavádět a kontrolovat, nedává smysl. Úřad se nijak nevypořádal ani s tím, že spolu s orgány veřejné moci bude stejný typ pracovníků poptávat ve stejné době i soukromá sféra, aby také splnila požadavky zákona. A to především s ohledem na skutečnost, že zákon požaduje plnění povinností do jednoho roku, čímž se vytváří další časová externalita, která bude mít dopad na výši administrativních i finančních nákladů.

Úřad nebere v úvahu dopad na příjmovou stranu státního rozpočtu

Nedostatky ve vyčíslení nákladů na plnění požadavků nového zákona o kybernetické bezpečnosti se promítají i do nedostatečného vyčíslení potenciálních dopadů na příjmovou stranu státního rozpočtu. Zvýšené náklady na straně povinných subjektů se mohou promítnout do snížení zisku a tím i k sníženému výběru daní od povinných subjektů. Je možné samozřejmě kalkulovat s tím, že náklady na zavádění lepších bezpečnostních opatření se promítnou do snížení nákladů na řešení potenciálních kyberbezpečnostních incidentů, ale právě to by mělo být předmětem analýzy, která ve Zprávě zcela absentuje.

Zároveň pro určité subjekty vznikne povinnost vyměnit část svých zařízení na základě podmínek mechanismu dodavatelského řetězce.

Pokud vezmeme v potaz, že mezi největšími plátci daně z přijmu právnických osob (2022) v TOP20 je minimálně 10 subjektů[15], na které dopadne nová regulace kybernetické bezpečnosti, a z toho dalších minimálně 5 firem, které budou muset řešit mechanismus dodavatelského řetězce, je naprosto zřejmé, že dopad na výběr daně a tím pádem na statní rozpočet může být nezanedbatelný. Nutnost odstranit určitého dodavatele ze systémů a sítí vyvolá nejen nové výdaje na hmotná aktiva, ale může s sebou nést další náklady v podobě zvýšené spotřeby elektrické energie, nutnosti přeškolit zaměstnance na nové systémy či

[14] Dostupný v systému eKlep pod PID ALBSD3BE76JB

[15] Největšími plátci daně z příjmů za rok 2022 jsou Kooperativa, Česká spořitelna a ČEZ | Tiskové zprávy 2023 | Tiskové zprávy GFŘ | Média a veřejnost | Finanční správa | Finanční správa (financnisprava.cz)

nutnosti nabrat nové zaměstnance, neboť nové systémy mohou být méně kvalitní než ty, které subjekty již nebudou moci z důvodu zásahu úřadu používat. Analýza tohoto problému ve Zprávě bohužel zcela chybí.

4. Je z předložené RIA zřetelná vysoká úroveň analyticko-výzkumné odbornosti?

Úřad nevyužil dostupné metodiky pro stanovení nákladů regulace

Vzdělávací manuál hovoří také o tom, jak vypočítat náklady na dodržování regulace – tedy o nutnosti zahrnout náklady vznikající podnikům a dalším subjektům, administrativní zátěž, náklady veřejné správy související s vynucováním regulace. Metodika pro měření celkových nákladů na plnění povinností vyplývajících z regulace je přitom k dispozici na stránkách Úřadu vlády již od roku 2016.[16] Úřad ji s velkou pravděpodobností nepoužil, protože na ni ve Zprávě neodkazuje a vyčíslení nákladů, o které se pokusil, neodpovídá doporučením z výše uvedené metodiky.

