Důvodová zpráva

Návrh nařízení vlády o regulovaných službách, které splňují podmínky strategicky významné služby, a o částech strategicky významných služeb tvořících nezbytný rozsah zajištění dostupnosti strategicky významných služeb

I. Obecná část

1.   Popis obsahu návrhu právního předpisu s uvedením důvodů, které k jeho předložení vedou, a shrnutí základních zásad a nejdůležitějších změn, které oproti stávající právní úpravě zavádí

Na konci roku 2022 byla přijata směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1146 (tzv. směrnice NIS2), která přináší významné změny v oblasti regulace kybernetické bezpečnosti. Tato směrnice je implementována návrhem nového zákona o kybernetické bezpečnosti (dále „návrh zákona“), který oproti stávajícímu zákonu č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů, stanovuje pouze jeden typ hlavní povinné osoby, kterým je tzv. „poskytovatel regulované služby“. Současně návrh zákona v návaznosti na směrnici NIS2, respektive její rozdělení subjektů na základní (*essential*) a důležité (*important*), zavádí pro poskytovatele regulované služby dva samostatné režimy povinností. Konkrétně se jedná o tzv. režim vyšších povinností a tzv. režim nižších povinností.

Pro vybrané organizace spadající do kategorie poskytovatele regulované služby v režimu vyšších povinností stanovuje návrh zákona specifické dodatečné povinnosti a tím je označuje jako tzv. poskytovatele strategicky významné služby (blíže § 25 a násl. návrhu zákona).

Stanovení kritérií pro určení toho, které zákonem regulované služby jsou považovány za strategicky významné služby, je prvním cílem tohoto nařízení vlády. Zmocnění k vydání nařízení vlády pro stanovení těchto kritérií je stanoveno v § 25 návrhu zákona.

Jednou z výše zmíněných povinností poskytovatele strategicky významné služby je povinnost spočívající v tom, že je potřeba zajistit dostupnost strategicky významné služby v nezbytném rozsahu, ve stanoveném čase a kvalitě z území České republiky (§ 33 návrhu zákona). Čas a kvalitu služby si stanoví sám poskytovatel strategicky významné služby, nicméně návrh zákona ukládá, že výčet částí strategicky významných služeb tvořících nezbytný rozsah a způsob jejich vymezení stanoví vláda nařízením. Nezbytným rozsahem se podle návrhu zákona rozumí část strategicky významné služby, jejíž nedostupnost by mohla mít závažný dopad na bezpečnost České republiky nebo vnitřní pořádek. Druhým cílem tohoto nařízení vlády je tedy specifikovat nezbytný rozsah dostupnosti tzv. strategicky významné služby podle § 33 odst. 4 návrhu zákona.

Oba tyto cíle je možné stanovit zároveň v rámci nařízení vlády, protože stanovení nezbytného rozsahu zajištění strategicky významné služby má úzkou návaznost na stanovení strategicky významných služeb jako takových.

2.   Zhodnocení platného právního stavu

Oblast strategicky významných služeb z hlediska kybernetické bezpečnosti dosud nebyla nijak komplexně regulována. Předkládaný návrh úpravy obsažený v nařízení vlády o strategicky významných službách tudíž představuje novou regulaci reflektující požadavek Bezpečnostní rady státu k vytvoření tzv. mechanismu prověřování bezpečnosti dodavatelského řetězce, které navazuje na vývoj na poli kybernetických bezpečnostních hrozeb a nutnost na ně ze strany státu přiměřeně reagovat.

Stanovení množiny strategicky významných služeb dle tohoto návrhu nařízení vlády pak představuje národní úpravu respektující požadavek Bezpečnostní rady státu v souladu s materiálem „Bezpečnost dodavatelských řetězců strategické infrastruktury státu“, č. j. 28261/2022-UVCR, jejž Bezpečnostní rada státu vzala na vědomí svým usnesením č. 41 ze dne 21. června 2022.

