POZIČNÍ DOKUMENT APMS

Mechanismus řízení bezpečnosti dodavatelských řetězců do strategicky významné infrastruktury

27. PROSINCE 2023

ASOCIACE PROVOZOVATELŮ MOBILNÍCH SÍTÍ
Karlovo náměstí 317/5, 128 00 Praha 2, IČ: 75118891

1. Manažerské shrnutí

V tomto dokumentu shrnuje APMS hlavní aspekty navrhovaného Mechanismu řízení bezpečnosti dodavatelských řetězců do strategicky významné infrastruktury České republiky („**Mechanismus**"), jeho problematické aspekty a jejich řešení. **Odstraněním sporných otázek bude možné přijmout včas nový zákon o kybernetické bezpečnosti jako transpoziční normu směrnice NIS2[1] včetně jasných a přiměřených pravidel pro regulaci bezpečnosti dodavatelských řetězců.**

Debata o regulaci dodavatelských řetězců do strategicky významné infrastruktury České republiky probíhá přes dva roky. Přesto se v meziresortním připomínkovém řízení k návrhu nového zákona o kybernetického bezpečnosti, který má Mechanismus obsahovat, objevilo množství zásadních připomínek ze soukromého sektoru i orgánů veřejné moci včetně ministerstev a některých regulačních úřadů. APMS je v diskusi o regulaci dodavatelských řetězců aktivní, protože hlavní dopady mají v této fázi směřovat do sítí elektronických komunikací. **Spolu s dalšími asociacemi, jako je Hospodářská komora České republiky a Svaz průmyslu a dopravy České republiky proto APMS a její členové – mobilní operátoři – zaslali přímo NÚKIB a do meziresortního připomínkového řízení připomínky a návrhy, kterými by se regulace dodavatelských řetězců stala přiměřenou a lépe naplňující svůj účel. V rámci vypořádání připomínek NÚKIB většinu návrhů odmítl.**

Bezpečnost telekomunikačních sítí a služeb je pro mobilní operátory základním předpokladem jejich obchodní činnosti. Žádný z nich proto neupřednostní levnější technologii a vyšší zisk nad bezpečností. Mobilní operátoři kladou na bezpečnost o to větší důraz, že jsou provozovateli kritické infrastruktury státu, jejíž integrita je nezbytná také pro zachování základních funkcí státu.

Ve vztahu k síťové infrastruktuře a službám mají mobilní operátoři již dnes uloženo velké množství povinností (cca 900 technicko-organizačních opatření) například zákonem o elektronických komunikacích,[2] zákonem o kybernetické bezpečnosti[3] anebo zákonem o krizovém řízení.[4] Vedle toho mají členové jejich volených orgánů povinnost jednat s péčí řádného hospodáře s hrozbou osobní majetkové odpovědnosti v případě jejího porušení.[5] Také proto mají mobilní operátoři zavedena opatření požadovaná obecně závaznými právními předpisy k zajištění bezpečnosti sítí a služeb a k tomu zavádí vlastní opatření, která odolnost dále zvyšují. Zejména výběru dodavatelů síťových technologií věnují mobilní operátoři mimořádnou pozornost a hodnocení uchazečů podle tisíců parametrů trvají i déle než 18 měsíců.

[1] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii, publikováno v Ústředním věstníku Evropské unie, L333/80.

[2] Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

[3] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.

[4] Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů.

[5] K péči řádného hospodáře viz blíže příslušná ustanovení zákona č. 89/2012 Sb., občanský zákoník (OZ), a zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích; ZOK) - zejm. § 159 odst. 1 OZ či § 51 ZOK.

Návrh Mechanismu bohužel existující bezpečnostní opatření ani technické aspekty telekomunikačních sítí nezohledňuje. Zaměřuje se pouze na hodnocení mezinárodněpolitických faktorů bez vysvětlení realizace možných hrozeb. Tento přístup může způsobit vícenáklady v řádu desítek miliard Kč na straně soukromého sektoru[6] a státu. Zvýšení nákladů však bezpečnost ani kvalitu telekomunikačních služeb pro občany, firmy ani státní instituce nezvýší.

Návrh Mechanismu předložený NÚKIB má sedm nejvýznamnějších nedostatků:

1. zahrnutí veškerých částí sítě (včetně okrajových) do rozsahu regulace,
2. bezprecedentní koncentraci pravomocí zasahujících do působnosti dalších ústředních správních orgánů a Parlamentu České republiky,
3. netransparentní a arbitrární hodnocení na základě vlastních hodnotících kritérií,
4. protiústavní určování rozsahu regulace vyhláškami NÚKIB,
5. neexistence řádného opravného prostředku proti rozhodnutí o regulaci prostřednictvím opatření obecné povahy,
6. neexistence pravidel náhrady škody způsobené regulací včetně zmařených investic do stávající infrastruktury, a
7. zvýšení administrativní zátěže v soukromém sektoru i ústředních správních orgánech.

APMS navrhuje následující změny umožňující přijetí Mechanismu bez uvedených nedostatků a se zachováním účelu Mechanismu:

1. zahájení otevřeného dialogu mezi soukromým sektorem a NÚKIB včetně sdílení bližších informací o hrozbách a zranitelnostech,
2. omezení regulace pouze na jádro mobilní telekomunikační sítě jako na její nejkritičtější část,
3. zahrnutí závazného stanoviska odvětvového regulátora – Českého telekomunikačního úřadu – mezi podmínky vydání OOP,
4. omezení koncentrace pravomocí NÚKIB zahrnutím rozsahu regulace přímo do nového zákona o kybernetické bezpečnosti,
5. specifikaci náležitostí OOP přímo v novém zákonu o kybernetické bezpečnosti, a
6. zavedení mechanismu náhrady škody vzniklou regulací nad rámec jádra sítě.

NÁSLEDUJÍCÍ PODKAPITOLY PODROBNĚJI VYSVĚTLUJÍ TŘI HLAVNÍ PROBLEMATICKÉ OBLASTI NÁVRHU MECHANISMU A ZPŮSOBY JEJICH ŘEŠENÍ.

1.1. Zapojení vlády a sektorového regulátora do Mechanismu

Návrh Mechanismu předpokládá, že NÚKIB samostatně stanoví rozsah regulace (dotčených aktiv), stanoví hodnotící kritéria bezpečnosti dodavatelského řetězce, na základě vlastní metodologie provede hodnocení a samostatně rozhodne o omezení, resp. vyloučení konkrétního dodavatele.

[6] K analýze nákladů hrozících v důsledku nepřiměřené regulace viz analýza vypracovaná Centrem ekonomických a tržních analýz pro APMS, podle které by náklady odvětví mobilních telekomunikací na výměnu síťových technologií mohly dosáhnout až 18 miliard Kč. Analýza dostupná na internetových stránkách APMS zde: https://apms.cz/narodni-bezpecnost-chytre-za-stovky-milionu-tupe-i-za-18-mld/. Přistoupeno 6.12.2023.

Takováto úprava je pro dle našeho názoru z ústavního hlediska nepřijatelná, protože představuje zcela nepřiměřenou a nekontrolovanou koncentraci moci u exekutivního orgánu.

Nad rámec výše uvedeného by NÚKIB svým postupem také významně zasahoval nejen do kompetencí jiných ústředních orgánů státní správy, jako je zejména Ministerstvo průmyslu a obchodu nebo Český telekomunikační úřad, ale také samotné vlády České republiky, která jediná může komplexně posoudit možný dopad zákazu dodavatele ze třetí země na zahraničně politické nebo bezpečnostní zájmy státu a ekonomickou bezpečnost státu[7].

NÚKIB má totiž dle ZKB plnit roli gestora a národní autority **v oblasti kybernetické bezpečnosti**, naopak **zahraničně ekonomickou politiku**, kterou proces posuzování třetích zemí a případný zákaz dodavatelů z těchto zemí jistě představuje, má dle § 13 odst. 1 písm. a) zákona č. 2/1969 Sb., ve znění pozdějších předpisů plnit **Ministerstvo průmyslu a obchodu. Do působnosti ministerstva navíc dle platné právní úpravy patří prověřování zahraničních investic, které je svým účelem zcela obdobné Mechanismu.**

Námitky, že takováto nekontrolovaná koncentrace moci neodpovídá principům demokratického právního státu a porušuje ústavní principy, však NÚKIB bez dalšího zamítl.

S ohledem na výše uvedené nedostatky navržené právní úpravy v předloženém materiálu navrhujeme zapojení:

1.1.1. Zapojení vlády

Zákazem či omezením plnění dodavatele dochází k významnému zásahu do svobody podnikání mnoha subjektů na trhu. Zákaz i omezení plnění dodavatele může mít významné ekonomické, ale i **geopolitické dopady**. Obdobné dopady již stát v minulosti hodnotil v rámci právní úpravy prověřování zahraničních investic. V rámci procesu prověřování zahraničních investic dochází obdobně jako v případě Mechanismu k prověřování osoby investora na základě strategických kritérií. Stejně jako v případě Mechanismu může také dojít k zákazu investice.

V případě prověřování zahraničních investic investici a osobu investora posuzuje Ministerstvo průmyslu a obchodu a případný zákaz investice podmíněn usnesením vlády. Samotný zákon odůvodňuje zapojení vlády následovně *„„[V]láda přijme do 45 dnů ode dne, kdy jí byla věc předložena k projednání, usnesení o tom, zda zahraniční investice může představovat ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. Při posuzování věci vláda zohlední možný dopad zahraniční investice na principy demokratického právního státu, ochranu života a zdraví obyvatel, obranu státu, **zahraničně politické nebo bezpečnostní zájmy státu, ekonomickou bezpečnost státu** a případně další skutečnosti důležité z hlediska ochrany bezpečnosti České republiky nebo vnitřního či veřejného pořádku.“*

Z tohoto ustanovení jednoznačně plyne vůle vlády České republiky a Parlamentu České republiky svěřit rozhodování o takto významných otázkách vládě České republiky, která i díky zapojení dotčených orgánů veřejné moci a dalších subjektů má schopnost posoudit širší

[7] Zákon č. 34/2021 Sb., o prověřování zahraničních investic a o změně souvisejících zákonů (zákon o prověřování zahraničních investic).

mezinárodněpolitické a hospodářské souvislosti postupu vůči konkrétní zahraniční osobě. Vláda České republiky má také schopnost posoudit širší hospodářské a vnitropolitické souvislosti přijatých opatření napříč odvětvími.

Postup navržený Mechanismem je nejenom shodný s procesem prověřování podle ZPZI, ale shodné mohou být také důsledky rozhodnutí o omezení či zákazu plnění konkrétního zahraničního dodavatele. Pro předejití nekontrolovatelných dopadů a pro zachování souladnosti právních norem by měl být zákaz dodavatele, obdobně jako osoby investora, podmíněn usnesením vlády.

1.1.2. Zapojení sektorového regulátora

Český telekomunikační úřad (ČTÚ) je orgánem veřejné moci s působností pro odvětví elektronických komunikací a tomu odpovídajícími regulatorními pravomocemi.[8] ČTÚ má však zároveň uloženou řadu povinností směřujících ke stabilitě a rozvoji odvětví, včetně problematiky infrastruktury, užívaných technologií, interoperability, přeshraniční spolupráce, bezpečnosti, integrity sítí a služeb a odolnosti sítí elektronických komunikací.[9] Zákon proto stanoví pravomoc ČTÚ dohlížet na plnění povinností uložených adresátům regulace, ukládat nápravná opatření v případě zjištěných nedostatků a ukládat ve správním řízení finanční pokuty.[10]

S ohledem na takto určenou odpovědnost je nezbytné zajistit, aby ČTÚ měl možnost se formou závazného stanoviska vyjádřit k regulačním opatřením jiných orgánů veřejné moci, jako je například NÚKIB, která mohou ovlivnit odvětví elektronických komunikací. Obdobný problém předpokládáme také ve vztahu mezi NÚKIB a dalšími regulačními úřady, například Energetickým regulačním úřadem, jehož působnost má být návrhem Mechanismu také dotčena.

V rámci vypořádání připomínek se Svazem průmyslu a obchodu NÚKIB představil vlastní návrh zapojení sektorových regulátorů do procesu Mechanismu. Jedná se však pouze o formu konzultačního postavení, kdy se NÚKIB stanoviskem sektorového regulátora nemusí řídit a je pro něj nezávazné.

APMS a její členové mají zato, že účast ČTÚ jako odborně vybaveného a zákonem určeného nezávislého správního úřadu pro odvětví elektronických komunikací je na přípravě OOP nezbytná pro předcházení excesů s negativním dopadem do odvětví elektronických komunikací. Obdobné zapojení lze shledat i v mnoha zahraničních přístupech. Stanovisko ČTÚ musí být pro NÚKIB závazné a OOP je musí reflektovat.

[8] K rozsahu regulace pro odvětví elektronických komunikací blíže viz zákon č. 127/2005 Sb., o elektronických komunikacích. K působnosti ČTÚ viz § 108 a násl. téhož zákona.

[9] K cílům a základním zásadám regulace blíže viz ustanovení § 4–6 zákona č. 127/2005 Sb., o elektronických komunikacích.

[10] K rozsahu přestupů a ukládání pokut viz blíže ustanovení § 118-120 zákona č. 127/2005 Sb., o elektronických komunikacích.

1.2 Případný zákaz dodavatele se má vztahovat pouze na ty nejkritičtější funkce sítě

Mobilní telekomunikační síť se skládá ze čtyřech hlavních částí: jádro sítě (core), přenosová síť (transmission network), rádiová přístupová síť (RAN) a koncová zařízení (např. mobil nebo modem). Jádro sítě zajišťuje důležité funkce nezbytné pro řádné fungování sítě a služeb. Kritičnost jádra sítě spočívá zejména v tom, že na něm zcela závisí poskytování regulované služby a omezením jeho funkčnosti, resp. vyřazením z provozu tak není možné regulovanou službu poskytovat. Přenosová síť a rádiová přístupová síť jsou od jádra sítě oddělené a stejně tak jsou oddělené i mezi svými jednotlivými částmi. Nefunkčnost jedné části přenosové nebo rádiové přístupové sítě proto nezpůsobí nefunkčnost jejich dalších částí. Krátkodobé výpadky jsou běžnou součástí provozu sítě například při výměně technologií, výpadku dodávek elektrické energie anebo poruše.

Jak uvedl NÚKIB, Mechanismus se má vztahovat pouze na tu nejkritičtější část strategické infrastruktury. NÚKIB však ve svém návrhu vymezil rozsah Mechanismu formou vyhlášky o nepominutelných funkcí, která pro oblast telekomunikací obsahuje jak ty nejkritičtější části sítě, jako je jádro sítě, tak i v obecné rovině méně kritické části sítě, jako je rádiová přístupová síť nebo aktiva, které nemají přímý vliv na nedostupnost regulovaných služeb, jako je fakturační systém. V návrhu zákona také zcela chybí odůvodnění, proč jsou kritické části stanoveného rozsahu aktiv definovány tak široce.

V návrhu změn Mechanismu jsme v APMS kritické části strategické infrastruktury transparentně rozdělili dle hrozeb a míry dopadu jejich realizace. **Nejvýznamnější hrozbou je výpadek regulované služby**. Rozsah Mechanismu jsme tak navrhli omezit na aktiva, jejichž nedostupnost má přímý okamžitý dopad na nedostupnost regulované služby na kritické úrovni. Pro oblast telekomunikací se bude jednat zejména o jádro sítě, případně části přenosové sítě.