Stejně tak nevyužil Metodiku měření a přeměřování administrativní zátěže podnikatelů[17] a Metodiku hodnocení dopadů regulace na malé a střední podniky[18]. To považujeme za zvláště alarmující. Zpráva neobsahuje žádné zhodnocení dopadů na malé a střední podniky. Velká část z oněch "odhadem" šesti tisíc subjektů, které budou podléhat regulaci, budou právě malé a střední podniky. Směrnice NIS 2 a z ní vycházející navrhovaná česká právní úprava sice dopadají primárně na střední a velké podniky, ale zároveň jsou z velikostního kritéria vyňati poskytovatelé služeb/sítí elektronických komunikací, u kterých dopadá regulace na všechny subjekty v daném odvětví. V Česku je "aktivních podnikatelů" v tomto odvětví 1 895 podle Zprávy o vývoji trhu elektronických komunikací se zaměřením na rok 2022.[19] Podíl čtyř největších podnikatelů na trhu na celkových tržbách je přibližně tři čtvrtiny, zbytek připadá právě na "ostatní", což budou v drtivé většině mikro, malé a střední podniky. Ve Zprávě se ale nepodařilo nalézt žádné relevantní zhodnocení této skupiny podnikatelů, které budou tvořit (pokud vycházíme z odhadu šesti tisíc povinných subjektů) skoro třetinu regulovaných subjektů.

Úřad nevyužil alternativní způsoby, jak kalkulovat náklady pro budoucí regulované subjekty

Úřad mohl rovněž zvážit možnost přiblížení požadavků, které vyplývají z plnění směrnice NIS2, například dodržování normy ISO/IEC 27001, jejichž zavedením už dnes subjekt může

[16] https://vlada.gov.cz/assets/ppov/lrv/ria/metodiky/Nakladova-metodika-_UV-2016-05-10_-finalni-verze.pdf
[17] http://download.mpo.cz/get/49032/55234/602983/priloha001.pdf
[18] https://www.vlada.cz/assets/ppov/lrv/ria/databaze/Metodika-MSP.pdf
[19] https://ctu.gov.cz/sites/default/files/obsah/stranky/472017/soubory/zovt_2022.pdf

splnit cca 70 % až 80 % nové regulace[20]. Dalším podkladem můžou být data z registru smluv zveřejněné subjekty, které jsou certifikovány podle této normy. Tím by mohl zhodnotit dopad nejen při samotném zavedení těchto povinností, ale také jejich udržování, což představuje významné náklady.

Problematickou částí související s návrhem zákona o kybernetické bezpečnosti je rozsáhlé použití prováděcích vyhlášek, ve kterých předkladatel plánuje definovat řadu klíčových institucí. Tento přístup může být problematický z hlediska kontroly implementace směrnice NIS2, stejně jako z hlediska hodnocení nákladů a finančních dopadů navrhované legislativy, protože základní nástroje spojené s návrhem zákona mají být upraveny až pomocí prováděcích předpisů. To lze považovat za významnou nedostatečnost Zprávy.

Přitom pokud se podíváme na implementaci předchozí směrnice NIS1 do českého právního řádu, ve zprávě RIA tehdy předkladatel uváděl:

Na základě dalšího průzkumu provedeného mezi členy pracovní skupiny II, sestávající se ze zástupců firem a odborné veřejnosti, bylo zjištěno, že při započítání dalších nákladů, jako jsou náklady na personální zajištění, náklady na investice a dále ***náklady na samotný provoz, lze předpokládat, že tyto náklady se mohou v průměru vyšplhat až na 24 mil. Kč na jeden regulovaný subjekt.*** *Je však nutno si uvědomit, že tato výše nákladů je závislá na počtu využívaných informačních systémů a současném stavu jejich zabezpečení, přičemž z uvedeného dotazníkového šetření bylo zjištěno, že toto zabezpečení je v průměru hodnoceno na velmi vysoké úrovni a subjekty ze značné části již bezpečnostní opatření provádějí. Lze tedy obecně očekávat náklady spíše nižší.* ***Vyšší náklady však mohou vzniknout v sektorech, které doposud nebyly předmětem žádné regulace a u kterých není na zabezpečení informačních systémů kladen velký důraz.***[21]

Pokud již v roce 2017 byly předpokládány tyto náklady a dopady, je zcela zarážející, že Úřad nejenže nepracoval s přechozími analýzami a postupy, ale vůbec tyto informace nezahrnul do implementace NIS2. Nyní jsme v situaci, kdy není jasný celkový počet regulovaných subjektů a máme prakticky nulové informace, kolik dané zavedení může nově regulované subjekty stát.