3.   Zhodnocení souladu návrhu právního předpisu s ústavním pořádkem a ostatními součástmi právního řádu České republiky

Návrh nařízení vlády je v souladu s ústavním pořádkem a ostatními součástmi právního řádu ČR.

Zmocnění pro vydání tohoto nařízení vlády je obsaženo v návrhu zákona a toto zmocnění není návrhem překročeno.

Samotné následky a dopady do právem hájených zájmů lze tak spojovat pouze s návrhem zákona jako takovým.

Nařízení vlády pak slouží k vymezení okruhu osob, na které dopadá tzv. mechanismus bezpečnosti dodavatelského řetězce, který výše zmíněný návrh zákona do českého právního řádu zavádí a rovněž jim návrh zákona stanoví i okruh osob, které mají povinnost zajišťovat dostupnost strategicky významné služby.

Zhodnocení samotné ústavnosti tohoto institutu bylo proveden v rámci důvodové zprávy k návrhu zákona, a to následovně:

Úzké části poskytovatelů regulované služby s potenciálně největšími dopady pro fungování státu (strategicky významné služby) může návrh zákona také omezit vlastnické právo, resp. právo na podnikání v rámci nově zaváděného mechanismu prověřování bezpečnosti dodavatelského řetězce.

K zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce je namístě konstatovat, že návrh zákona je také v tomto směru v souladu s ústavním pořádkem České republiky

Zavedení uvedeného mechanismu je v souladu s článkem 2 odst. 3 ústavního zákona č. 1/1993 Sb., Ústava České republiky, který stanovuje, že státní moc lze uplatňovat jen v případech, v mezích a způsoby, které stanoví zákon, s článkem 41 odst. 2 Ústavy, podle kterého má vláda právo zákonodárné iniciativy, a článkem 79 odst. 1 Ústavy, podle kterého lze působnost správních orgánů stanovit pouze zákonem.

Navrhovaný způsob posuzování dodavatelů je rovněž v souladu s čl. 2 odst. 2 Listiny, podle kterého lze státní moc uplatňovat jen v případech a mezích stanovených zákonem, a to způsobem, který zákon stanoví, článek 4 odst. 1 Listiny, podle kterého mohou být ukládány povinnosti toliko na základě zákona a v jeho mezích a jen při zachování lidských práv a svobod, a článek 2 odst. 3 Listiny, podle kterého každý může činit, co není zákonem zakázáno, a nikdo nemůže být nucen činit, co zákon neukládá.

Listina upravuje možnost omezení některých práv v ní zakotvených, konkrétně v případě předkládaného návrhu zákona práva podnikat stanoveného článkem 26 odst. 1 Listiny nebo práva na ochranu dobré pověsti stanového v článku 10 odst. 1 Listiny. Obecně platí, že některá základní práva mohou být podle Listiny omezena. Omezení musí být ovšem stanovena zákonem, musí být v souladu s Listinou a musí být založena na jejich potřebnosti k dosažení legitimních společenských cílů, jako je např. zabezpečení existence státu, ochrany jeho demokratické povahy, zachování veřejného zdraví a pořádku (srov. např. usnesení Ústavního soudu ze dne 19. 3. 2009, sp. zn. IV. ÚS 266/09-1 či usnesení Ústavního soudu ze dne 7. 3. 2014, sp. zn. I. ÚS 110/14-1). Při posuzování souladu těchto omezení s ústavním pořádkem je uplatňován princip proporcionality, kdy jsou aplikována kritéria vhodnosti, potřebnosti a poměřování (srov. nález Ústavního soudu ze dne 12. 10. 1994, sp. zn. Pl. ÚS 4/94).