Pro tyto kritické části, které mohou způsobit okamžitou nedostupnost strategicky významné služby, je tedy vhodné, aby byla dána možnost státu okamžitým zásahem zakázat vybraného dodavatele, u kterého identifkuje významnou hrozbu.

Pro zbylé části aktiv strategicky významné služby, které nemohou ze své podstaty způsobit nedostupnost služby na kritické úrovni, je s ohledem na princip proporcionality vhodné, aby poskytovatel strategicky významné služby sám na základě analýzy rizik minimalizoval rizika, která v rámci opatření obecné povahy identifikoval NÚKIB. NÚKIB by jako doposud nad implementovanými bezpečnostními opatřeními vykonával dohled. Bezpečnostní opatření specifická pro daného dodavatele by nově byla upravena zvlášť v bezpečnostní dokumentaci, kterou by poskytovatel strategicky významné služby měl povinnost každoročně aktualizovat.

Tento systém jsme nazvali kaskádou bezpečnostních povinností, kdy pro tu nejkritičtější část strategické infrastruktury bude povinnost řídit se případným zákazem uvedeným v opatření obecné povahy, a pro ty méně kritické části strategické infrastruktury bude nově dána povinnost zohlednit rizika identifikovaná státem a implementovat odpovídající bezpečnostní opatření.

Omezení regulace pouze na jádro, tedy stanovení rozsahu Mechanismu, musí být také upraveno přímo v zákoně. Stanovení rozsahu Mechanismu vyhláškou, jak navrhuje NÚKIB, považuje APMS za protiústavní, zejména s ohledem na závažný ekonomický, právní i administrativní dopad Mechanismu

na poskytovatele regulované služby. Ponechání této kompetence v rukou moci výkonné, nikoli zákonodárné, by vedlo k nepřiměřené koncentraci pravomocí v rukou jednoho z orgánů veřejné moci.

2. Telekomunikace podléhají přísné a rozsáhlé regulaci již dnes

Návrh Mechanismu přináší novou a obsáhlou regulaci do odvětví, jehož bezpečnost a odolnost již dnes upravuje řada obecně závazných právních předpisů. Jedná se zejména o zákon o elektronických komunikacích („**ZEK**“),[11] zákon o kybernetické bezpečnosti („**ZKB**“)[12] anebo zákon o krizovém řízení („**ZKŘ**“).[13] Provozovatelé mobilních telekomunikačních sítí provádějí již dnes cca 900 technicko-organizačních opatření, aby byli v souladu s aktuálně platnou regulací. Vedle toho mají členové jejich volených orgánů povinnost jednat s péčí řádného hospodáře s hrozbou osobní majetkové odpovědnosti v případě jejího porušení.[14]

Cílem citované legislativy je zejména posílit bezpečnost a odolnost telekomunikačních služeb a infrastruktury a připravit je na řešení krizových stavů a zajištění základních funkcí státu. Vzhledem k tomu **se Mechanismus jeví jako duplicitní regulace, jejíž inkrementální přínos k bezpečnosti a odolnosti strategické infrastruktury státu je v poměru k již existujícím opatřením minimální, ale jejíž nákladovost je mimořádná.**

Pro lepší porozumění základům bezpečnosti a odolnosti telekomunikační infrastruktury a služeb shrnujeme níže hlavní aspekty již existující regulace v jednotlivých oblastech.

2.1. Povinnosti uložené telekomunikační regulací

Základním regulačním předpisem pro elektronické komunikace je ZEK. Vedle určení východisek regulace odvětví, působnosti a pravomocí Českého telekomunikačního úřadu („**ČTÚ**“) jako odvětvového regulátora a podmínek poskytování služeb elektronických komunikací upravuje ZEK také požadavky na zajištění bezpečnosti a integrity sítí a služeb elektronických komunikací včetně krizových stavů.[15]

Základní povinností je v této souvislosti je **zajištění takové úrovně bezpečnosti, která odpovídá míře existujícího rizika s cílem předejít nebo minimalizovat dopad bezpečnostních incidentů na uživatele a na sítě a služby.**[16] Bezpečností sítě a služby se přitom rozumí jejich „*schopnost odolávat s dostatečnou spolehlivostí veškerým zásahům, které narušují dostupnost, hodnověrnost, integritu nebo důvěrnost této sítě a služby, uchovávaných, předávaných nebo zpracovávaných dat nebo souvisejících služeb, které tato síť nebo služba elektronických komunikací nabízí nebo které jsou jejich*

[11] Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

[12] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.

[13] Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů.

[14] K péči řádného hospodáře viz blíže příslušná ustanovení zákona č. 89/2012 Sb., občanský zákoník (OZ), a zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích; ZOK) - zejm. § 159 odst. 1 OZ či § 51 ZOK.

[15] K rozsahu povinností v oblasti bezpečnosti a integrity sítí a služeb elektronických komunikací včetně krizových stavů viz blíže ustanovení § 98-99 ZEK.

[16] K předepsané úrovni bezpečnosti viz ustanovení § 98 odst. 1 ZEK.

prostřednictvím přístupné.[17] **Jinými slovy, regulace v odvětví elektronických komunikací již dnes vyžaduje, aby provozovatelé sítí a poskytovatelé služeb přijali potřebná opatření k ochraně infrastruktury i služeb.** O závažném narušení bezpečností sítě a služeb a ztrátě integrity sítě pak mají regulované subjekty povinnost informovat ČTÚ a uvést, jaká nápravná opatření plánují v jakém termínu zavést.[18]

Na plnění uložených povinností dohlíží ČTÚ a může regulované osobě uložit povinnost provést na své náklady bezpečnostní audit nezávislým kvalifikovaným subjektem. Výsledy auditu následně ČTÚ zhodnotí s cílem posoudit úroveň bezpečnosti regulované osoby.[19]

Vzhledem ke svému celospolečenskému významu mají regulované subjekty také povinnost zajistit připravenost na krizové stavy a vyhotovit za tím účelem technickoorganizační pravidla v rozsahu určeném prováděcím předpisem k ZEK.[20]

Je tedy zjevné, že již existující regulace odvětví elektronických komunikací zajišťuje bezpečnost včetně integrity sítí a služeb a ČTÚ má pravomoc dohledu a správního trestání zjištěných povinností v této oblasti.[21]

2.2. Povinnosti uložené regulací kybernetické bezpečnosti

Regulace kybernetické bezpečnosti prochází zásadní změnou v důsledku transpozice směrnice NIS2[22] do českého právního řádu. Výsledkem bude nahrazení stávajícího zákona č. 181/2014 Sb., o kybernetické bezpečnosti („**ZKB**“), novým zákonem o kybernetické bezpečnosti („**nZKB**“). Navrhovaný Mechanismus zamýšlí NÚKIB začlenit do nZKB **nad rámec požadavků směrnice NIS2.[23]**

ZKB upravuje povinnosti provozovatelů určených systémů a služeb včetně odvětví elektronických komunikací. Mobilní operátoři tak mají podle ZKB povinnost "*[...] zavést a provádět vhodná a přiměřená bezpečnostní opatření pro sítě elektronických komunikací a informační systémy, které využívá v souvislosti se zajišťováním své služby, přičemž tato bezpečnostní opatření zohledňují zajištění bezpečnosti informací, zvládání kybernetických bezpečnostních incidentů, řízení kontinuity činností, monitorování, audit, testování a soulad s mezinárodními předpisy.*“[24]

[17] *Ibid.*

[18] K rozsahu informační povinnosti viz blíže ustanovení § 98 odst. 4 ZEK.

[19] K povinnosti provést bezpečnostní audit viz blíže ustanovení § 98 odst. 6 ZEK.

[20] K povinnosti vytvořit technickoorganizační pravidla pro krizové stavy viz ustanovení § 99 odst. 1 ZEK.

[21] K řešení deliktů viz blíže ustanovení § 118 odst. 14 písm. f)-h) ZEK.

[22] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii, publikováno v Ústředním věstníku Evropské unie, L333/80.

[23] K podrobnostem rozsahu Mechanismu nad rámec požadavků evropského práva ve směrnici NIS2 viz blíže podkapitola 4.1.

[24] K rozsahu povinnosti viz blíže ustanovení § 4 odst. 3 ZKB.

V kontextu návrhu Mechanismu je významné, že **již dnes ZKB ukládá mj. povinnost přijmout organizační opatření včetně (i) stanovení bezpečnostních požadavků na dodavatele**,[25] (ii) řízení aktiv[26] a (iii) řízení kontinuity činností.[27]

Jako prováděcí předpis k ZKB vydal NÚKIB vyhlášku č. 82/2018 Sb., o kybernetické bezpečnosti, která ukládá ca 900 podrobných požadavků, které jsou mobilní operátoři povinni zavádět jako technickoorganizační opatření pro vybraná aktiva a služby v rámci své činnosti.

Je zjevné, že stát vtělil rozsah regulace kybernetické bezpečnosti do ZKB a vymezil také odpovídající pravomoc NÚKIB s cílem zajistit maximální ochranu strategicky významné infrastruktury v odvětví elektronických komunikací. V souladu s požadavky evropského práva se nové požadavky směrnice NIS2 v rámci její transpozice stanou součástí nZKB a tím zajistí maximální ochranu téže infrastruktury na nové úrovni včetně regulace dodavatelů i bez zavedení navrhovaného Mechanismu.

2.3. Povinnosti uložené regulací krizového řízení

Vzhledem ke svému významu v rámci kritické infrastruktury státu mají mobilní operátoři také povinnosti uložené ZKŘ jako subjektu kritické infrastruktury určené podle nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

Cílem těchto povinností je zajistit připravenost určených subjektů kritické infrastruktury na krizové stavy a poskytovat součinnost orgánům krizového řízení státu. Součástí uložených povinností je mj. vypracování plánů krizové připravenosti stanovící postupy na ochranu funkce svých prvků kritické infrastruktury.[28]

Krizová legislativa prochází obdobnou změnou jako oblast kybernetické bezpečnosti, když stávající ZKŘ nahradí nový zákon jako transpoziční norma evropské směrnice CER.[29] **Navrhovaný Mechanismus nemá oporu ani ve směrnici CER a jde nad její rámec.**

Je zjevné, že povinnost zajistit poskytování služeb a funkčnost určených prvků strategicky významné infrastruktury státu vyplývá již dnes pro mobilní operátory také z legislativy v oblasti krizového řízení a stát tím stanoví požadavky na zajištění svých základních funkcí i bez zavedení navrhovaného Mechanismu.

[25] Uložení povinnosti viz ustanovení § 4 odst. 2 písm. e) ZKB.

[26] Uložení povinnosti viz ustanovení § 4 odst. 2 písm. f) ZKB.

[27] Uložení povinnosti viz ustanovení § 4 odst. 2 písm. l) ZKB.

[28] K povinnosti vypracovat plán krizové připravenosti viz ustanovení § 29b ZKŘ.

[29] Směrnice Evropského parlamentu a Rady (EU) 2022/2557ze dne 14. prosince 2022 o odolnosti kritických subjektů.

3. Mobilní operátoři bezpečnost a odolnost svých sítí zajišťují

Jak uvedeno výše, regulační předpisy stanoví rozsáhlé povinnosti v oblasti bezpečnosti a zajištění integrity sítí a služeb. **Mobilní operátoři však usilují o maximální dosažitelnou úroveň bezpečnosti a odolnosti svých sítí nejen k naplnění regulačních požadavků, ale také pro zajištění svých strategických cílů. Bez naplnění vysokých standardů bezpečnosti a odolnosti by mobilní operátor ztratil schopnost vykonávat svou obchodní činnost.**

O rozsahu investic síťové infrastruktury vypovídají mj. údaje ČTÚ, podle kterých dosáhly v roce 2022 investice do telekomunikačních sítí v České republice výše 17,1 miliardy Kč, z toho 8,5 miliardy Kč do mobilních sítí.[30] Také s ohledem na vysokou investiční náročnost volí provozovatelé telekomunikačních sítí dodavatele, kteří zajistí dlouhodobou provozuschopnost, rozvoj, bezpečnost a odolnost dodaných technologií.

3.1. Výběr dodavatele síťové technologie trvá i přes 18 měsíců

Výběr dodavatele technologií pro výstavbu a provoz telekomunikačních sítí je výstupem náročného procesu, který trvá 18 a více měsíců a hodnotí tisíce konkrétních parametrů popsaných na stovkách stran dokumentace. Vzhledem k výši nákladů, dlouhodobosti smluvních vztahů a složitosti výměny dodavatelů jde o jeden z nejkritičtějších a nejpečlivěji řízených procesů v telekomunikacích. Operátoři přitom využívají zkušeností a poznatků v rámci nadnárodních skupin, jejichž součástí jsou.

Telekomunikační sítě jsou mimořádně složitým souborem hardwarových a softwarových komponent od množství dodavatelů z více zemí. I přes zažité vnímání, že veškeré síťové technologie dané sítě dodává pouze jeden ze tří největších výrobců (evropské nadnárodní společnosti Ericsson a Nokia a čínská společnost Huawei**) jsou integrální součástí každé sítě desítky dalších dodavatelů, jako jsou například další velké nadnárodní korporace – americké společnosti Cisco, Juniper, Dell, HP Enterprise, Adtran nebo VMware.**

Rozhodnutí o zahájení výběru dodavatelů pro telekomunikační sítě dělá operátor z řady důvodů, jako jsou například (i) změna komerčních podmínek, (ii) výměna technologií v důsledku jejich vývoje anebo (iii) úprava podmínek podpory a údržby. Před výběrem dodavatele hodnotí zadavatelé tisíce předem stanovených parametrů, například v oblastech jako jsou (i) odolnost a bezpečnost, (ii) garantovaná dostupnost, (iii) kompatibilita s technologiemi jiných dodavatelů, (iv) plány technologického rozvoje, (v) energetická efektivita, (vi) úroveň podpory a údržby a (vii) zajištění aktualizací. Výsledky testování představují jeden z pokladů pro výběr dodavatele. Výhodou nadnárodních skupin je, že pro takové testování mohou využívat početné týmy a zajistit rozsah prověření, který by pro malého operátora v jedné zemi byl obtížně dosažitelný.

Vedle investic do síťových technologií investovali mobilní operátoři desítky miliard Kč do získání práv využití kmitočtových přídělů v aukcích a při pravidelné obnově kmitočtů. Protože platí, že bezpečnost a spolehlivost rovná se předpoklad podnikatelského úspěchu, **za žádných okolností**

[30] K rozsahu investic do telekomunikačních sítí viz Český telekomunikační úřad – Zpráva *o vývoji trhu elektronických komunikací se zaměřením na rok 2022,* str. 18. Online dostupné na internetových stránkách ČTÚ zde: https://www.ctu.cz/sites/default/files/obsah/stranky/472017/soubory/zovt_2022.pdf. [cit. 2023-12-03].

telekomunikační operátor nesleví z požadavků odolnosti a bezpečnosti výměnou za nižší cenu, protože by tím ohrožoval sám své vlastní podnikání.

Mobilní operátoři kontinuálně usilují o diverzitu dodavatelů ve svých sítích, aby tak zvýšili jejich odolnost a bezpečnost. V přenosových sítích vyplývá diverzita dodavatelů mimo jiné z množství externích dodavatelů poskytujících jednotlivé optické trasy v různých částech území České republiky. Pro rádiovou přístupovou síť RAN se v důsledku inovací brzy otevřou nové možnosti v podobě technologie Open RAN, která umožňuje kombinaci prvků více dodavatelů.

3.2. Kritickou částí sítě je její jádro

Mobilní telekomunikační síť se skládá ze tří hlavních částí: jádro sítě (core), přenosová síť (transmission network) a rádiová přístupová síť (RAN).