Úřad zároveň jako jeden ze zdrojů uvádí pravidelné zprávy NIS Investments Report pro rok 2021 a 2022 (kapitola 3.1.3. a 3.1.4.) Zprávy. Bohužel s nimi nepracuje dostatečně. Zároveň

[20] NIS2 Directive explained: What's coming and how to prepare with ISO 27001, https://www.dataguard.co.uk/blog/nis2-directive-explained-and-how-to-prepare-with-iso-27001
[21] https://odok.cz/portal/services/download/attachment/KORNAGCLCR75/ str. 56

není jasné, proč pro účely Zprávy nevyužil report pro rok 2023, který vyšel v listopadu roku 2023[22] (Zprávu bylo možné o tato data aktualizovat před konečným předložením vládě). Zprávy jsou přitom plné informací, které je možné využít pro vytvoření odhadu nákladů pro regulované sektory – například počet jednotkových pracovních míst na sektor, průměrný a mediánový počet pracovníků zabývajících se informační bezpečností oproti všem pracovníkům v IT a další, včetně průměrných a mediánových investic na informační bezpečnost pro poskytovatele základních služeb a poskytovatele digitálních služeb, a rovněž počet subjektů, kteří využívají pojištění v oblasti kybernetické bezpečnosti. Jde o údaje, které by Úřadu velmi pravděpodobně (pokud by se spojily s kvalitní analýzou počtu a charakteru budoucích povinných subjektů a dalšími analytickými podklady) daly určitý obrázek o možných budoucích nákladech na soulad s povinnostmi z nového zákona o kybernetické bezpečnosti).

V každém případě není možné navrhovat zákon, aniž by bylo známé alespoň rozpětí nákladů pro povinné subjekty (minimálně kvalifikované odhady pro střední a velkou firmu z každého z regulovaných odvětví dle směrnice NIS 2), a to v každé zvažované variantě.

Úřad neplánuje podrobit prováděcí vyhlášky hodnocení dopadů regulace

NÚKIB plánuje drtivou většinu povinností specifikovat podzákonnými předpisy (vyhláškami), především pak rozsah regulace (kritéria pro to, které subjekty budou regulované, které budou mít režim nižších a které vyšších povinností), kritéria subjektů, které budou předmětem "mechanismu bezpečnosti dodavatelského řetězce", způsob, jakým má regulovaný subjekt plnit požadavky zákona (vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších/nižších povinností), funkce v systémech a sítích povinných subjektů, jejichž dodavatelé budou předmětem posuzování a způsob tohoto posuzování. Teprve těmito vyhláškami fakticky dojde k stanovení rozsahu regulace a bude konkrétně jasné, kolik subjektů bude regulováno a jaké budou jejich konkrétní povinnosti. Jakkoli nehodnotíme vhodnost tohoto postupu, přijde nám alarmující, že Úřad dle dostupných zdrojů (Plánu přípravy vyhlášek na rok 2024[23]) nehodlá k těmto vyhláškám zpracovávat Zprávu o hodnocení dopadů regulace.

Jde o následující vyhlášky:

- *Návrh vyhlášky o regulovaných službách*

[22] https://www.enisa.europa.eu/publications/nis-investments-2023
[23] https://ria.gov.cz/wp-content/uploads/57464_2023_FINAL_Plan-vyhlasek-2024.pdf

- *Návrh vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností*
- *Návrh vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností*
- *Návrh vyhlášky o Portálu Úřadu a požadavcích na vybrané úkony*
- *Návrh vyhlášky o nepominutelných funkcích stanoveného rozsahu*

Do určité míry by bylo možné akceptovat fakt, že detailní zpracování hodnocení dopadů regulace není v zákoně, protože Úřad se rozhodl využít ve velké míře vyhlášky, a poté detailně posoudil dopady právě při návrhu vyhlášek. Ale aby nebyly dopady hodnocené prakticky vůbec, jako je to v tomto případě, považujeme za nepřijatelné. O to závažnější je, že všechny vyhlášky související s návrhem zákona o kyberbezpečnosti dostaly výjimku a jejich regulační dopad nebyl analyzován v rámci RIA.