V případě prověřování bezpečnosti dodavatelského řetězce je takovýmto legitimním cílem ochrana bezpečnosti státu a vnitřního pořádku, v jejímž rámci stát v souladu s čl. 4 odst. 2 ve spojení s čl. 26 odst. 2 Listiny stanoví omezení pro výkon určitých činností, a tím omezí právo podnikat a provozovat jinou hospodářskou činnost, které je zakotveno v čl. 26 odst. 1 Listiny. Obdobné lze říci i o právu na ochranu dobré pověsti, které náleží i právnickým osobám (srov. např. rozsudek Nejvyššího soudu ze dne 14. 3. 2018, sp. zn. 23 Cdo 5173/2017 či nález Ústavního soudu ze dne 10. 10. 2001, sp. zn. I. ÚS 201/01), a které může být procesem prověřování bezpečnosti dodavatelského řetězce dotčeno. Případné omezení těchto práv je proto v souladu s ústavním pořádkem České republiky.

Článek 11 odst. 4 Listiny stanoví, že vyvlastnění nebo nucené omezení vlastnického práva je možné ve veřejném zájmu, a to na základě zákona a za náhradu. Předkládaný návrh může omezit možnost provozovatelů strategicky významné infrastruktury svobodně nakládat se svým majetkem, ale k takovému omezení dochází při uplatnění principu proporcionality vůči ochraně veřejného zájmu ve formě zvyšování bezpečnosti státu. Minimalizaci zásahu do vlastnictví povinných osob zajišťuje přiměřená lhůta k výměně produktu či služby vysoce rizikového dodavatele, která v maximální možné míře respektuje životní cyklus produktů.

Institut zajišťování dostupnosti strategicky významné služby je pak jen nadstavbou zavádění bezpečnostních opatření, která návrh zákona ukládá všem povinným osobám, nejen okruhu poskytovatelů strategicky významných služeb. S tímto se návrh zákona ve své důvodové zprávě vypořádal následovně: Omezení práva na užívání majetku, za které by snad povinná bezpečnostní opatření uložená tímto návrhem zákona a jeho budoucími prováděcími právními předpisy mohla být považována, resp. jejich účel, chrání obecné zájmy, kterými jsou bezpečnost státu a obyvatelstva či významné ekonomické a společenské zájmy. Kybernetická bezpečnost České republiky jako podmnožina bezpečnosti České republiky spadá do rozsahu působnosti ústavního zákona o bezpečnosti České republiky. Podle čl. 1 uvedeného ústavního zákona je zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot základní povinností státu. Návrh zákona lze považovat za jeden z prostředků plnění této povinnosti státu. Návrh zákona zároveň reflektuje postavení kybernetické bezpečnosti jako nedílného předpokladu rozvoje digitální společnosti a ekonomiky, o nějž Česká republika jako členský stát EU usiluje.

4.   Zhodnocení souladu návrhu právního předpisu se závazky vyplývajícími pro Českou republiku z jejího členství v Evropské unii

V otázce stanovení množiny tzv. strategicky významných služeb se jedná o otázku, která je upravena z národních požadavků – strategicky významné služby bylo potřeba v rámci návrhu zákona vytvořit zejm. pro potřeby národního požadavku Bezpečnostní rady státu k vytvoření tzv. mechanismu prověřování bezpečnosti dodavatelského řetězce, ale i pro stanovení okruhu adresátů pro zajištění dostupnosti strategicky významné služby. Vytvoření množiny strategicky významných služeb návrh zákona podmiňuje tím, že se musí podle § 25 návrhu zákona jednat o již zákonem regulovanou službu. Toto stanovení není v rozporu s právem Evropské unie.