Signál z koncového zařízení, jako je například mobilní telefon, modem anebo zařízení vstupuje prostřednictvím rádiových kmitočtů do mobilní telekomunikační sítě přes RAN. Z antény umístěné na věži nebo střeše přivádí kabelové rozvody signál do technologie základnové stanice, která signál předává přenosové síti, jejímž prostřednictvím signál putuje do jádra sítě.

Jádro sítě zajišťuje nastavení služeb, ověření uživatele, směrování provozu, přidělování technických prostředků (např. IP adresy) a další důležité funkce nezbytné pro řádné fungování sítě a služeb. Kritičnost jádra sítě spočívá zejména v tom, že na něm zcela závisí poskytování regulované služby a omezením jeho funkčnosti, resp. vyřazením z provozu tak není možné regulovanou službu poskytovat. **Protože výpadek jádra sítě by ochromil funkčnost celé sítě, zavádí mobilní operátoři řadu opatření k posilování jeho odolnosti.**

Přenosová síť a rádiová přístupová síť jsou od jádra sítě oddělené a stejně tak jsou oddělené i mezi svými jednotlivými částmi. Nefunkčnost jedné části přenosové nebo rádiové přístupové sítě proto nezpůsobí nefunkčnost jejich dalších částí. Krátkodobé výpadky jsou běžnou součástí provozu sítě například při výměně technologií, výpadku dodávek elektrické energie anebo poruše. Mobilní operátoři takové situace umí řešit a pro provoz anebo bezpečnost sítě nepředstavují hrozbu.

Z výše uvedeného vyplývá podstatný a zjevný rozdíl mezi kritičností jádra a ostatních částí sítě. Pokud platí záměr NÚKIB zahrnout do regulace v rámci Mechanismu pouze nejkritičtější části sítě, musí to být právě její jádro.

3.3. Sítě a služby jsou dostupné i při nenadálých událostech

Základním požadavkem na mobilní telekomunikační sítě je zajištění dostupnosti základních služeb (hlasová služba, datová služba, SMS). Tomu odpovídá plánování a výstavba sítí tak, aby při výpadku omezeného počtu prvků došlo k minimálnímu omezení poskytovaných služeb.

Datová centra jsou proto plánována tak, aby při výpadku jednoho z nich mohla zajištění provozu převzít další a zákazník výpadek nezaznamenal. Optické trasy přenosové sítě se budují tak, aby v případě přerušení kabelu mohl provoz procházet jinou částí sítě a nedošlo k omezení služeb.

Základnové stanice v rádiové přístupové síti jsou vybavené akumulátory zajišťujícími po přechodnou dobu dodávku elektrické energie v případě výpadku její dodávky. Datová centra v jádru sítě jsou vedle akumulátorů vybavena také naftovými generátory elektrické energie.

Vzhledem k tomu, že krátkodobé výpadky mohou být způsobené také poruchou některého z prvků síťové technologie, požadují mobilní operátoři po svých dodavatelích krátké termíny výměny nefunkčních prvků. Pro snížení rizik souvisejících s logistickými řetězci proto mobilní operátoři, resp. jejich dodavatelé, využívají snadno dosažitelných meziskladů.

Mobilní operátoři testují technologickou odolnost a zavádí opatření, které ji dále zvyšují. V souladu s požadavky právních předpisů také vypracovávají plány krizové připravenosti a jsou schopni řešit širokou škálu událostí. Tuto schopnost prokázali mimo jiné v době pandemie nemoci Covid-19, kdy řadu situací řešili ve vzájemné součinnosti s cílem zajistit propustnost sítí zatížených zvýšením datového provozu v důsledku celonárodního přechodu na práci z domova.

Příprava na mimořádné události je běžnou součástí činnosti mobilních operátorů a je také součástí již existujících povinností uložených regulačními právními předpisy.[31] Mobilní operátoři v souladu s těmito regulačními normami i vlastní řídící dokumentací řídí svá kritická aktiva, vyhotovují plány krizové připravenosti a prověřují vhodnost opatření v simulovaných cvičeních zahrnujících výpadky určených prvků své infrastruktury. Orgány veřejné moci vykonávají v této oblasti dohled a dosud neidentifikovaly žádné závažné porušení povinností uložených mobilním operátorům obecně závaznými právní předpisy.

Mobilní operátoři by vzhledem k existujícím opatřením, pružnému přemisťování technologií a mimořádným postupům dokázali za vysokých nákladů řešit také zastavení dodávek síťových komponent od svých dodavatelů. [32]

[31] K přehledu existující regulace viz blíže kapitola **Chyba! Nenalezen zdroj odkazů.** tohoto dokumentu.

[32] Ke schopnosti mobilních operátorů řešit zastavení dodávek viz např. článek na serveru lupa.cz ze dne 15. 11. 2023: „Co když nám Čína utne dodávky? Sítě jsme i tak schopní provozovat dva roky, říkají čeští operátoři.“ Online dostupné zde: https://www.lupa.cz/clanky/co-kdyz-nam-cina-utne-dodavky-site-jsme-i-tak-schopni-provozovat-dva-roky-rikaji-cesti-operatori/. [cit. 2023-11-30].

4. NÚKIB navrhuje regulaci dodavatelů do telekomunikačních sítí

Nad rámec rozsáhlé regulace, kterou přináší NIS2 a transpoziční norma nZKB navrhuje NÚKIB zavést také tzv. mechanismus prověřování bezpečnosti dodavatelského řetězce („**Mechanismus**“). Deklarovaným cílem návrhu Mechanismu je zajistit pro NÚKIB pravomoc omezit anebo zakázat rozsah dodávek konkrétních dodavatelů, pokud by takové dodávky mohly ohrozit bezpečnost České republiky. Kritéria pro omezení či zákaz dodávek nespočívají v hodnocení kybernetické bezpečnosti, ale v geopolitických a ideologických hlediscích.

Přestože mobilní operátoři podporují posilování národní bezpečnosti, považují předložený návrh Mechanismu za nepřiměřený, nákladný a neúčinný. V tomto smyslu zaslali prostřednictvím Asociace provozovatelů mobilních sítí („APMS“) velké množství věcných připomínek, jejichž obsah je v zásadě shodný s připomínkami dalších připomínkovatelů včetně tzv. povinných připomínkových míst jako jsou Úřad vlády České republiky, ministerstva vlády České republiky, Hospodářská komora České republiky anebo Svaz průmyslu a dopravy České republiky.

Naprostou většinu vznesených připomínek NÚKIB bohužel zamítl a Mechanismus tak zůstává v kontextu kybernetické bezpečnosti nevhodným regulačním nástrojem navrženým v rámci nZKB.

4.1. Navržený Mechanismus překračuje rámec evropského práva

NÚKIB navrhuje regulovat prostřednictvím opatření obecné povahy bezpečnostně významné dodávky zejména technických, výpočetních, programových nebo komunikačních prostředků směřující do kritických částí strategicky významných služeb. **Rozsah regulace není v tuto chvíli známý s ohledem na to, že NÚKIB pro sebe navrhuje pravomoc upravit rozsah regulace až po nabytí účinnosti nZKB vlastními vyhláškami.** Legislativní proces, v jehož rámci jsou vyhlášky přijímány, je přitom výrazně redukovaný oproti procesu přijetí zákona, možnost bránit se vadnému návrhu vyhlášky je tedy omezena a bez ohledu na dopady nepodléhá schválení Parlamentem České republiky.

Výstupem takto pojaté regulace má být omezení rozsahu dodávek vybraných dodavatelů, resp. jejich zákaz. O takových dodavatelích budou mít povinnost poskytovatelé strategicky významných služeb zjišťovat a evidovat řadu informací a hlásit je NÚKIB.

Transpozice směrnice NIS2 podle dřívějších odhadů cca zdesetinásobí počet regulovaných subjektů také na střední a menší podniky a může se nově týkat 6-8 tisíc podnikatelů.[33] Mechanismus přitom rozsah regulačních povinností subjektů ve vybraných odvětvích a s tím související administrativní zátěž dále zvýší, a to výrazně nad rámec požadavků směrnice NIS2, která sama o sobě mechanismus, tak jak ho pojímá nZKB, neobsahuje. Mechanismus je čistě národní iniciativou, která nemá svůj podklad ve směrnici NIS2.

Základním principem návrhu Mechanismu je, že NÚKIB na základě jemu dostupných informací zhodnotí parametry pro určení rizikovosti dodavatele, které si sám zamýšlí stanovit interní směrnicí, a na základě tohoto hodnocení rozhodne o rozsahu povolených dodávek konkrétního dodavatele. Rozsah zákazu dodávek, tedy na jaké části sítě se případný zákaz bude vztahovat, určuje NÚKIB

[33] K odhadovanému počtu regulovaných subjektů blíže viz článek: „*NÚKIB představuje evropskou směrnici NIS2*“ ze dne 7. září 2022 publikovaný na internetových stránkách NÚKIB. Online dostupné zde: https://www.nukib.cz/cs/infoservis/aktuality/1874-nukib-predstavuje-evropskou-smernici-nis2/. [cit. 2023-12-03].

prostřednictvím vyhlášky o nepominutelných funkcích. Dle současné verze vyhlášky regulované části sítě zahrnují jak jádro sítě, tak rádiovou část navzdory podstatnému rozdílu v jejich kritičnosti.

Hodnocené parametry se nemají vztahovat ke kybernetické bezpečnosti, ale ke vnitropolitickému uspořádání země původu dodavatele. Hodnotit se tak má například úroveň demokracie dané země, její soudní systém, právní režim bezpečnostních služeb apod.[34] Hodnotící kritéria ani pohled NÚKIB na jejich rizikovost součástí návrhu nZKB nejsou. NÚKIB opakovaně deklaroval, že informace, podle kterých bude dodavatele hodnotit, nemusí být veřejné, a tedy je nebude s dodavateli ani regulovanými poskytovateli služeb sdílet.

Na základě vlastního (neveřejného) zhodnocení vnitropolitického uspořádání země původu dodavatele navrhuje NÚKIB vydání opatření obecné povahy („OOP"), kterým stanoví podmínky pro dodávky hodnoceného dodavatele včetně jejich omezení nebo úplného zákazu. Vydání OOP zamýšlí NÚKIB projednat s blíže nespecifikovanými **vybranými ústředními správními úřady, mezi něž dle posledního návrhu NÚKIB nepatří formou závazného stanoviska sektoroví regulátoři** (zejm. ČTÚ a ERÚ), kteří jinak mají ve své oborové legislativě uložené pravomoci a povinnosti týkající se regulace jim svěřených odvětví. OOP také NÚKIB zamýšlí sdílet pro informaci anebo projednání s Bezpečnostní radou státu („**BRS"**). Návrh Mechanismu proces sdílení informací a zapojení ústředních správních orgánů neobsahuje.

Navržená forma regulace prostřednictvím OOP znamená, že proti omezení, resp. zákazu dodávek není možné podat řádný opravný prostředek, jak je to obvyklé ve správním řízení, a je možné jej napadat pouze žalobou ve správním soudnictví. Poskytovatelé strategicky významných služeb ani nejsou účastníky (správního) řízení o vydání OOP. Navzdory tomu je důsledkem vydání OOP jeho závaznost pro všechny regulované subjekty.

Probíhající diskuse o návrhu Mechanismu pouze obsahují možnost, že by NÚKIB měl požádat o závazné stanovisko Ministerstvo průmyslu a obchodu, Ministerstvo zahraničních věcí a Ministerstvo vnitra v těch případech, kdy by v důsledku regulace mělo dojít k výměně již realizovaných dodávek před uplynutím doby jejich odepisování nebo ve lhůtě kratší než 5 let. Součástí diskusí je řešení náhrady škody například v důsledku předčasné výměny, ale samotný návrh Mechanismu řešení neobsahuje.

Důsledkem navrhovaného Mechanismu by tedy *de facto* i *de iure* byla nezávislá pravomoc NÚKIB regulovat na základě vlastních principů a pravidel dodavatele do libovolného odvětví v gesci kteréhokoli ministerstva vlády České republiky a libovolného regulačního úřadu. V kontextu českého právního řádu je takto široce pojatá působnost jedinečná a nemá srovnání s působností kteréhokoli jiného ústředního správního úřadu.

4.2. Na nedostatky Mechanismu upozorňuje soukromý sektor i orgány veřejné moci

Návrh Mechanismu nejenom významně přesahuje rámec regulace požadovaný směrnicí NIS2, ale koncentrací moci výkonné a legislativní porušuje princip dělby moci a tím porušuje základní ústavní

[34] Blíže viz Teze prováděcích právních předpisů k navrhované právní úpravě nZKB – Vyhláška o kritériích rizikovosti dodavatele. Online dostupné zde: https://odok.cz/portal/veklep/material/ALBSCSSFKU7S/. [cit. 2023-12-05].

principy, přesahuje působnost NÚKIB zaváděním pravomoci hodnotit vnitropolitické uspořádání země původu dodavatele, zvyšuje administrativní zátěž podnikatelů a nejistotu a hrozí způsobením významných škod na straně soukromého i veřejného sektoru, bez naplnění účelu Mechanismu, tedy zajištění vyšší míry bezpečnosti. Většinu připomínek **(povinných) připomínkových míst v tomto smyslu NÚKIB zamítl.**

APMS má za to, že takto pojatá regulace je v rozporu s principy právního státu a je nezbytné ji zásadně přepracovat, pokud se má stát součástí českého právního řádu.

4.2.1. Rozsah Mechanismu je nepřiměřeně široký

Návrh Mechanismu zahrnuje možnost regulace všech tří hlavních částí mobilních telekomunikačních sítí (jádro – core, přenosová síť – transmission, rádiová přístupová síť – RAN)[35]. Vzhledem k tomu, že kritickou částí síťové infrastruktury je pouze její jádro, jehož napadením je možné vyřadit z provozu celou síť, není důvod do regulace zahrnovat také další částí sítě. **Námitky, že návrh Mechanismu zahrnující všechny části sítě není odůvodněný a je nepřiměřený, však NÚKIB zamítl.**

NÚKIB opakovaně deklaroval záměr regulovat dodavatele pouze do kritických částí telekomunikačních sítí. Současný návrh vyhlášky o nepominutelných funkcích k nZKB však zahrnuje nejenom jádro sítě (jako jedinou skutečně kritickou část mobilních telekomunikačních sítí), ale zahrnuje také přenosovou síť a dokonce rádiovou přístupovou síť (RAN).

APMS souhlasí s tím, že kritičnost jádra mobilní telekomunikační sítě ospravedlňuje jeho zahrnutí do regulace bezpečnosti dodavatelského řetězce. Zařazení dalších částí sítě však považuje za nesprávné a nepřiměřené. Vzhledem k charakteru těchto částí sítě[36] nezpůsobí výpadek jedné její části vyřazení celé sítě z provozu a nemá přímý okamžitý dopad na významnou nedostupnost regulované služby. Proto by přijetí opatření ve vztahu k přenosové síti a rádiové přístupové síti mělo následovat režim nZKB a jeho standardní regulační požadavky.

I přesto ve svém návrhu APMS představuje nad rámec současných regulačních požadavků další bezpečnostní opatření, která lze přijmout pro zbylé části sítě, aby byla zajištěna vyšší míra bezpečnosti dodavatelského řetězce.

Navržený rozsah Mechanismu je tedy nepřiměřený vzhledem k účelu regulace a jejím předpokládaným dopadům.