5. Využívá RIA všechna relevantní dostupná ekonomicko-analytická data pro správné posouzení dopadů regulace?

Analytické podklady poskytují objektivní a kvantitativní údaje o stávajícím stavu, problémech a potenciálních dopadech navrhované regulace. To umožňuje vládě a dalším zúčastněným subjektům objektivně posoudit, jaké bude mít dopady. Dále pomáhají politikům a regulačním orgánům porozumět komplexním otázkám a rozhodnout se na základě faktů podložených údajů. Pokud jsou opatření podložena spolehlivými analytickými daty, je pravděpodobnější, že budou vnímána jako racionální a opodstatněná.

Celkově lze tedy říci, že analytické podklady jsou klíčovou složkou procesu RIA, která poskytuje základní informace pro kvalitní a efektivní tvorbu a implementaci regulací a legislativy. Jsou nezbytné pro zajištění transparentnosti, legitimity a účinnosti rozhodovacího procesu veřejné politiky.

Charakteristika specifických a především zásadních dopadů:

Podle zásad hodnocení RIA – Metodiky pro hodnocení dopadů regulace (RIA), část A, bod 10.1., se vyžaduje uvedení předpokládaného hospodářského a finančního dosahu navrhované právní úpravy na státní rozpočet a ostatní veřejné rozpočty. Tato část je bohužel naprosto nedostačující. Úřad upozorňuje, že náklady, které vzniknou v důsledku nových předpisů o kybernetické bezpečnosti, budou muset být zohledněny v budoucích rozpočtech povinných subjektů, včetně těch, které již spadají pod zákon o kybernetické bezpečnosti. **Nicméně Úřad konstatuje, že není schopen přesně odhadnout finanční dopady**, jelikož jejich výše není předem stanovitelná, a tak zpracované odhady mají jen malou vypovídací hodnotu. Úřad odhaduje, že náklady na implementaci předchozích právních předpisů činily mezi 800 000 a 1 500 000 Kč na jeden zabezpečovací systém, avšak tento odhad není zcela jasný. Dotčené subjekty poskytující srovnatelné veřejné služby vyjádřily v šetření náklady od 6 000 000 do 11 000 000 Kč za organizaci. Tento rozptyl nákladů ukazuje, že hrubé odhady Úřadu se mohou velmi lišit od skutečnosti. Dopady na státní rozpočet může mít také zvýšení nákladů poskytovatelů strategicky důležitých veřejných služeb, avšak Úřad tyto náklady ani nekomentuje, ani je nevyčísluje.

Podle zásad hodnocení RIA – Metodiky pro hodnocení dopadů regulace (RIA), část A, bod 10.2., je nutné posoudit dopady a faktory ovlivňující mezinárodní ekonomickou konkurenceschopnost České republiky v kontextu jejího hospodářského růstu, inovační

a investiční činnosti a zaměstnanosti. To zahrnuje zhodnocení očekávaných dopadů na konkurenční postavení firem se sídlem v České republice jak na vnitřním trhu EU, tak vůči třetím zemím.

Podle zásad hodnocení RIA – Metodiky pro hodnocení dopadů regulace (RIA), část A, bod 10.3., je ve zprávě RIA třeba uvést detailní popis očekávaných dopadů, zejména s ohledem na velikost podniků (zejména osoby samostatně výdělečně činné a malé a střední podniky) a také dopady na trh práce.