Specificky cílem povinnosti zajištění dostupnosti strategicky významné služby podle § 33 je řešit situace, kdy je část primárních a podpůrných aktiv strategicky významných služeb umístěna mimo území České republiky. Lokalizace primárních a podpůrných aktiv strategicky významných služeb mimo území České republiky s sebou nese určitou míru rizika pro zajištění dostupnosti těchto strategicky významných služeb v případě omezení dostupnosti nepostradatelných aktiv nacházejících se v zahraničí v důsledku kybernetického bezpečnostního incidentu (jde zejména o rizika spojená s nedostupností dat a služeb v případech přírodních katastrof, války, havárie v datovém centru, ztráty konektivity, pandemie či jiných nepředvídatelných událostí na území cizích států, kdy Česká republika nemá legální ani faktickou možnost činit potřebná opatření k řešení dopadů těchto událostí v případech, kdy budou zasažena aktiva potřebná k zajištění fungování strategicky významných služeb). Zákaz vývozu klíčových aktiv není vhodný a není ani návrhem zákona požadován, a proto bylo potřeba nalézt opatření, které takový zákaz nevyžaduje, ale nastavuje procesy, jak mitigovat dopady uvedené situace. Hlavním cílem zajištění dostupnosti strategicky významné služby tedy není přenesení primárních a podpůrných aktiv strategicky významných služeb na území České republiky, nýbrž zajištění kontinuity poskytování klíčových (strategicky významných) služeb zásadních pro stabilitu, vnitřní pořádek a bezpečnost České republiky, a to tím, že poskytovatel služby zajistí kontinuitu služby o omezené míře (tzv. nezbytný rozsah, tedy legislativně dané omezení oproti běžnému rozsahu služby na nezbytnou míru poskytovaných služeb, viz níže) zpravidla náhradním způsobem (navíc tak, že způsob a čas si stanoví poskytovatel sám, viz níže). Povinnost obsažená v odůvodňovaném ustanovení cílí na rizika spojená s dostupností poskytované strategicky významné služby. Mitigace těchto rizik je stanovena jako semi-performativní cíl tohoto ustanovení. Poskytovateli strategicky významné služby je uložena povinnost zajistit dostupnost této služby s ponecháním svobody ve výběru prostředků, jakými tohoto cíle dosáhne. Nicméně je limitován nutností zajistit v případě nastalého problému tuto dostupnost z České republiky a zajistit ji v nezbytném rozsahu, který stanoví toto nařízení vlády. Je tedy omezen v možnosti zajistit dostupnost služeb poskytovaných z území mimo území České republiky pouze za využití standardních smluvních ujednání mezi poskytovatelem služby a jejím uživatelem/odběratelem (typicky tzv. SLA, Service-Level Agreement), jelikož na tyto se nelze v případě mimořádných událostí, jako je válka či přírodní katastrofa, u takto významných služeb spoléhat. Zajištění dostupnosti strategicky významné služby z území České republiky nevylučuje možnost poskytování těchto služeb a jejich řízení za běžné situace a v rámci běžného rozsahu poskytování takové služby také z území mimo Českou republiku. Musí však existovat takový scénář, zejména v rámci plánu zajišťování kontinuity činností, kdy v případě problému bude poskytovatel strategicky významné služby schopen zajistit obnovení dostupnosti poskytované strategicky významné služby v nezbytném (legislativně daném) rozsahu a její další poskytování výhradně z území České republiky, a to bez použití aktiv mimo území České republiky. Takováto povinnost není v rozporu s právem Evropské unie.

V oblasti předmětné úpravy ani kybernetické bezpečnosti v širším smyslu nebyla doposud vytvořena žádná judikatura soudních orgánů Evropské unie.

Nařízení vlády je v souladu s obecnými zásadami práva Evropské unie.

5.   Zhodnocení souladu navrhované právní úpravy s mezinárodními smlouvami, jimiž je Česká republika vázána

Na mezinárodním poli neexistuje mezinárodní smlouva, která by upravovala problematiku kybernetické bezpečnosti, co se týče návrhu tohoto nařízení, zde jsou pro vyhodnocení relevantní zejména dohody týkající se mezinárodního obchodu, s čímž se důvodová zpráva k samotnému návrhu zákona vyrovnala následujícím způsobem:

Předkládaný návrh nařízení je v souladu rovněž s výjimkami smluv inkorporovaných do Dohody o zřízení Světové obchodní organizace. Jejich společným cílem je zamezení vytváření bariér mezinárodního obchodu a vzájemná doložka nejvyšších výhod, tzn. povinnost zacházet s investory a dodavateli smluvních stran ne méně příznivě než se subjekty třetích států. Předkládaný návrh má potenciál omezit zacházení s dodavateli některých smluvních stran na úroveň méně příznivou ve srovnání se zacházením s dodavateli ze třetích států, ale dochází tak v rámci níže uvedených povolených výjimek.