4.2.2. NÚKIB by získal bezprecedentně koncentrované pravomoci napříč odvětvími

Návrh Mechanismu předpokládá, že NÚKIB samostatně stanoví rozsah regulace (dotčených aktiv), stanoví hodnotící kritéria bezpečnosti dodavatelského řetězce, na základě vlastní metodologie provede hodnocení a samostatně rozhodne o omezení, resp. vyloučení konkrétního dodavatele. Tím by ve své působnosti nejenom spojil legislativní a výkonné pravomoci, ale mohl by zasahovat do regulovaných odvětví v gesci jednotlivých ministerstev vlády České republiky a

[35] K vysvětlení jednotlivých pojmů a jejich funkce v mobilní telekomunikační síti blíže viz kapitola **Chyba! Nenalezen zdroj odkazů.** tohoto dokumentu.

[36] *Ibid.*

ústředních správních úřadů. **Námitky, že takováto nekontrolovaná koncentrace moci neodpovídá principům demokratického právního státu a porušuje ústavní principy, však NÚKIB bez dalšího zamítl.**

Návrh Mechanismu tak požaduje zavést nový postup k již existujícímu (prakticky shodnému) procesu prověřování zahraničních investic za účasti dotčených orgánů veřejné moci a vlády České republiky, přestože východiska Mechanismu i prověřování zahraničních investic jsou téměř stejná.[37] Podobnost obou procesů přitom jednoznačně vybízí k následování postupu prověřování zahraničních investic také v Mechanismu zejména vzhledem k podobnosti hodnocených kritérií i segmentů národního hospodářství.

Podle návrhu Mechanismu si NÚKIB může vyžádat od ministerstev nebo jiných orgánů veřejné moci stanovisko k rizikovosti konkrétního dodavatele, avšak záleží na jeho vlastním uvážení. Pro vydání samotného OOP stanovujícího rozsah omezení dodávek konkrétního dodavatele však takové stanovisko (pokud si je NÚKIB vyžádá) není závazné. **V důsledku takto navržené pravomoci může NÚKIB bez dalšího zasahovat také do regulovaných odvětví, jako jsou telekomunikace, energetika, zdravotnictví a další, v gesci jiných ministerstev vlády České republiky a zcela je obejít.** Návrh Mechanismu sice počítá s formálním zapojením BRS, avšak pouze v režimu „pro informaci", resp. v nejzávažnějších případech pak projednání, přičemž kritéria závažnosti návrh Mechanismu neobsahuje.

Vzhledem k nezávislému postavení NÚKIB jako ústředního správního orgánu by mohlo jím vydané OOP obsahovat jakákoli omezení pro jakéhokoli dodavatele v jakémkoli odvětví. Protože také rozsah regulace a hodnotící kritéria si NÚKIB má určit sám, stal by se tak skutečným *superúřadem* ve struktuře orgánů veřejné moci v České republice s bezprecedentní působností a pravomocemi.

Takto široce navržené pravomoci mimo hlavní působnost NÚKIB v oblasti kybernetické bezpečnosti není možné akceptovat, protože by vedla k následujícím důsledkům:

1. NÚKIB by dle navržené právní úpravy samostatně určil rozsah regulovaných služeb, a to buď vlastní vyhláškou o regulovaných službách anebo vlastním rozhodnutím.
2. NÚKIB by samostatně vyhláškou určoval nepominutelné funkce stanoveného rozsahu, které jsou zásadní pro určení prvků spadajících pod Mechanismus.
3. NÚKIB by samostatně formou interního předpisu určil kritéria rizikovosti dodavatele, aniž by tato kritéria byla předem známa, čímž by se následné hodnocení stalo nepředvídatelným, netransparentním a prakticky nepřezkoumatelným.
4. NÚKIB by samostatně na základě vlastních kritérií provedl hodnocení dodavatele a následně rozhodoval o vydání opatření obecné povahy, pro které není stanovena jakákoli limitace, podmínky, ani obsahové náležitosti
5. NÚKIB by mohl rozhodovat bez závazného stanoviska jiných orgánů veřejné moci i v případech, kdy s nimi opatření obecné povahy předem projednal, a to i v nejzávažnějších

[37] K procesu prověřování zahraničních investic blíže viz zákon č. 34/2021 Sb., zákon o prověřování zahraničních investic a o změně souvisejících zákonů (zákon o prověřování zahraničních investic).

případech, kdy má být předloženo opatření obecné povahy (OOP) k projednání alespoň Bezpečnostní radě státu.

Takto bezprecedentní a nekontrolovaná koncentrace moci je v demokratickém právním státě nepřijatelná. Důkazem nepřijatelnosti takové působnosti a pravomocí je například excesivní postup Finanční správy při vydávání zajišťovacích příkazů v daňových řízeních, které vedly k likvidaci řady fungujících podniků.

4.2.3. Návrh procesu posuzování dodavatelů je nepředvídatelný, netransparentní, arbitrární, a proto nedůvěryhodný a hrozící svévolí

Přestože je NÚKIB ústředním správním orgánem pro oblast kybernetické bezpečnosti, návrhem Mechanismu by rozhodoval na základě vlastního hodnocení vnitropolitických poměrů libovolného státu a bez nutnosti získávat předchozí vyjádření jiných orgánů veřejné moci by mohl zasáhnout do mezinárodněpolitických vztahů České republiky tím, že zakáže dodávky z jím určených zemí. **Na základě navrženého Mechanismu by zakázané dodávky nemusely vůbec představovat kyberbezpečnostní hrozbu, protože s hodnocením kyberbezpečnosti Mechanismus nepočítá a jako podklad pro vydání OOP omezujícího či zakazujícího dodávky se nevyžaduje.**

NÚKIB v Mechanismu navrhuje hodnotit nikoli dodavatele ale zemi jeho původu. **NÚKIB by tak nehodnotil kybernetickou bezpečnost ani důvěryhodnost příslušného dodavatele, ale vhodnost vnitřního uspořádání země jeho původu. Vůbec by tak nehodnotil schopnost dodavatele splnit požadavky nZKB ani rizikovost jeho dodávek. Současně také NÚKIB v rámci hodnocení nebere v potaz již zavedená bezpečnostní opatření ze strany regulovaných subjektů. Schopnost regulovaného subjektu ošetřit rizika identifikovaná ze strany NÚKIB totiž nejsou součástí hodnocení rizikovosti dodavatele. Takto navržená hodnotící kritéria kritizovali silně nejen zástupci soukromého sektoru, ale například také jedna ze zpravodajských služeb – Úřad pro zahraniční styky a informace. Jejich výhrady jsou v souladu s dalšími již uvedenými nedostatky k návrhu Mechanismu, když varují před velkým prostorem ke svévoli ze strany NÚKIB a upozorňují na to, že takto pojaté hodnocení má spíše charakter politické úvahy.**

Pod tíhou kritiky NÚKIB v ústním vypořádání připomínek uvedl, že návrh Mechanismu upraví a kritéria rizikovosti dodavatele nebude vydávat formou vyhlášky, ale vlastním předpisem. Jediným hodnotícím kritériem uvedeným v novém zákoně o kybernetické bezpečnosti by tak zůstala „možná hrozba pro bezpečnost České republiky, vnitřní či veřejný pořádek“, aniž by NÚKIB vysvětlil význam anebo obsah tohoto kritéria.[38] **V důsledku této změny se návrh Mechanismu ještě zhoršil vzhledem k tomu, že jediné hodnotící kritérium opět připouští benevolenci a lze pod něj podřadit prakticky cokoli, a vzhledem k tomu, že kritéria rizikovosti bude NÚKIB nadále vydávat vnitřním předpisem, tedy neveřejně.**[39]

[38] Viz § 29 nZKB ve znění návrhu zákona po zohlednění připomínek ze strany NÚKIB.

[39] Uvedené vyplývá z ústního sdělení NÚKIB při vypořádání připomínek, jakož i vypuštění vyhlášky o kritériích rizikovosti dodavatele z § 28 odst. 4 nZKB ve znění návrhu zákona předloženého do elektronické knihovny k

4.2.4. Určování rozsahu hodnocení vlastními vyhláškami NÚKIB je protiústavní

V rámci Mechanismu NÚKIB navrhl, aby rozsah regulace, tedy na jaké části infrastruktury se případný zákaz dodavatele vztahuje, byl určen v rámci vyhlášky o nepominutelných funkcích. V případě mobilních sítí by to znamenalo, že by NÚKIB sám určoval, na jaké částí sítě (Core/Transmission/RAN) se případný zákaz dodavatele vztahuje. V případě rozsahu regulace takový systém způsobuje nepřijatelnou nepředvídatelnost na straně podnikatelů, kteří své investice plánují na mnoho let dopředu, jelikož NÚKIB by fakticky mohl měnit rozsah regulace jednoduše formou vyhlášky. **Přitom právě rozsah regulace určuje, zda náklady vzniklé zákazem nebo omezením dodavatele budou v řádech jednotek nebo desítek miliard.**

Nad rámec výše uvedeného úprava rozsahu Mechanismu formou vyhlášky také vylučuje **posouzení přiměřenosti** právní úpravy Mechanismu v souladu s principem proporcionality. Vyhláška o nepominutelných funkcích totiž ze své podstaty (jako podzákonný právní předpis) není součástí legislativního procesu nového zákona o kybernetické bezpečnosti, prostřednictvím kterého se Mechanismus zavádí.

Podle článku 4 odst. 1 Listiny základních práv a svobod mohou být povinnosti ukládány „*toliko na základě zákona a v jeho mezích a jen při zachování základních práv a svobod*“.40 Navrhovanou pravomoc NÚKIB určovat rozsah regulace vlastními vyhláškami kritizoval také například Odbor kompatibility Úřadu vlády, když uvedl, že „*Důležité instituty předkladatel plánuje definovat až v prováděcích právních předpisech. Takové řešení se jeví problematické nejenom z pohledu kontroly správné implementace práva EU, ale také z ústavněprávního hlediska, jelikož práva a povinnosti subjektů mají být jasně stanoveny zákonem*.“41

Je nutné říci, že vyhláška o nepominutelných funkcích není jediným sporným aspektem v rámci zamýšlených prováděcích právních předpisů. Za silně problematickou lze také označit otázku určení kritérií rizikovosti dodavatele, na jejichž základě má NÚKIB dodavatele posuzovat. Původní přístup NÚKIB spočíval v návrhu vyhlášky, kterou měl vydat NÚKIB a která by tato kritéria obsahovala. Taková úprava však zakládala právní nejistotu pro poskytovatele strategicky významných služeb i bezpečnostně významné dodavatele, protože kritéria hodnocení rizikovosti se takto mohla v budoucnu významně a snadno změnit změnou vyhlášky - mnoho subjektů v rámci připomínek proto tuto vyhlášku kritizovalo a žádalo přenesení kritérií do nového zákona o kybernetické bezpečnosti.[42] NÚKIB však tomuto odůvodněnému požadavku nevyhověl a naopak učinil krok k ještě větší netransparentnosti a nepřezkoumatelnosti svého rozhodování, když předmětnou vyhlášku zrušil a

připomínkovému řízení. Online dostupné zde: https://odok.cz/portal/veklep/material/ALBSCSSFKU7S/. [cit. 2023-12-05].

[40] K ukládání povinností na základě zákona viz blíže čl. 4 odst. 1 usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součástí ústavního pořádku České republiky (Listina základních práv a svobod).

[41] Viz písemné vypořádání připomínky Odboru kompatibility (vláda) č. 339 v dokumentu vypracovaném NÚKIB: ”Vypořádání připomínek k materiálu s názvem Návrh zákona o kybernetické bezpečnosti”, s. 270.

[42] Viz. např. připomínky Svazu průmyslu a dopravy ČR k nZKB, online dostupné zde: https://odok.cz/portal/veklep/material/pripominky/ALBSCSSFKU7S/.

kritéria rizikovosti, podle nichž má dodavatele posuzovat, mají napříště být neveřejná (pouze ve formě interního předpisu NÚKIB).

Přitom i v případě prověřování zahraničních investic, jehož podstata je takřka shodná s posuzováním bezpečnosti dodavatelského řetězce, jsou základní parametry posuzování dodavatele (investora) stanoveny zákonem. Není zde žádný důvod pro to, aby se v případě nového zákona o kybernetické bezpečnosti u tak zásadních aspektů, jako je určení rozsahu regulace Mechanismu, nebo kritéria rizikovosti dodavatele postupovalo jinak, a to i s ohledem na to, že práva a zejména povinnosti subjektů mají být jasně stanoveny zákonem, jak vyplývá z ústavního pořádku.[43]

S ohledem na závažný ekonomický, právní i administrativní dopad na poskytovatele regulované služby nelze přijmout model právní úpravy, kdy by zejména nepominutelné funkce stanoveného rozsahu či kritéria rizikovosti dodavatele byly stanoveny vyhláškou vydávanou NÚKIB a nikoli zákonem. Ponechání této kompetence v rukou moci výkonné, nikoli zákonodárné, by vedlo k nepřiměřené koncentraci pravomocí v rukou jednoho z orgánů veřejné moci, jak je již uvedeno výše.

4.2.5. Proti omezení či zákazu dodavatele formou OOP není řádný opravný prostředek

NÚKIB zamýšlí v rámci Mechanismu vydávat opatření obecné povahy (**OOP**), kterými by omezil nebo zakázal plnění konkrétního dodavatele. Tento institut je velmi specifický - jde o abstraktně-konkrétní správní akt s konkrétně určeným předmětem (určuje se jím rozsah práv a povinností v konkrétní věci) a s obecně vymezeným okruhem adresátů. Nejde tedy ani o právní předpis, ani rozhodnutí.

Vzhledem k tomu, že OOP není rozhodnutím, nepřísluší ani osobám, které jsou vydáním OOP dotčeny, práva účastníků ve správním řízení - včetně práva vyjádřit se, navrhovat důkazy, nahlížet do spisu či podávat opravné prostředky.

V rámci řízení o vydání OOP mohou dotčené osoby pouze podat připomínky, toť vše. **Proti OOP nelze podat opravný prostředek,**[44] tedy nelze podat odvolání ani rozklad. Je zde možnost podnětem iniciovat přezkumné řízení, ale toto je dozorčím nástrojem, nikoli opravným prostředkem, a na jeho zahájení není právní nárok. Přezkumné řízení tak rozhodně nelze klást na roveň opravnému prostředku, i když se NÚKIB toto snaž tvrdit. Jedinou možností obrany proti OOP tak zůstává žaloba v soudním řízení správním.

Práva dotčených osob - jak poskytovatelů regulovaných služeb, tak dodavatelů - jsou v případě vydání OOP významně omezena, a to v situaci, kdy důsledkem vydání OOP v rámci Mechanismu mohou být až miliardové škody (nejen) na straně dotčených subjektů.

[43] Viz čl. 2 odst. 3 LZPS: "*Každý může činit, co není zákonem zakázáno, a nikdo nesmí být nucen činit, co zákon neukládá*."

[44] Viz § 173 odst. 2 zákona č. 500/2004 Sb., správní řád.

Dalším problematickým aspektem OOP je to, že se případný zákaz či omezení plnění dodavatele má (vzhledem k obecně určenému okruhu adresátů) automaticky vztahovat na všechny povinné osoby Mechanismu. **V rámci OOP tak nelze vzít v potaz individuální aspekty každé povinné osoby, jako jsou např. již zavedená bezpečnostní opatření.** Právě tato zavedená bezpečnostní opatření však mohou být rozhodující pro posouzení, zda se NÚKIBem identifikovaná hrozba může u jednotlivých subjektů vůbec realizovat.