Úřad v RIA uvádí rizika spojená s dodavatelským řetězcem, zejména strategická rizika spočívající v zemi původu dodavatele. Zmiňuje, že v současné době v České republice chybí komplexní mechanismus, který by umožňoval cíleně, účinně a flexibilně vyhodnocovat a minimalizovat rizika spojená s těmito strategickými hrozbami pro strategicky významnou infrastrukturu. Zároveň zdůrazňuje, že v rámci evropských zemí jsou běžné mechanismy pro posuzování a omezení či vyloučení rizikových dodavatelů a Česká republika by neměla zaostávat v této oblasti. Nicméně i přes uvedení důvodů pro zavedení tohoto mechanismu není ve Zprávě jasně uvedeno, proč je tento mechanismus navrhován právě v této specifické podobě. To, že Bezpečnostní rada státu uložila úřadu přijmout "zákon", nemůže být důvodem, proč Úřad nezvažuje i jiné varianty.

Argumenty, které Úřad v rámci této problematiky zmiňuje, jsou tak robustní, že by měla být vypracována samostatná RIA pouze pro část **„Mechanismus prověřování bezpečnosti dodavatelského řetězce".**

Obecně je možné říci, že analytické podklady jsou velmi nedostatečné pro takto široce pojatou regulaci s významným důsledkem pro povinné osoby (drakonické pokuty za neplnění) a s velkou pravděpodobností vysokými náklady pro relativně velký počet povinných osob.

Úřad reguluje nad rámec směrnice

V případě, že navrhovatel v zákoně, který implementuje evropskou směrnici, postupuje v návrhu nad rámec ustanovení, která směrnice požaduje, jde o takzvanou "neminimalistickou implementaci práva EU". V takovém případě požaduje Metodická pomůcka pro prevenci nadbytečné regulatorní zátěže při implementaci práva EU[24] posoudit, zda zvolená varianta

[24] https://ria.vlada.cz/wp-content/uploads/Metodicka-pomucka-prevence-zateze-pri-transpozici-prava-EU-UV-2016.pdf

implementace nepředstavuje nadbytečnou regulatorní zátěž. Každé odchýlení od minimalistické implementace by mělo být odůvodněno.
Protože za "minimalistickou implementaci" označuje NÚKIB varianty II a IV, které nakonec nevybral jako vhodné, předpokládáme, že zákon je neminimalistickou implementací (minimálně, ale nikoli pouze v rozsahu regulace a počtu povinných subjektů, které zamýšlí Úřad regulovat nad rámec definic ve směrnici). Úřad ale v rozporu s výše zmíněnou metodikou ani neprovedl žádné odůvodnění, ani nekvantifikoval případné negativní následky a nepublikoval závěry tohoto posouzení.

Navíc Úřad plánuje nejen povinnosti nad rámec směrnice pro některé povinné subjekty (především mechanismus bezpečnosti dodavatelského řetězce), ale také širší rozsah regulovaných subjektů oproti směrnici. Směrnice NIS 2 ve svých přílohách definuje, která jsou "Vysoce kritická odvětví" a "další kritická odvětví", ve kterých jsou identifikované subjekty, které mají plnit povinnosti. Návrh zákona stanovení odvětví a druhů subjektu ponechává na Vyhlášce o regulovaných službách. Některé povinné subjekty ale zjevně požaduje regulovat či regulovat s vyššími povinnostmi nad rámec požadavků ze směrnice, a to, aniž by adekvátně Úřad zdůvodnil proč.

Například v odvětví Doprava, pododvětví železniční doprava, směrnice požaduje regulovat "železniční podniky ve smyslu čl. 3 bodu 1 směrnice 2012/34/EU". Ve směrnici je definovaný jako železniční podnik "každý veřejný nebo soukromý podnik licencovaný v souladu s touto směrnicí, **jehož hlavní činností** je železniční přeprava zboží nebo cestujících, přičemž tento podnik zajišťuje trakci; jsou zde rovněž zahrnuty podniky, které pouze poskytují trakci".