Všeobecná dohoda o clech a obchodu 1994 (GATT) připouští v čl. XX opatření omezující mezinárodní obchod za předpokladu jejich nutnosti a) k ochraně života a zdraví lidí, nebo d) zachování zákonů a jiných předpisů, které nejsou neslučitelné s jejími ustanoveními. Všeobecná dohoda o obchodu službami (GATS) v čl. XIV upravuje výjimky obdobně jako GATT, přičemž opatření k zabezpečení shody s právními předpisy doplňuje demonstrativní výčet explicitně zmiňující bezpečnostní předpisy (čl. XIV písm. c) bod (iii)).

Omezení mezinárodního obchodu předkládaným návrhem zákona je plně v souladu s výjimkami GATT i GATS, a proto neodporuje závazkům České republiky přijatým v rámci Světové obchodní organizace.

Uvedené skutečnosti se rovněž aplikují ve vztahu k bezpečnosti dodavatelského řetězce. V kontextu této problematiky Úřad provedl průzkum a konzultace u zahraničních partnerů Úřadu, jako jsou analogie Úřadu ze Spojeného království či Německa. Uvedené země již obdobným mechanismem disponují, přičemž gestoři mechanismů neshledávají rozpor mezi fungováním vlastního mechanismu bezpečnosti dodavatelského řetězce, směřujícímu k ochraně bezpečnosti a veřejného pořádku, a smyslem smluv GATT či GATS, jakožto závazcích těchto zemí přijatých na plénu Světové obchodní organizace.

V rámci mechanismu by měly být uplatněny výjimky v případě limitování nebo zákazu dodavatele, zejména ve smyslu čl. XIV GATS a čl. XX GATT a také ve smyslu čl. XIVbis GATS a čl. XXI GATT. Nástroje mechanismu bezpečnosti dodavatelského řetězce se vztahují pouze na nejkritičtější infrastrukturu, jejíž narušení má schopnost narušit jak veřejný pořádek či veřejnou morálku ve smyslu č. XIV GATS a XX GATT, tak také ohrozit bezpečnost státu, což spadá pod čl. XIVbis GATS a čl. XXI GATT.

Navrhovaná právní úprava je dále v souladu s bilaterálními dohodami o podpoře a ochraně investic. Dohody o ochraně investic zavazují Českou republiku k tomu, aby poskytovala ochranu investorům pocházejícím z jiných smluvních států a jejich investicím v České republice. Jednou z podmínek zakotvených ve valné většině bilaterálních dohod o podpoře a ochraně investic, která určuje, zda je zahraniční investice chráněnou investicí, je soulad hospodářských aktivit investora s vnitrostátními předpisy druhé smluvní strany. Předkládaný návrh vytváří právní rámec především pro budoucí investice, kladení nových nároků na dodavatele tudíž není v rozporu s uvedeným.

Ochrana stávajících investic podle bilaterálních dohod o podpoře a ochraně investic taktéž není narušena, neboť návrh respektuje životní cyklus produktů, proto nevytváří nadbytečné náklady spojené s již uskutečněnou investicí. Dostatečná lhůta navíc umožňuje investorům se na nové právní podmínky adaptovat, jak změnou dodavatelů, tak snížením vlastní rizikovosti investorů, jejíž kritéria jsou součástí předkládaného návrhu zákona. Jedná se tudíž o minimální možný zásah k dosažení účelu předkládaného návrhu zákona, zajištění bezpečnosti dodavatelského řetězce strategicky významné infrastruktury. V neposlední řadě obsahuje většina bilaterálních dohod o podpoře a ochraně investic doložku se základními bezpečnostními zájmy smluvních stran. Doložka opravňuje strany přijmout taková opatření, která považují za nezbytná pro ochranu svých základních bezpečnostních zájmů. Ochrana nejvýznamnější kritické infrastruktury nezbytné pro fungování státu se řadí pod základní bezpečnostní zájem státu, tudíž lze případná omezení vyplývající z aplikace předkládaného návrhu podřadit pod skutkovou podstatu uvedené výjimky.