Vzhledem k tomu, jak rozsáhlé předpokládané dopady mají být se zavedením Mechanismu spojené, je tento individualizovaný přístup nutný, a to za účelem minimalizace dopadů nZKB na dotčené subjekty po stránce finanční i administrativní, při současném zajištění vysoké úrovně kybernetické bezpečnosti. Individualizovaným přístupem toho lze dosáhnout. Takto proces posuzování dodavatele (investora) ostatně funguje i u již zmiňovaného zákona o prověřování zahraničních investic, kde zákonodárce nastavil právní úpravu tak, aby se rozhodovalo o konkrétní dodávce (investici) v rámci správního řízení, aby pokud možno minimalizoval zásah státu z moci úřední do činnosti dotčeného subjektu, a aby nedocházelo ke koncentraci rozhodovací moci v rukou jediného orgánu.

Z výše uvedeného plyne, že řízení o případném omezení či zákazu plnění dodavatele by mělo probíhat formou správního řízení, které ústí ve vydání individuálního správního rozhodnutí, umožňuje vzít v potaz individuální aspekty týkající se povinných osob a poskytuje dotčeným osobám větší rozsah práv. Pokud by však zákonodárce trval na vydávání OOP v rámci Mechanismu, pak je nutné, aby v zákoně byly uvedeny limity a konkrétní kritéria pro vydání OOP – tzn. zejména jaké podmínky a v jakém rozsahu musí být splněny pro vydání OOP omezujícího nebo zakazujícího plnění dodavatele. Tento aspekt je zcela zásadní jak z hlediska nutnosti legitimního očekávání dotčených subjektů, tak i hlediska jasnosti, transparentnosti a obecně přezkoumatelnosti obsahu OOP vydaného NÚKIB.

4.2.6. Navržený Mechanismus by zvýšil administrativní zátěž a provozní náklady

Původním záměrem NIS2 a nZKB bylo ochránit evropskou infrastrukturu proti kybernetickým hrozbám. Nadcházející obsáhlá právní úprava nZKB a její důsledné vymáhání ze strany státních orgánů by k tomu cíli vedly.

V téže době objevily inkrementální iniciativy směřující k prevenci dodavatelů technologií z Číny, konkrétně těch od společností Huawei nebo ZTE.[45] Přestože (nebo možná protože) dosud NÚKIB neseznámil provozovatele mobilních sítí se žádnou zranitelností v jimi používaných technologiích společnosti Huawei, rozhodl se NÚKIB navrhnout Mechanismus, kterým měl namísto kyberbezpečnostních důvodů pro omezení, resp. zákaz dodávek využít vlastního hodnocení vnitropolitických poměrů v Číně.[46]

[45] Viz Varování NÚKIB před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation ze dne 17. 12. 2018. Online dostupné na úřední desce NÚKIB zde: https://www.nukib.cz/cs/uredni-deska/. [cit. 2023-12-05]

[46] K popisu části mechanismu zabývajícího se hodnocením vnitropolitických poměrů země původu dodavatelů blíže viz § 29 a násl. nZKB ve znění návrhu zákona po zohlednění připomínek ze strany NÚKIB, jakož i důvodová zpráva k nZKB.

Vzhledem k nedostatku informací o hrozbách, zranitelnostech či rizicích NÚKIB budoucím adresátům regulace nevysvětlil nezbytnost regulace v tak široce navrženém rozsahu. **Návrh Mechanismu však doprovodil požadavkem na zřízení** desítek nových tabulkových míst (dle slov NÚKIB až **52) v NÚKIB a dalších úřadech.[47] Důvodem navýšení počtu úředníků má být prověřování dodavatelů. Je proto důvodná obava, že díky navrženému Mechanismu dojde (i) k navýšení administrativní zátěže soukromého sektoru a růstu jeho nákladů, a (ii) k růstu nákladů na výkon státní správy.** Toto vše v kontextu všech výhrad ukazujících, že regulace je příliš široká a zavádí postupy nekonformní s principy demokratického právního státu.

Mobilní operátoři na to reagovali nabídkou regulace aplikované na kritickou část sítě (jádro), čímž by v zásadě vyřešili jak problém rostoucí administrativy, tak nákladů ve veřejném i soukromém sektoru. NÚKIB však tento návrh dosud odmítá, přestože se jedná o přiměřený rozsah regulace řešící s přijatelnými dopady bezpečnostní hrozby spojené s telekomunikačními sítěmi.

Návrh mobilních operátorů dobrovolně přijmout regulaci kritické části by podpořil vládu České republiky v jejím úsilí zefektivnit výkon veřejné moci, snížit administrativní zátěž a reagovat na rostoucí tlak způsobený růstem nákladů v důsledku inflace a růstem cen energií. NÚKIB však odmítnutím návrhu nadále postupuje proti Programovému prohlášení vlády mj. uvádějícímu, že vláda provede komplexní revizi systému kontrol veřejných prostředků s důrazem na posílení prvků hospodárnosti, efektivity a účelnosti a na snižování administrativní zátěže na straně kontrolovaných osob.[48]

[47] Viz zpráva RIA k navrhované právní úpravě nZKB, s. 4. Online dostupné zde: https://odok.cz/portal/veklep/material/ALBSCSSFKU7S/. [cit. 2023-12-05].

[48] Viz Programové prohlášení vlády z ledna 2022. Online dostupné zde: programove-prohlaseni-vlady-Petra-Fialy.pdf (gov.cz). [cit. 2023-12-05].

5. Mobilní operátoři podporují vyšší míru zabezpečení dodavatelského řetězce

APMS a její členové – mobilní operátoři – podporují úsilí vlády České republiky posilovat odolnost státu proti bezpečnostním hrozbám. Chápou proto potřebu snížit závislost subjektů kritické infrastruktury na dodavatelích s cílem předcházet narušení vybraných činností – služeb – zajišťovaných subjekty kritické infrastruktury a jsou srozuměni s tím, že naplnění tohoto záměru může vyžadovat omezení některých dodávek do kritických částí vybrané infrastruktury.

Je nicméně zřejmé, že navržený Mechanismus a způsob, kterým jej NÚKIB připravil a kterým jej prosazuje v rámci transpozice směrnice NIS2, k takovému výsledku nevede, narušuje důvěru mezi soukromým sektorem a veřejnou mocí a ve svém důsledku může odolnost České republiky naopak poškodit.

Se záměrem podpořit včasnou transpozici směrnice NIS2 přijetím nZKB včetně nástrojů řízení bezpečnosti dodavatelských řetězců proto považujeme za nezbytné přistoupit k následujícím krokům a změnám navrženého Mechanismu:

1. Zahájit otevřený dialog mezi NÚKIB a soukromým sektorem
2. Omezit rozsah Mechanismu na jádro mobilních sítí
3. Zahrnout sektorového regulátora – Českého telekomunikačního úřadu – do přípravy OOP
4. Omezit meziodvětvovou koncentraci pravomocí v rukou NÚKIB
5. Určit rozsah regulace a její principy v nZKB namísto vyhláškách vydávaných NÚKIB
6. Nastavit principy náhrady škody vzniklé zaváděním opatření v důsledku Mechanismu

Podrobné vysvětlení podstaty jednotlivých návrhů obsahují následující podkapitoly.

5.1.1. Zahájení otevřeného dialogu mezi NÚKIB a mobilními operátory

APMS a její členové – mobilní operátoři – považují NÚKIB za odborně vybaveného regulátora v oblasti kybernetické bezpečnosti. S potěšením také sledovali přípravu transpozice NIS2 prostřednictvím nZKB a oceňovali úsilí a otevřenost, s jakou NÚKIB ve velkém předstihu připravoval návrh nZKB v otevřeném dialogu s odbornou veřejností. Po přijetí NIS2 tak byla Česká republika připravena přistoupit k zahájení národního legislativního procesu, který se očekával jako bezproblémový a rychlý právě díky dlouhodobé přípravě ve spolupráci se soukromým sektorem.

Příprava návrhu Mechanismu však byla od otevřené spolupráce při přípravě transpozice NIS2 zcela odlišná. Přes opakovaná setkávání NÚKIB se zástupci soukromého sektoru se nejednalo o konstruktivní dialog, ale spíše o sdílení stále se zpřísňujících pohledů NÚKIB na připravovanou regulaci. Návrhy mobilních operátorů NÚKIB v zásadě zamítal, konkrétní rizika ani zranitelnosti vedoucí k potřebě regulace nesdílel a základním motivem vysvětlujícím rozsah Mechanismu bylo spíše ideologické hledisko boje proti „nedemokratickým státům“, aniž by zástupci NÚKIB tento ideologický rozdíl blíže vysvětlili. Výsledkem tohoto procesu byl možná nejpřísnější návrh regulace bezpečnosti dodavatelského řetězce v EU.

Pro pokračování efektivní spolupráce mezi NÚKIB a mobilními operátory je proto nezbytné obnovit důvěru spočívající na otevřenosti, která umožní pochopit potřeby a nalézt přiměřené řešení prospěšné především pro posílení odolnosti České republiky. V té souvislosti považujeme za nezbytné, aby NÚKIB s mobilními operátory sdílel konkrétní poznatky, hrozby, zranitelnosti a rizika,

jejichž vhodné ošetření může předejít jejich vzniku či minimalizovat dopady a pravděpodobnost vzniku. Nesdílením takových poznatků paradoxně dochází k oslabování odolnosti kritické infrastruktury a oslabování vzájemné důvěry.

5.1.2. Omezení Mechanismu na kritickou část mobilní sítě – její jádro

APMS a její členové jsou srozuměni s potřebou regulace vybraných odvětví a činností. V tom smyslu také dlouhodobě s dotčenými orgány veřejné moci spolupracují. Dlouhodobá zkušenost a poznatky z různých přístupů k regulaci potvrzují, že účinná regulace je pouze ta, která zavádí opatření přiměřená svému účelu. Zatímco nedostatečná regulace poskytuje prostor pro své obcházení, přílišná regulace svazuje podnikatele natolik, že omezuje jejich schopnost účinně rozvíjet hospodářskou soutěž a v souladu s péčí řádného hospodáře a při vědomí vlastní soukromoprávní a veřejnoprávní odpovědnosti volit nejvhodnější řešení identifikovaných problémů.

Jednou z regulovaných oblastí týkající se mobilních operátorů je právě kybernetická bezpečnost. Vedle zákonných pravidel popsaných výše[49] se zabývají statutární orgány a vrcholový management jednotlivých korporací problémy vznikajícími při podnikatelské činnosti a investují svěřené prostředky tak, aby zajistili dlouhodobě odolnou činnost, tedy včetně schopnosti předcházet narušení své činnosti.

Jedním z rizik v oblasti síťové infrastruktury je přílišná závislost na jednom dodavateli, a proto mobilní operátoři mají již dnes ve svých sítích více dodavatelů z různých zemí.[50] Dalším rizikem je nemožnost poskytovat regulované služby v důsledku výpadku síťových technologií například v důsledku kybernetického útoku na některý z prvků mobilní telekomunikační sítě, a proto mobilní operátoři mají vlastní programy k posílení kybernetické bezpečnosti a využívají k tomu mezinárodních zkušeností.

Kritickou částí mobilní telekomunikační sítě je její jádro (angl. *core*).[51] Vyřazením této části sítě je možné omezit její funkčnost. Oproti tomu vyřazením některé z částí rádiové přístupové sítě (angl. *RAN*) anebo přenosové sítě (angl. *transmission*) k vyřazení celé sítě nedojde a nedojde tak neposkytování regulované služby. Jádro sítě je proto kritickou částí, která zasluhuje zvláštní pozornost.

Mobilní operátoři proto považují prioritní zaměření na jádro sítě za přiměřené identifikovaným hrozbám. Případná rizika v dalších částech sítě totiž ošetřují v souladu se ZKB a do budoucna budou řešit v souladu s nZKB, čímž své sítě budou chránit na nejvyšší úrovni.

Také z těchto důvodů APMS dlouhodobě doporučuje stanovit rozsah Mechanismu tak, aby se vztahoval na kritickou část mobilní telekomunikační sítě – její jádro. Současný návrh Mechanismu je však krajním přístupem s nejvyššími transakčními náklady a riziky spojenými s masivní technologickou změnou. Odolnosti a bezpečnosti mobilních telekomunikačních sítí lze dosáhnout méně invazivním způsobem.

---

[49] K přehledu regulačních pravidel dopadajících na mobilní operátory blíže viz kapitola **Chyba! Nenalezen zdroj odkazů.** tohoto dokumentu.

[50] K architektuře sítě blíže viz 3.1 tohoto dokumentu.

[51] K významu jádra sítě pro funkčnost síťové infrastruktury blíže viz podkapitola 0 tohoto dokumentu.

Návrh APMS omezit Mechanismus pouze na jádro mobilních sítí je v souladu s opakovaně deklarovaným záměrem NÚKIB regulovat pouze nejkritičtější části infrastruktury.[52] APMS i její členové se zaměřením regulace na takovou část infrastruktury souhlasí a podporují ji. Protože nejvýznamnějším rizikem je nedostupnost regulované služby, APMS navrhla omezení Mechanismu pouze na jádro sítě, případně další individuálně určené prvky, z důvodů vysvětlených výše.[53]

Pro ostatní aktiva významná pro strategicky významné služby, které nemohou ze své podstaty způsobit nedostupnost služby na kritické úrovni, by mobilní operátoři v souladu s principem přiměřenosti analyzovali rizika identifikovaná při své činnosti anebo identifikovaná NÚKIB a přijímali opatření k jejich ošetření. Svá bezpečnostní opatření by mobilní operátoři evidovali v pravidelně aktualizované bezpečnostní dokumentaci, která by podléhala dohledu ze strany NÚKIB stejně jako ostatní povinnosti vyplývající ze ZKB, resp. nZKB.

Tento systém jsme nazvali kaskádou bezpečnostních povinností, kdy pro tu nejkritičtější část strategické infrastruktury má být dána povinnost řídit se případným zákazem uvedeným v opatření obecné povahy, a pro ty méně kritické části strategické infrastruktury má být nově dána povinnost zohlednit rizika identifikovaná státem a implementovat odpovídající bezpečnostní opatření.

Tento návrh považujeme za dostatečný a přiměřený vzhledem k identifikovaným hrozbám a možnostem řešení v případě, že některá z nich nastane.

Omezení regulace pouze na jádro, tedy stanovení rozsahu Mechanismu, musí být také upraveno přímo v zákoně. Stanovení rozsahu Mechanismu vyhláškou, jak navrhuje NÚKIB, považuje APMS za protiústavní, zejména s ohledem na závažný ekonomický, právní i administrativní dopad Mechanismu na poskytovatele regulované služby. Ponechání této kompetence v rukou moci výkonné, nikoli zákonodárné, by vedlo k nepřiměřené koncentraci pravomocí v rukou jednoho z orgánů veřejné moci, jak je již uvedeno výše.

5.1.3. Zahrnutí závazného stanoviska odvětvového regulátora – Českého telekomunikačního úřadu – jako předpokladu vydání OOP

Český telekomunikační úřad (ČTÚ) je orgánem veřejné moci s působností pro odvětví elektronických komunikací a tomu odpovídajícími regulatorními pravomocemi.[54] ČTÚ má však zároveň uloženou řadu povinností směřujících ke stabilitě a rozvoji odvětví, včetně problematiky infrastruktury, užívaných technologií, interoperability, přeshraniční spolupráce, bezpečnosti, integrity sítí a služeb a odolnosti sítí elektronických komunikací.[55] Zákon proto stanoví pravomoc ČTÚ dohlížet

[52] Viz důvodová zpráva k navrhované právní úpravě nZKB, s. 126. Online dostupné zde: https://odok.cz/portal/veklep/material/ALBSCSSFKU7S/. [cit. 2023-12-05]

[53] K významu jádra sítě pro poskytování regulované služby blíže viz také podkapitola 0.