V návrhu vyhlášky o regulovaných službách je definované jako regulované odvětví "provoz drážní dopravy na celostátní dráze" (případně regionální dráze), kde bude muset plnit požadavky na poskytovatele regulované služby v režimu vyšších povinností, pokud je provozovatel drážní dopravy na celostátní (či regionální) dráze podle zákona o drahách daný podnik velkým podnikem.

Mezi provozovateli drážní dopravy[25] je přitom i řada společností (především zabývajících se železničním stavitelstvím), jejichž **hlavní činností** železniční přeprava zboží nebo cestujících rozhodně není. I ony ale dle návrhu NÚKIB spadnou pod regulaci (a zřejmě i do režimu vyšších povinností, protože jde o velké firmy se stovkami zaměstnanců), ač drážní doprava pravděpodobně činí pouze zlomek jejich tržeb.

[25] https://ducr.cz/wp-content/uploads/2024/01/Seznam-dopravcu-v-CR-10.1.2024.pdf

NÚKIB navrhuje zahrnout mezi regulované subjekty i “Držitele licence na obchod s elektřinou podle energetického zákona. Těmito držiteli je ale i řada společností, které nemusí s elektřinou obchodovat ve smyslu prodeje zákazníkům, jak předpokládá směrnice NIS2 (požaduje regulovat “elektroenergetické podniky ve smyslu čl. 2 bodu 57 směrnice Evropského parlamentu a Rady (EU) 2019/944 (1), které zastávají funkci „dodávky“ ve smyslu čl. 2 bodu 12 uvedené směrnice”), ale licenci mají pouze k tomu, aby mohli nakupovat elektřinu přímo na burze – typicky jde o velké výrobní podniky, které ale jinak v regulovaných odvětvích nepodnikají (jako jsou např. papírny).

6. Doporučuje hodnotitel dopracovat RIA v nějakých konkrétních oblastech a pokud ano, v jakých?

Ano, jak je z posouzení zjevné, Zpráva nebyla vytvořena v souladu s metodikami, které předepisují legislativní pravidla jako závazné, především Metodikou stanovení nákladů na výkon státní správy v přenesené působnosti a Měřením administrativní zátěže podnikatelů. Zároveň předkladatel nezpracoval Zprávu ani dle metodik, které jsou nabízené na webových stránkách Úřadu vlády jako vodítka k tomu, jak podobné Zprávy připravit. Pokud by tak postupoval, návrh zákona by postavil na konkrétních analytických podkladech, vyčíslil by s maximální mírou průkaznosti náklady a přínosy pro veřejnou správu i soukromé subjekty a stanovil si objektivní a měřitelné cíle, které chce zákonem dosáhnout. Nic takového bohužel Zpráva neobsahuje, takže je na místě pochybovat o tom, zda z ní vycházející zákon je skutečně řešením, které je nejvhodnějším a proporcionálním řešením problému zajištění kybernetické bezpečnosti.

Na základě našeho posouzení doporučujeme následující kroky:

- Jasně analyzovat stávající stav, specifikovat problém a zdůraznit důvody, proč se s existujícími nástroji nedaří problém vyřešit; dále doplnit informace o rozsahu problému, jako jsou kvantifikace škod, počty útoků a podobně.
- Specifikovat cíle metodou SMART (specifické, měřitelné, adekvátní, reálné a termínované). Stanovit cíle, které chce stát zákonem dosáhnout – snížení počtu incidentů, zvýšení kontroly státu nad procesem zajišťování kybernetické bezpečnosti.
- Zdůvodnit, proč není možné dospět k cíli jiným způsobem než zákonnou normou, případně navrhnout jiný způsob, pokud analýza dospěje k závěru, že to možné je.
- Ve variantách nepracovat pouze s binárními možnostmi zavést/nezavést regulaci či zavést ji na úrovni určitých odvětví, ale s úrovněmi regulace (nelegislativní řešení, alternativy k tvrdé regulaci) i alternativními rozsahy regulace na úrovni infrastruktury organizací. To je sice částečně plněné definicí Kritické části strategicky významné infrastruktury, ale tato definice je příliš extenzivní, čímž se stává nejasnou. Bylo by lepší nadefinovat jednotlivé podmnožiny, které by úžeji definovaly jednotlivé parametry a tím snížily následné ekonomické dopady.
- Detailně popsat očekávaný výsledek uplatnění nebo implementace navrhovaného zákona a uvést měřitelné a kvantifikovatelné údaje o žádoucím cílovém stavu. Stanovit, dle jakých měřitelných parametrů se bude posuzovat úspěšnost navržené regulace a v jakém časovém období dojde k vyhodnocení.