[54] K rozsahu regulace pro odvětví elektronických komunikací blíže viz zákon č. 127/2005 Sb., o elektronických komunikacích. K působnosti ČTÚ viz § 108 a násl. téhož zákona.

[55] K cílům a základním zásadám regulace blíže viz ustanovení § 4–6 zákona č. 127/2005 Sb., o elektronických komunikacích.

na plnění povinností uložených adresátům regulace, ukládat nápravná opatření v případě zjištěných nedostatků a ukládat ve správním řízení finanční pokuty.[56]

S ohledem na takto určenou odpovědnost je nezbytné zajistit, aby ČTÚ měl možnost se formou závazného stanoviska vyjádřit k regulačním opatřením jiných orgánů veřejné moci, jako je například NÚKIB, která mohou ovlivnit odvětví elektronických komunikací. Obdobný problém předpokládáme také ve vztahu mezi NÚKIB a dalšími regulačními úřady, například Energetickým regulačním úřadem, jehož působnost má být návrhem Mechanismu také dotčena. **Současný návrh Mechanismu však se zapojením žádného z těchto regulátorů do přípravy OOP ve formě závazného stanoviska nepočítá.**

APMS a její členové mají zato, že účast ČTÚ jako odborně vybaveného a zákonem určeného nezávislého správního úřadu pro odvětví elektronických komunikací je na přípravě OOP nezbytná pro předcházení excesů s negativním dopadem do odvětví elektronických komunikací. Stanovisko ČTÚ musí být pro NÚKIB závazné a OOP je musí reflektovat.

5.1.4. Omezit koncentraci pravomocí NÚKIB v souladu s principy dělby moci: zapojení Ministerstva průmyslu a obchodu a vlády

APMS navrhuje vyřešit koncentraci pravomocí NÚKIB navrhovanou pro Mechanismus replikací obdobného zákonného postupu pro prověřování zahraničních investic.[57] V souladu s cílem nezvyšovat, resp. snižovat administrativní zátěž a zefektivňovat výkon veřejné moci by navržené řešení nevyžadovalo zavádění nového procesu s dodatečnými zdroji, ale pouze by se již existující a legislativním procesem schválené řešení využilo také na prověřování dodavatelů do strategicky významné infrastruktury dle Mechanismu.

Vhodnost navrženého postupu vyplývá zejména z následujících již existujících parametrů zákona o prověřování zahraničních investic (ZPZI):

1. Účelem ZPZI je ochrana bezpečnosti České republiky a vnitřního či veřejného pořádku;[58]
2. ZPZI se mj. vztahuje na ty případy, kdy zahraniční investor může získat přístup k informacím, systémům nebo technologiím, které jsou důležité z hlediska ochrany bezpečnosti České republiky nebo vnitřního či veřejného pořádku;[59]
3. Prověřování podle ZPZI se vztahuje mj. na zahraniční investice do oblasti kritické informační infrastruktury;[60]
4. Součástí prověřování zahraničních investic je mj. hodnocení informací poskytnutých zpravodajskými službami a určenými ministerstvy vlády České republiky;[61]

---

[56] K rozsahu přestupů a ukládání pokut viz blíže ustanovení § 118-120 zákona č. 127/2005 Sb., o elektronických komunikacích.

[57] K problematice koncentrace pravomocí v návrhu Mechanismu blíže viz 4.2.2[OBJ]. tohoto dokumentu. K prověřování zahraničních investic blíže viz zákon č. 34/2021 Sb., o prověřování zahraničních investic.

[58] K předmětu právní úpravy blíže viz ustanovení § 1 zákona č. 34/2021 Sb., o prověřování zahraničních investic (”***ZPZI***”).

[59] K určení hranice kontroly zahraničním dodavatelem blíže viz ustanovení § 5 písm. d) ZPZI.

[60] K prověřovaným investicím blíže viz ustanovení § 7 písm. c) ZPZI.

[61] K řízení o prověřování zahraničních investic blíže viz ustanovení § 11 ZPZI.

5. Výsledkem prověření zahraniční investice může být stanovení podmínek její realizace.[62]

Z tohoto přehledu je patrné, že postup ZPZI umožňuje zajistit míru ochrany bezpečnosti České republiky, pro kterou vzniká Mechanismus. Je tedy možné tento existující proces podle ZPZI replikovat také v nZKB pro hodnocení bezpečnosti dodavatelů do strategicky významné infrastruktury.

Hlavní výhodou postupu podle ZPZI je však oproti Mechanismu omezení meziodvětvové koncentrace pravomocí NÚKIB a zapojení dotčených orgánů veřejné moci. Tato výhoda se nejsilněji projevuje v povinném projednání vládou České republiky těch případů, kdy z prověření zahraniční investice vyplyne možnost ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku.[63]

Za obzvláště významné je z tohoto pohledu ustanovení § 13 odst 4 ZPZI, podle kterého *„[V]láda přijme do 45 dnů ode dne, kdy jí byla věc předložena k projednání, usnesení o tom, zda zahraniční investice může představovat ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. Při posuzování věci vláda zohlední možný dopad zahraniční investice na principy demokratického právního státu, ochranu života a zdraví obyvatel, obranu státu, zahraničně politické nebo bezpečnostní zájmy státu, ekonomickou bezpečnost státu a případně další skutečnosti důležité z hlediska ochrany bezpečnosti České republiky nebo vnitřního či veřejného pořádku.“*

Z tohoto ustanovení jednoznačně plyne vůle vlády České republiky a Parlamentu České republiky svěřit rozhodování o takto významných otázkách vládě České republiky, která i díky zapojení dotčených orgánů veřejné moci a dalších subjektů má schopnost posoudit širší mezinárodněpolitické a hospodářské souvislosti postupu vůči konkrétní zahraniční osobě. Vláda České republiky má také schopnost posoudit širší hospodářské a vnitropolitické souvislosti přijatých opatření napříč odvětvími.

Postup navržený Mechanismem je nejenom shodný s procesem prověřování podle ZPZI, ale shodné mohou být také důsledky rozhodnutí o omezení či zákazu plnění konkrétního zahraničního dodavatele. Navíc ZPZI počítá právě s prověřováním ve vztahu ke strategicky významné infrastruktuře České republiky, a proto je v něm definovaný proces vhodný také na prověřování dodavatelů v rozsahu navrhovaného Mechanismu a měl by se pro něj v rámci nZKB použít.

5.1.5. Zakotvení nezbytných náležitostí OOP v nZKB

Návrh Mechanismu umožňuje NÚKIB vydávat opatření obecné povahy (OOP) jako nástroje regulace určujícího pravidla dotčeným adresátům, kteří však nebyli účastníky řízení o jeho vydání a nemají možnost řádného opravného prostředku proti němu.[64]

Replikací postupu upraveného v ZPZI by tento problém odpadl. Má-li však být zachován postup podle Mechanismu včetně vydávání OOP, je nezbytné stanovit jeho náležitosti a podmínky vydání přímo v nZKB.

---

[62] K ukládání podmínek pro realizaci zahraniční investice blíže viz § 12 ZPZI.

[63] K povinnému projednání vládou České republiky blíže viz ustanovení § 13 ZPZI.

[64] K problematičnosti postupu regulace vydáváním OOPblíže viz podkapitoly **Chyba! Nenalezen zdroj odkazů.** a **Chyba! Nenalezen zdroj odkazů.**.

Jako nezbytné se proto jeví upravit ustanovení § 31 nZKB tak, aby obsahovalo podstatné náležitosti a podmínky vydání daného OOP zejména ve vztahu k omezování či zákazu plnění určených dodavatelů.

5.1.6. Zavedení mechanismu náhrady škody

Vzhledem k dlouhodobosti investic do telekomunikační infrastruktury by omezení dodávek či zákaz dodavatele mohlo vyvolat nutnost výměny prvků dotčených regulací podle Mechanismu. Změna dodavatele může způsobit škodu (i) nutností nakoupit nové technologie před uplynutím životnosti těch stávajících, (ii) narušením daňového odepisování vyřazovaných technologií, (iii) zvýšením nákladů na pořízení technologií v situaci, kdy se díky omezení nebo zákazu dodavatele významně zvýší poptávka po produktech omezeného počtu jiných dodavatelů, (iv) vyššími provozními náklady nových technologií (vyšší spotřeba elektrické energie, nižší výkonnost apod.) **Navzdory tomu Mechanismus vůbec neobsahuje způsob výpočtu ani mechanismus náhrady takto vzniklých škod, přestože české právo s náhradou škody způsobené výkonem veřejné moci počítá.**

V rámci navrhu APMS jsme náhradu škody dle předmětného ustanovení koncipovali jako náhradu za nemožnost používání technologie po plnou dobu jejího životního cyklu a konkrétní výše je určována znalcem, a to na základě účetních odpisů, s tím, že by byla určena na základě rozdílu mezi délkou životního cyklu plnění dodavatele a lhůty stanovené Úřadem pro omezení či odstranění plnění dodavatele. Metoda určení výše náhrady škody dle odpisů se použije právě a jen pro případy náhrady za nemožnost používání dlouhodobého majetku v plném rozsahu. Pokud by tedy např. Úřad stanovil lhůtu pro odstranění plnění dodavatele v délce 3 roky a životní cyklus plnění dodavatele (technologie) by byl dle účetních odpisů 5 let, mohl by poskytovatel strategicky významné služby požadovat náhradu škody odpovídající 2 zbývajícím rokům odpisů. **Pro náhradu dalších účelně vynaložených nákladů vzniklých v důsledku plnění povinností uvedených v opatření obecné povahy se metoda odpisů z povahy věci nevyužije.**

Pokud bude rozsah regulace nastaven tak, jak je uvedeno v tomto návrhu, tedy na “jádro” sítě, lze říci, že kompenzace např. v oblasti telekomunikací nebudou reálně žádné. Ustanovení je však nastaveno tak, že pokud by škoda způsobena byla (například v jiných dotčených sektorech), nebo by došlo k novelizaci zákona a rozšíření rozsahu regulace, existovala by zde zákonná možnost nárokovat náhradu škody.

6. Návrh upraveného znění nZKB – Mechanismu

Po jednáních APMS se svými členy a dalšími oborovými asociacemi, jako je například Hospodářská komora České republiky a Svaz průmyslu a dopravy České republiky, připravila návrh paragrafového znění části nZKB týkající se Mechanismu. Spolu s návrhem paragrafového znění připravila APMS také důvodovou zprávu.

Návrh paragrafového znění přikládáme jako přílohu číslo 1 tohoto dokumentu.

Důvodovou zprávu přikládáme jako přílohu číslo 2 tohoto dokumentu.

Příloha č. 1

NÁVRH PARAGRAFOVÉHO ZNĚNÍ

Prověřování rizik spojených s dodavatelem
§ 28

1. Úřad shromažďuje a vyhodnocuje informace a data spojené s orgánem či osobou, které se týkají možné hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovosti dodavatele.
2. Činnosti podle odstavce 1 prioritizuje Úřad podle přístupu založeného na rizicích a dostupných kapacitách.
3. Pro potřeby mechanismu prověřování bezpečnosti dodavatelského řetězce se rozumí
   a. kritickou částí stanoveného rozsahu aktiva stanoveného rozsahu strategicky významné služby, u kterých poskytovatel strategicky významné služby postupem podle prováděcího právního předpisu ohodnotil dopad narušení bezpečnosti informací na stanovený rozsah strategicky významné služby úrovní kritická, a jejichž nedostupnost má současně přímý okamžitý dopad na nedostupnost strategicky významné služby,
   b. bezpečnostně významnou dodávkou plnění směřující do kritické části stanoveného rozsahu spočívající v poskytnutí, vývoji, výrobě, sestavení, správě, provozu či servisu
      1. technického prostředku nebo vybavení s výpočetní kapacitou,
      2. programového prostředku nebo vybavení, nebo
      3. informační či komunikační služby,
   c. dodavatelem bezpečnostně významné dodávky ten, kdo poskytovateli strategicky významné služby poskytne přímo či jako poddodavatel bezpečnostně významnou dodávku.

§ 30

Omezení rizik spojených s dodavatelem

1. Zjistí-li Úřad na základě vyhodnocení kritérií rizikovosti dodavatele možné významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku, předloží věc k projednání Vládě České republiky (dále jen "Vláda"). Před předložením věci Vládě je Úřad povinen vyhotovit odhad nákladů povinných osob spojených se zavedením omezení či zákazu plnění dodavatele, který je nedílnou součástí dokumentace předkládané Vládě. Poskytovatel strategicky významné služby je povinen na výzvu poskytnout Úřadu potřebnou součinnost.
2. Vláda přijme do 45 dnů ode dne, kdy jí byla věc předložena k projednání, usnesení o tom, zda plnění dodavatele může představovat ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. Při posuzování věci Vláda zohlední soulad případného plnění dodavatele s principy demokratického právního státu, dopad na ochranu života a zdraví obyvatel, obranu státu, zahraničně politické nebo bezpečnostní zájmy státu, ekonomickou bezpečnost státu a případně další skutečnosti důležité z hlediska ochrany bezpečnosti České republiky nebo vnitřního či veřejného pořádku.
3. V návaznosti na usnesení Vlády, že plnění dodavatele představuje významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku, vydá Úřad opatření obecné povahy, kterým stanoví podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu.
4. Usnesení Vlády je pro Úřad závazné a vydání opatření obecné povahy omezující či zakazující plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu je vydáním usnesení Vlády podmíněno.

5. Zakáže-li nebo omezí-li Úřad opatřením obecné povahy dle odstavce 3 plnění dodavatele, určí zároveň v opatření obecné povahy přiměřenou lhůtu zákazu nebo zohlednění podmínek plnění dodavatele. Lhůtu pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy stanoví Úřad s přihlédnutím k jejich dopadům na poskytovatele strategicky významné služby. Úřad vždy musí lhůtu předem konzultovat s příslušnými ústředními orgány státní správy, do jejichž působnosti spadá strategicky významná služba, do které směřuje bezpečnostně významné plnění dodavatele.
6. Před vydáním opatření obecné povahy je Úřad povinen projednat s příslušnými ústředními orgány státní správy, do jejichž působnosti spadá strategicky významná služba, do které směřuje bezpečnostně významné plnění dodavatele, zda návrh opatření obecné povahy a jeho možné dopady neohrozí plnění povinností stanovených a vyplývajících ze zvláštních právních předpisů. Úřad je povinen při vydání opatření obecné povahy stanovisko ústředního orgánu státní správy zohlednit.
7. Jestliže zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy podle odstavce 3 může ohrozit poskytování strategicky významné služby anebo představuje bezprostřední hrozbu kybernetického bezpečnostního incidentu, který podstatným způsobem ohrožuje poskytování strategicky významné služby, je poskytovatel strategicky významné služby povinen plnit opatření obecné povahy až po pominutí takové hrozby.
8. Úřad doručí návrh opatření obecné povahy veřejnou vyhláškou a vyzve dodavatele, vůči jehož plnění opatření obecné povahy míří, a další dotčené osoby, aby k návrhu opatření obecné povahy podávali připomínky. Lhůta pro podání připomínek činí 30 dnů, nestanoví-li Úřad jinak. Ustanovení § 172 odst. 1 a 5, § 173 odst. 1 věty první, část věty za středníkem, a § 173 odst. 1 věty druhé správního řádu se pro postup podle tohoto ustanovení nepoužijí.
9. V případě vydání opatření obecné povahy odstavce 3 musí poskytovatel strategicky významné služby provést analýzu rizik spojených s dodavatelem uvedeným v opatření obecné povahy podle odstavce 3 pro aktiva strategicky významné služby, která nezařadil do kritické části stanoveného rozsahu podle § 28 odst. 3 písm. a).
10. Na základě analýzy rizik vypracuje poskytovatel strategicky významné služby plán zvládání rizik dle odstavce 9, v němž uvede bezpečnostní opatření minimalizující rizika spojená s dodavatelem uvedeným v opatření obecné povahy podle odstavce 3. Plán zvládání rizik je poskytovatel strategicky významné služby povinen aktualizovat alespoň jednou za kalendářní rok.
11. Úřad přezkoumá alespoň jednou za 3 roky trvání skutečností, na jejichž základě bylo vydáno opatření obecné povahy podle odstavce 3. Zjistí-li Úřad, že tyto skutečnosti pominuly, opatření obecné povahy zruší.

§30a

Náhrada účelně vynaložených nákladů

1. V případě, že lhůta pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy podle §30 odstavce 3 je kratší, než životní cyklus bezpečnostně významné dodávky, nejdéle však 7 let, má každý poskytovatel strategicky významné služby vůči státu právo na náhradu účelně vynaložených nákladů vzniklých v důsledku plnění povinností podle § 30 odstavce 3, a to včetně nákladů na náhradu dlouhodobého majetku, který poskytovatel strategicky významné služby v důsledku opatření obecné povahy podle § 30 odstavce 3 nemůže dále využívat. Výši účelně vynaložených nákladů podle věty první určí Úřad na základě znaleckého posudku, pro jehož vyhotovení poskytne poskytovatel strategicky významné služby součinnost.
2. Životní cyklus bezpečnostně relevantní dodávky bude znalcem určen na základě účetních odpisů zařízení.
3. Zrušením opatření obecné povahy podle § 30 odstavce 11 nezaniká právo na náhradu nákladů podle tohoto ustanovení. Ve věci náhrady nákladů podle tohoto ustanovení jménem státu jedná Úřad.

§ 31

Výjimky z omezení rizik spojených s dodavatelem

1. Úřad může, pokud to povaha daného ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku připouští, povolit výjimku z podmínek či zákazu stanovených opatřením obecné povahy podle § 30, jestliže by plnění opatření obecné povahy poskytovatelem strategicky významné služby mohlo podstatným způsobem ohrozit poskytování strategicky významné služby.
2. Řízení o povolení výjimky podle odstavce 1 lze zahájit na žádost poskytovatele strategicky významné služby nebo z moci úřední. Žadatel je povinen v rámci žádosti připojit důkazy prokazující skutečnosti, kterých se dovolává.
3. Úřad v rozhodnutí o povolení výjimky stanoví podmínky jejího uplatnění. V případě závažného porušení podmínek pro uplatnění výjimky nebo v případě pominutí důvodu, pro který byla povolena, Úřad výjimku rozhodnutím zruší.
4. Úřad výjimku nepovolí, pokud by to zcela zmařilo účel opatření obecné povahy podle § 30.
5. Informace týkající se výjimky je v souladu s právními předpisy[65] označována jako utajovaná informace.

§ 34

Zajištění dostupnosti strategicky významné služby

1. Poskytovatel strategicky významné služby je povinen zajistit dostupnost strategicky významné služby v rozsahu kritické části stanoveného rozsahu ve stanoveném čase a kvalitě z území České republiky.
2. Poskytovatel strategicky významné služby v odvětví 16.1 Poskytování veřejně dostupní služby elektronických komunikací a 16.2. Zajišťování veřejně dostupné komunikační sítě elektronických komunikací podle přílohy k vyhlášce o regulovaných službách je povinen v rozsahu kritické části stanoveného rozsahu ve stanoveném čase a kvalitě z území České republiky zajistit dostupnost strategicky významné služby spočívající v
   a) poskytování veřejně dostupné mobilní služby elektronických komunikací,
   b) zajišťování veřejné mobilní komunikační sítě elektronických komunikací,
   c) poskytování veřejně dostupné služby elektronických komunikací v pevném místě.
3. Poskytovatel strategicky významné služby je povinen testovat schopnost zajištění poskytování strategicky významné služby v rozsahu kritické části stanoveného rozsahu z území České republiky nejméně jednou za dva roky.
4. Poskytovatel strategicky významné služby začne plnit povinnosti uvedené v odst. 1 a 2 pro každou strategicky významnou službu nejpozději do jednoho roku ode dne doručení vyrozumění o zápisu strategicky významné služby do evidence poskytovatelů regulovaných služeb nebo od doručení rozhodnutí o určení strategicky významné služby podle § 27 odst. 2.
5. Stanovený čas a kvalitu služby stanoví poskytovatel regulované služby v závislosti na cílech řízení kontinuity činností podle prováděcího právní předpisu.
6. Pro potřeby tohoto ustanovení je kritická část stanoveného rozsahu vymezena v § 28 odst. 3 písm. a).

[65] zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti

Detailní rozbor jednotlivých ustanovení

K § 28 návrhu nového ZKB:

- je navržena úprava kritické části stanoveného rozsahu aktiv tak, aby se jednalo pouze o aktiva ohodnocená povinnými subjekty na **úrovni kritická, jejichž nedostupnost má současně přímý okamžitý dopad na nedostupnost strategicky významné služby**
    - rozsah mechanismu jsme definovali na základě hrozeb a důsledku jejich případné realizace. Jako nejvýznamnější hrozbu jsme označili **nedostupnost strategicky významné služby**. -> zákaz dodavatele pro aktiva, jejichž výpadek může způsobit nedostupnost strategicky významné služby je tedy s ohledem na princip proporcionality **přiměřený**
    - pro oblast telekomunikací jde v zásadě o vztažení mechanismu pouze na části sítě zvané: „jádro sítě" a části „přenosové sítě". Úprava je formulována obecněji, aby se vztahovala na všechny oblasti, nejen telekomunikace

K § 30 návrhu nového ZKB:

- Nad rámec výše uvedeného jsme zavedli **tzv. kaskádu bezpečnostních opatření**, kdy v případě vydání opatření obecné povahy (OOP) je pro poskytovatele strategicky významné služby zakotvena **nově povinnost provést analýzu rizik** pro aktiva strategicky významné služby, která nezařadil do kritické části stanoveného rozsahu (tj. pro zbývající aktiva, která nejsou na úrovni kritická) – § 30 odst. 9-10
    - v rámci analýzy rizik musí povinná osoba zohlednit rizika, která NÚKIB uvedl v OOP
    - na základě analýzy rizik poskytovatel vypracuje plán zvládání rizik, jehož součástí jsou i bezpečnostní opatření minimalizující rizika spojená s dodavatelem uvedeným v OOP
    - tento plán musí pravidelně aktualizovat
    - NÚKIB tedy může zakázat dodavatele v kritické části stanoveného rozsahu (**kde hrozí nedostupnost strategicky významné služby na kritické úrovni**). Pro zbytek aktiv vznikne povinným osobám automaticky povinnost provést analýzu rizik uvedených v OOP a vypracovat strategií zvládání rizik včetně implementace odpovídajících bezpečnostních opatření
- do procesu posuzování dodavatele je nově zapojen(a):
    - vláda (obdobně je tomu v zákoně o prověřování zahraničních investic) – § 30 odst. 1-4
    - sektorový regulátor – § 30 odst. 5-6
        - poskytuje konzultaci a stanovisko k tématice lhůty omezení či zákazu plnění dodavatele a možnosti ohrožení plnění povinností dle zvláštního právního předpisu – > NÚKIB musí stanovisko zohlednit

K § 30a návrhu nového ZKB:

- v § 30a je nově zakotvena možnost náhrady škody
    - poskytovatel strategicky významné služby má vůči státu právo na náhradu účelně vynaložených nákladů vzniklých v důsledku plnění povinností z OOP
    - náhrada škody je určována znalcem, a to na základě účetních odpisů
    - maximální doba odpisů je omezena na 7 let, aby nedocházelo k umělému protahování odpisů
    - v případě zachování znění § 28 nevznikne operátorům škoda, kterou by nárokovali po státu

K § 31 návrhu nového ZKB:

- Navrhuje se doplnění odstavce č. 5, v němž je zakotveno, že všechny informace týkající řízení o udělení výjimky a obsahu vydaného rozhodnutí Úřadu o povolení výjimky jsou v souhlasu se zákonem č.

412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti označovány jako utajované informace.

K § 34 návrhu nového ZKB:

- nově vloženo ustanovení (nový odstavec 2) deklarující speciální úpravu zajištění dostupnosti strategicky významné služby ve vymezených oblastech elektronických komunikací
    - cílem je zamezení možných dezinterpretací a výkladových nejasností problematiky zajištění dostupnosti strategicky významných služeb pro oblast telekomunikací

Příloha č. 2

DŮVODOVÁ ZPRÁVA

Zvláštní část

§20, § 30, § 30a, § 31, § 34

K návrhu znění § 28 návrhu nového ZKB:

Navrhované ustanovení ponechává pravomoc Národního úřadu pro kybernetickou a informační bezpečnost („*Úřad*“) provádět prověřování rizik spojených s dodavatelem, tak jak přepokládá návrh nového zákona o kybernetické bezpečnosti („*návrh ZKB*“), odlišně však vymezuje některé pojmy spojené s touto pravomocí. Vzhledem k odlišné koncepci pojmu kritické části stanoveného rozsahu (viz níže), je obsolentní zakotvení vydání vyhlášky o nepominutelných funkcích stanoveného rozsahu, jak předpokládá návrh ZKB, proto byla ze znění tohoto návrhu vypuštěna.

Pravomoc Úřadu má být realizována, v souladu s návrhem ZKB, prostřednictvím shromažďování a vyhodnocování informací, jež mohou přispět k vyvození závěrů o existenci hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovosti dodavatele stanovených prováděcím právním předpisem, a které jsou spojeny s plněním konkrétního dodavatele. Kritéria rizikovosti dodavatele stanoví prováděcí právní předpis – vyhláška, k jejímuž vydání je zmocněn Úřad v § 55 návrhu ZKB.

Jak uvádí Úřad v důvodové zprávě k návrhu ZKB, cílem mechanismu prověřování bezpečnosti dodavatelského řetězce („*mechanismus*“) je umožnit státu identifikovat a vyhodnocovat hrozby spojené jak s orgány nebo osobami, které již jsou dodavateli do infrastruktury poskytovatelů strategicky významné služby, tak s orgány nebo osobami, u nichž se lze domnívat, že by svá plnění do této infrastruktury dodávat mohly, a to s cílem odhalit hrozbu ještě dříve, než bude u strategicky významné služby moci způsobit narušení bezpečnosti informací. S ohledem na velké množství orgánů a osob, které mohou být předmětem prověřování, je stanovena možnost Úřadu prioritizovat činnosti spojené s prověřováním stávajících a potenciálních dodavatelů, tak jak to předpokládá i návrh ZKB, a to s ohledem na možná rizika a dostupné kapacity Úřadu.

Odstavec 3 předmětného ustanovení vymezuje pojmy, které navrhovaná právní úprava dále užívá v souvislosti s mechanismem. Pojem *„bezpečnostně významná dodávka“*, který vymezuje plnění, na která se mohou vztahovat omezení využití plnění rizikových dodavatelů, a *„dodavatel bezpečnostně významné dodávky“,* který vymezuje okruh orgánů a osob, na jejichž plnění se mohou vztahovat omezení využití v důsledku prověření rizik s nimi spojených, je dle tohoto návrhu shodný se zněním uvedeným v návrhu ZKB, proto se mu text zde nebude věnovat.

Změny však v tomto předkládaném návrhu doznal pojem *„kritická část stanoveného rozsahu“,* který vymezuje aktiva poskytovatele strategicky významné služby, na která se mohou vztahovat omezení využití plnění rizikových dodavatelů.

Úřad opakovaně deklaroval, že mechanismus se má vztahovat pouze na tu nejkritičtější část strategické infrastruktury. V návrhu ZKB však Úřad vymezil rozsah mechanismu formou vyhlášky o nepominutelných funkcí, která je výrazně širší, než bylo deklarováno, a například pro oblast telekomunikací obsahuje jak ty nejkritičtější části sítě (jako je jádro sítě – „core“), tak i méně kritické části sítě (jako je např. rádiová přístupová síť) nebo aktiva, které nemají přímý vliv na nedostupnost regulovaných služeb (např. fakturační systém). V návrhu ZKB i důvodové zprávě k němu zcela chybí odůvodnění, proč jsou kritické části stanoveného rozsahu aktiv definovány tak široce.

Ve zde předkládaném návrhu je stanovena nová úprava kritické části stanoveného rozsahu aktiv tak, aby se jednalo pouze o aktiva ohodnocená povinnými subjekty na **úrovni kritická, jejichž nedostupnost má současně přímý okamžitý dopad na nedostupnost strategicky významné služby.**

Předkládaný návrh vychází z předpokladu, že kritická část stanoveného rozsahu se skládá z podmnožiny aktiv strategicky významných služeb, u kterých si poskytovatel strategicky významné služby postupem podle prováděcího právního předpisu upravujícího bezpečnostní opatření poskytovatele regulované služby v režimu vyšších povinností sám v rámci plnění povinností podle § 13 návrhu ZKB ohodnotil dopad narušení bezpečnosti informací úrovní kritická.

Kritické části strategické infrastruktury jsou transparentně rozděleny dle úrovně hrozby a dopadů její případné realizace. Nejvýznamnější hrozbou je výpadek regulované služby – rozsah mechanismu tak byl v návrhu omezen výlučně na aktiva, jejichž nedostupnost má přímý okamžitý dopad na nedostupnost regulované služby na kritické úrovni. Pro příklad – pro oblast telekomunikací se jedná zejména o jádro sítě, případně části přenosové sítě. Úprava je formulována obecněji, aby se vztahovala na všechny oblasti, nejen telekomunikace.

Pro tyto kritické části, které mohou způsobit okamžitou nedostupnost strategicky významné služby, je přiměřené, aby byla dána možnost státu okamžitým zásahem omezit či zakázat vybraného dodavatele, u kterého identifkuje významnou hrozbu.

Pro zbylé části aktiv strategicky významné služby, které nemohou ze své podstaty způsobit nedostupnost služby na kritické úrovni, je s ohledem na princip proporcionality vhodné, aby poskytovatel strategicky významné služby sám na základě analýzy rizik minimalizoval rizika, která v rámci opatření obecné povahy identifikoval Úřad. Úřad by přitom jako doposud nad implementovanými bezpečnostními opatřeními vykonával dohled. Bezpečnostní opatření specifická pro daného dodavatele by nově měla být upravena zvlášť v bezpečnostní dokumentaci, kterou by poskytovatel strategicky významné služby měl povinnost každoročně aktualizovat (blíže viz odůvodnění § 30 návrhu níže).

K návrhu úpravy § 30 návrhu nového ZKB:

Navrhované ustanovení zakotvuje možnost omezit nebo zakázat využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu, a to zjistí-li Úřad postupem podle § 28 odst. 1 návrhu ZKB, že může být významně ohrožena bezpečnost České republiky nebo vnitřní či veřejný pořádek.

Oproti návrhu ZKB je do procesu prověřování rizik spojených s dodavatelem zapojena vláda. Zapojení vlády v procesu prověřování rizikovosti dodavatele je zásadně smysluplné a důležité, a to jak z hlediska transparentnosti a objektivity rozhodování, tak vzhledem k závažnosti opatření obecné povahy, které na základě uvedeného ustanovení zákona může být vydáno. Případný zákaz či omezení plnění dodavatele musí vždy být až nejzazším řešením – představuje totiž značný zásah do ústavně zaručených práv a povinností jednotlivých subjektů, i proto musí být podmíněn právě usnesením vlády.