- Důsledně pracovat s principem proporcionální analýzy a kvantifikovat dosažení určitého cíle oproti nákladům na to, jak tohoto cíle dosáhnout (zvláště pak s důrazem na dopad na malé a střední podniky).
- Provést detailní analýzu nákladů a výnosů. Není možné spokojit se s tvrzením, že *"Výši finančních dopadů není možné předem stanovit a veškeré předchozí požadavky na jejich vyčíslení vedly k vytvoření odhadů s nízkou vypovídající hodnotou."*

Zároveň z důvodu přehlednosti a vzájemné neprovázanosti doporučujeme rozdělit v rámci Zprávy cíle, dopady a vyhodnocování samotné implementace směrnice NIS 2 a cíle, dopady a vyhodnocování "Mechanismu prověřování bezpečnosti dodavatelského řetězce".

Úřad by se měl v této zprávě zaměřit především na:

- Vymezení rozsahu problému, možnost výskytu a vyjádření pravděpodobnosti výskytu s tím, že závěry je nutné podpořit relevantními důkazy, zejména empirickými daty, závěry analýz, zprávami odborníků,
- Předkladatel vytipuje a uvede dotčené subjekty, na které přímo či nepřímo dopadnou jeho důsledky s tím, že především rozlišuje dopady na přímé nebo nepřímé,
- Dále pak náklady a přínosy posuzovat na základě kvalifikovaného odhadu fungování navrhovaného řešení ve vztahu k současné situaci,
- **Především je nutné zvážit rizika spojená s implementací, která ovlivňují výši nákladů a přínosů,**
- Je potřeba náklady vyjádřit peněžně nebo alespoň číselně, pokud je to možné – například možné náklady v Kč,
- V průběhu vyhodnocování dopadů provádět konzultace s dotčenými subjekty, přičemž je cílem získat data, která jsou jinak nedostupná, a v rámci analýzy dospět k relevantním závěrům.

Závěr

Je zjevné, že hodnocení dopadů regulace bylo provedeno jen formálně a s velkou pravděpodobností pouze ex post (tedy že Úřad nejdříve napsal zákon a pak k němu provedl hodnocení dopadů, nikoli že by nejdříve provedl analýzy, poté zhodnotil jejich dopady a poté vybral tu, která přináší nejvíce přínosů s nejnižšími náklady). Nicméně to je bohužel při tvorbě zákonů v ČR zřejmě běžná praxe.

Autoři

PhDr. Radek Soběhart, Ph.D.
Ředitel Laboratoří behaviorálních studií (LABS) FSE UJEP, odborník na veřejnou správu a teorii regulace v České republice, autorem několika zpráv RIA a posudků určených pro Legislativní radu vlády České republiky.

Ing. Michael Fanta
Student doktorského programu "Aplikovaná ekonomie a veřejná správa" FSE UJEP, analytik, specializuje se na dopady regulace v síťových odvětvích a závislostních průmyslech.

Ing. Kateřina Fojtů, Ph.D.
Absolventka doktorského programu „Podnikové finance“ FP VUT v Brně, specializuje se na behaviorální ekonomii a finance.
behaviorální ekonomii a finance.