Je třeba podotknout, že vláda do jisté míry v současnosti již do posuzování rizikovosti dodavatele (resp. investora) zapojena je, a to dle zákona č. 34/2021 Sb., o prověřování zahraničních investic („*zákon o prověřování zahraničních investic*“). Dle zákona o prověřování zahraničních investic jsou přijetím usnesení vlády podmíněna rozhodnutí omezující či zakazující zahraniční investici, a to právě s ohledem na míru zásahu do práv dotčených subjektů v důsledku tohoto omezení či zákazu. Začlenění vlády do procesu prověřování rizikovosti dodavatele má tedy pevné základy již v aktuálně účinné právní úpravě a rozhodnutí o omezení či zákazu plnění dodavatele by mělo být podmíněno usnesením vlády (obdobně jako u zahraničních investic), a to zejména s ohledem na to, že plošný zákaz či omezení plnění dodavatele může mít mnohem větší dopad na trh než zákaz doposud neuskutečněné investice.

Řešení otázky dodavatelského řetězce zasahuje do vícero oblastí, nejen do oblasti bezpečnostní. Pouze vláda může posoudit jak geopolitické a ekonomické dopady věci, tak i bezpečnostní aspekty – ostatně takto to činí již

dle zákona o prověřování zahraničních investic, kdy vláda posuzuje, zda je případné omezení či zákaz zahraniční investice nutný z důvodu ochrany bezpečnosti České republiky nebo vnitřního či veřejného pořádku, přičemž při posuzování jsou hodnocena i strategická kritéria, jako je hodnocení investorů z hlediska země jejich původu (např. zda je zahraniční investor ovládán přímo či nepřímo vládou třetí země, či zda již byl zapojen do činností ovlivňujících bezpečnost nebo veřejný pořádek v některém členském státě EU). Právě z důvodu komplexnosti celé problematiky a přesahu do rozličných oblastí není vhodné, aby věc byla konzultována pouze s Bezpečnostní radou státu („*BRS*"), jejímž předmětem činnosti je výhradně koordinace problematiky bezpečnosti České republiky, jak navrhuje návrh ZKB z dílny Úřadu. Nadto je třeba říci, že usnesení vlády jsou závazná zásadně šířeji, než usnesení BRS (usnesení vlády zavazují všechny členy vlády, ministerstva, jiné ústřední orgány státní správy, ostatní správní úřady a další subjekty, pokud tak stanoví zvláštní zákon, zatímco pokud jde o usnesení BRS, zde je závazná pouze jeho ukládací část (jen v oblasti zajišťování bezpečnosti České republiky), a to pouze pro určené členy vlády a vedoucí jiných správních úřadů).

Vedle zapojení vlády počítá předkládaný návrh rovněž s účastí sektorových regulátorů (příslušných ústředních orgánů státní správy), jejichž pozice je v návrhu ZKB značně opomíjena, je však v procesu prověřování zcela zásadní. Právě příslušní sektoroví regulátoři disponují potřebným penzem informací a odborných znalostí o fungování a činnosti daného regulovaného sektoru a jsou schopni posoudit reálné dopady případného omezení či zákazu plnění dodavatele, jakož i přesah do oblasti úpravy zajišťované zvláštními právními předpisy pro daný sektor (např. ohrožení plnění povinností subjektů stanovených těmito zvláštními právními předpisy).

V návaznosti na usnesení vlády a konzultaci se sektorovými regulátory, je dána Úřadu pravomoc vydat konkrétní omezení formou opatření obecné povahy, kterým se budou muset řídit všichni poskytovatelé strategicky významných služeb. Toto opatření obecné povahy však musí být přijato na základě usnesení vlády a zohledňovat stanovisko příslušného sektorového regulátora.

Proces prověřování rizikovosti dodavatele je dle tohoto návrhu nastaven následovně:

Pokud Úřad na základě vyhodnocení kritérií rizikovosti dojde k závěru, že plnění dodavatele může představovat významné ohrožení bezpečnosti anebo vnitřního či vnějšího pořádku České republiky, předloží věc k projednání vládě.

Vzhledem k tomu, že možné opatření omezující či zakazující plnění konkrétního dodavatele může mít rozsáhlé dopady nejen na dodavatele samého, ale i na povinné osoby (poskytovatele strategicky významných služeb), jichž se opatření obecné povahy dotýká, je Úřad ještě před předložením věci vládě povinen vypracovat odhad nákladů spojených s implementací povinností stanovených v opatření obecné povahy povinnými osobami. Tento podklad je zásadní pro samotnou vládu, aby mohla věc posoudit ve všech souvislostech (včetně případných ekonomických dopadů) a učinit informované rozhodnutí s vědomím veškerých hrozících dopadů. Za účelem vypracování odhadu nákladů jsou poskytovatelé strategicky významné služby povinni Úřadu poskytnout potřebnou součinnost.

Vláda má následně k dispozici lhůtu 45 dnů k projednání a vydání usnesení o tom, zda plnění dodavatele může představovat ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku (dále jen „*ohrožení*"), přičemž při posuzování věci vláda zohledňuje jak možný dopad plnění dodavatele na principy demokratického právního státu, ochranu života a zdraví obyvatel, obranu státu, zahraničně politické nebo bezpečnostní zájmy státu, ekonomickou bezpečnost státu a případně další skutečnosti důležité z hlediska ochrany bezpečnosti České republiky nebo vnitřního či veřejného pořádku. Usnesení vlády je pro Úřad vždy závazné a je jím podmíněno vydání zakazujícího či omezujícího opatření obecné povahy.

V návaznosti na usnesení vlády o tom, že plnění dodavatele představuje významné ohrožení, je Úřadu dána pravomoc vydat opatření obecné povahy, kterým stanoví podmínky nebo zakáže plnění dodavatele bezpečnostně významné dodávky. Z povahy opatření obecné povahy vyplývá, že jde o opatření, kterým se budou muset řídit všichni poskytovatelé strategicky významných služeb – směřuje však vždy vůči vymezeným plněním daného dodavatele (proti bezpečnostně významné dodávce). Stejně jako v návrhu ZKB, se vydání opatření

obecné povahy řídí obecnou právní úpravou obsaženou ve správním řádu, a to s výjimkou ustanovení, která pojmově nejsou přiléhavá k problematice prověřování rizikovosti dodavatele (týkají se typicky nemovitostí a územního rozvoje). Z obecné právní úpravy také vyplývá možnost přezkoumat opatření obecné povahy v přezkumném řízení nebo v soudním řízení správním dle obecné úpravy správního řádu a správního řádu soudního, nelze však proti němu podat opravný prostředek.

V rámci omezujícího či zakazujícího opatření obecné povahy Úřad vždy stanoví i přiměřenou lhůtu pro zohlednění podmínek či zákazu. Nově předkládaný návrh stanovuje, že lhůta musí být vždy stanovena v návaznosti na projednání s příslušnými ústředními orgány státní správy (sektorovými regulátory), do jejichž působnosti náleží strategicky významná služba, do níž směřuje bezpečnostně významné plnění dodavatele, neboť právě sektoroví regulátoři disponují objektivními informacemi, na jejichž základě lze přiměřenou lhůtu stanovit.

Je nutné trvat na tom, aby omezení či zákaz stanovený prostřednictvím opatření obecné povahy byl vždy proporcionální a přiměřené a nekolidoval s právní úpravou obsaženou ve zvláštních právních předpisech. Vzhledem k tomu, že případné omezení či zákaz plnění dodavatele může mít významný dopad na schopnost povinných osob plnit své zákonné povinnosti vyplývající ze zvláštních právních předpisů, je za tímto účelem navrženo, aby Úřad projednal s příslušnými ústředními orgány státní správy (sektorovými regulátory), do jejichž působnosti náleží strategicky významná služba, do níž směřuje bezpečnostně významné plnění dodavatele, zda návrh opatření obecné povahy a jeho možné dopady neohrozí plnění povinností uvedených ve zvláštních právních předpisech. Například pro oblast telekomunikací jde mj. o výstavbové povinnosti vyplývající ze zákona č. 127/2005 Sb. o elektronických komunikacích. Je tedy zásadní, aby daný sektorový regulátor, v tomto případě Český telekomunikační úřad, měl možnost se k implementaci omezení či zákazu vyjádřit a Úřad musel k jeho stanovisku přihlédnout.

V souladu s návrhem ZKB je i v tomto návrhu zachována povinnost Úřadu pravidelně (nejméně jednou za 3 roky) přezkoumávat trvání skutečností, na jejichž základě bylo vydáno omezení či zákaz, aby byla v případě jejich pominutí bezodkladně zrušena.

Navrhovatel si je vědom nutnosti zajištění kybernetické bezpečnosti a bezpečnosti informací, a to v celé síti, proto v rámci ustanovení § 30 navrhuje nově zavést taktéž povinnost pro poskytovatele strategicky významné služby **provést analýzu rizik spojených s dodavatelem dotčeným opatřením obecné povahy** u těch aktiv strategicky významné služby, které poskytovatel strategicky významné služby nezařadil do kritické části stanoveného rozsahu dle § 28 odst. 3 písm. a). Jde v podstatě o zavedení jakési kaskády bezpečnostních opatření, kdy pro tu nejkritičtější část strategické infrastruktury, kde hrozí přímý okamžitý dopad na nedostupnost strategicky významné služby, bude dána povinnost řídit se případným omezením či zákazem uvedeným v opatření obecné povahy, a pro ty méně kritické části strategické infrastruktury bude nově dána povinnost zohlednit rizika identifikovaná státem a implementovat odpovídající bezpečnostní opatření.

Na základě analýzy rizik poskytovatel strategicky významné služby vypracuje plán zvládání rizik, jehož součástí jsou i bezpečnostní opatření minimalizující rizika spojená s dodavatelem uvedeným v opatření obecné povahy, který musí pravidelně (alespoň jednou za kalendářní rok) aktualizovat.

Úřad tedy může omezit či zakázat plnění dodavatele v kritické části stanoveného rozsahu tam, kde hrozí nedostupnost strategicky významné služby. Pro zbytek aktiv pak vznikne poskytovatelům strategicky významné služby automaticky povinnost provést analýzu rizik uvedených v opatření obecné povahy i pro aktiva nezařazená do kritické části stanoveného rozsahu a vypracovat strategii zvládání rizik včetně implementace odpovídajících bezpečnostních opatření.

Návrh na doplnění § 30a do návrhu nového ZKB:

Navrhuje se zakotvení možnosti náhrady škody, a to obdobně, jak je tomu např. v zákoně č. 289/2005 Sb., o vojenském zpravodajství („*zákon o vojenském zpravodajství*“), v němž je přiznána náhrada škody každému, komu škoda nebo nemajetková újma vznikla v souvislosti s činnostmi Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu.[66] Náhrada škody je upravena ve vloženém ustanovení § 30a předkládaného návrhu, podle nějž má poskytovatel strategicky významné služby vůči státu nárok na náhradu účelně vynaložených nákladů vzniklých v důsledku plnění povinností z opatření obecné povahy.

Náhrada škody dle předmětného ustanovení je koncipována jako náhrada za nemožnost používání technologie po plnou dobu jejího životního cyklu a konkrétní výše je určována znalcem, a to na základě účetních odpisů, s tím, že by byla určena na základě rozdílu mezi délkou životního cyklu plnění dodavatele a lhůty stanovené Úřadem pro omezení či odstranění plnění dodavatele. Metoda určení výše náhrady škody dle odpisů se použije právě a jen pro případy náhrady za nemožnost používání dlouhodobého majetku v plném rozsahu. Pokud by tedy např. Úřad stanovil lhůtu pro odstranění plnění dodavatele v délce 3 roky a životní cyklus plnění dodavatele (technologie) by byl dle účetních odpisů 5 let, mohl by poskytovatel strategicky významné služby požadovat náhradu škody odpovídající 2 zbývajícím rokům odpisů. Pro náhradu dalších účelně vynaložených nákladů vzniklých v důsledku plnění povinností uvedených v opatření obecné povahy se metoda odpisů z povahy věci nevyužije.

Pro zajištění větší právní jistoty státu je maximální doba odpisů omezena na 7 let, aby nedocházelo k umělému protahování odpisů.

Pokud bude rozsah regulace nastaven tak, jak je uvedeno v tomto návrhu, lze říci, že kompenzace např. v oblasti telekomunikací nebudou reálně žádné. Ustanovení je však nastaveno tak, že pokud by škoda způsobena byla (například v jiných dotčených sektorech), nebo by došlo k novelizaci zákona a rozšíření rozsahu regulace, existovala by zde zákonná možnost nárokovat náhradu škody.

K návrhu úpravy § 31 návrhu nového ZKB

Navrhuje se doplnění odstavce č. 5, v němž je zakotveno, že všechny informace týkající řízení o udělení výjimky a obsahu vydaného rozhodnutí Úřadu o povolení výjimky jsou v souhlasu se zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti označovány jako utajované informace.

Vzhledem k citlivosti informací, které jsou v rozhodnutí o povolení výjimky uvedeny, je potřebné, aby rozhodnutí nebylo veřejně dostupné. S ohledem na potřebu zajištění kybernetické bezpečnosti a ochrany informací, jakož i obchodního tajemství dotčených subjektů, není přípustné, aby bylo rozhodnutí o povolení výjimky veřejně dostupné. Zveřejnění informací o tom, komu a jak byla Úřadem povolena výjimka, je z hlediska cíle zajištění kybernetické bezpečnosti, jakož i z hlediska hospodářské soutěže a ochrany údajů zásadně nevhodné rozporné se smyslem zákona.

---

[66] Viz § 16n zákona o vojenském zpravodajství:

(1) *Každý, komu vznikla škoda nebo nemajetková újma v souvislosti s činnostmi Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu, má právo na jejich náhradu.*
(2) *Fyzické nebo právnické osobě se nahrazuje také škoda nebo nemajetková újma, která jí vznikla v důsledku realizace opatření přijatých Vojenským zpravodajstvím v zájmu provedení aktivního zásahu směřujícího k odstranění kybernetického útoku nebo hrozby v rámci zajišťování obrany státu v kybernetickém prostoru.*
(3) *Povinnost státu k náhradě škody nebo nemajetkové újmy podle odstavců 1 a 2 nevznikne, pokud se jedná o škodu nebo nemajetkovou újmu způsobenou fyzické nebo právnické osobě, která vyvolala útok nebo hrozbu.*
(4) *Za škodu nebo nemajetkovou újmu způsobenou Vojenským zpravodajstvím odpovídá stát. Náhradu škody nebo nemajetkové újmy poskytuje v zastoupení státu Ministerstvo obrany.*

K návrhu úpravy § 34 návrhu nového ZKB

Navrhuje se doplnění nového odstavce č. 2, v němž je zakotvena speciální úprava zajištění dostupnosti strategicky významné služby pro oblast elektronických komunikací.

Vzhledem k tomu, že oblast elektronických komunikací je velmi specifickým sektorem a již krátce po zveřejnění návrhu ZKB v eKLEP bylo zřejmé, že úprava navržená v návrhu ZKB (ve spojení s příslušnými prováděcími právními předpisy) způsobuje výkladové nejasnosti ohledně rozsahu a dopadu daného ustanovení, navrhuje se zakotvení speciální úpravy zajištění dostupnosti strategicky významné služby pro oblast elektronických komunikací, a to s cílem zamezit možným dezinterpretacím daného ustanovení pro oblast elektronických komunikací.