Bilaterální dohody o podpoře a ochraně investic také řadí mezi základní bezpečnostní zájmy smluvní strany ty zájmy, které vyplývají z jejího členství v celní, hospodářské nebo měnové unii, volném trhu nebo zóně volného obchodu. Směrnice NIS 2 ukládá členským státům, aby zajistily přijetí opatření k řízení bezpečnostních rizik sítí a informačních systému, přičemž bezpečnost dodavatelského řetězce zmiňuje v čl. 21 odst. 2. písm. d) v demonstrativním výčtu minima nutných opatření. Návrh právní úpravy mechanismu prověřování bezpečnosti dodavatelského řetězce tedy není v rozporu s bilaterálními dohodami o ochraně investic, jimiž je Česká republika vázána.

6.   Zhodnocení, zda návrh právního předpisu neobsahuje ustanovení, které by bylo svou povahou technickým předpisem podle právního předpisu upravujícího technické požadavky na výrobky

Ustanovení návrhu tohoto nařízení obsahují pouze vymezení okruhu osob – poskytovatelů strategicky významné služby, žádné technické požadavky na výrobky toto nařízení neobsahuje.

7.   Informace o splnění oznamovací povinnosti podle tohoto právního předpisu (ve vztahu k ne/obsaženým ustanovením, která by byla svou povahou technickým předpisem podle právního předpisu upravujícího technické požadavky na výrobky)

Vzhledem k posouzení dle bodu 6 oznamovací povinnost nevznikla.

8.   Informace o konzultaci návrhu právního předpisu s Evropskou centrální bankou a výsledku konzultace, podléhá-li návrh právního předpisu takové konzultaci

Návrh nařízení vlády nemá vliv na měnovou politiku Evropské unie, tedy nepodléhá konzultaci s Evropskou centrální bankou.

9.   Předpokládaný hospodářský a finanční dopad návrhu právního předpisu na státní rozpočet a ostatní veřejné rozpočty

Samotné nařízení vlády dopad na státní rozpočet ani ostatní veřejné rozpočty nemá, dopady vyvolává zákon, k jehož provedení je vydáváno. Zvýšení zabezpečení u organizací naplňujících kritéria založená návrhem zákona a stanovená tímto návrhem nařízení vlády bude mít finanční dopady vyčíslené v rámci důvodové zprávy k návrhu zákona, každopádně však přispěje k budování důvěry spotřebitelů a obchodních partnerů, případně i zahraničních investorů, které může přilákat právě vysoká míra bezpečnosti českého ICT prostředí.

Stanovení kritérií pro strategicky významné služby přímo ovlivňuje to, jakým typům organizací a kolika takovým organizacím budou aktivovány návrhem zákona předpokládané povinnosti týkající se strategicky významných služeb. Těmito povinnostmi jsou zapojení se do mechanismu prověřování bezpečnosti dodavatelského řetězce a povinnost řešit zajištění dostupnosti strategicky významné služby.

V otázce vyčíslení nákladů na zapojení se do mechanismu prověřování bezpečnosti dodavatelského řetězce lze odkázat plně na důvodovou zprávu k návrhu zákona – důvodová zpráva a hodnocení dopadů regulace byly k tomuto tématu zpracovány již v první verzi návrhu zákona do mezirezortního připomínkového řízení a následně byly ještě dále na základě požadavků doplňovány. Zkráceně je možno uvést, že náklady přímo spojené s plněním této povinnosti jsou dány v rozsahu administrativní zátěže, která bude provedena přímo v souvislosti s vynaložením přiměřeného úsilí při zjišťování informací o dodavatelích bezpečnostně významných dodávek a evidencí a hlášením těchto informací ve smyslu § 31 návrhu zákona. Další případné náklady případně může generovat omezení rizik spojených s dodavatelem, pokud bude takové omezení vydáno – toto je však již předmětem aplikace daného mechanismu na danou situaci a jako takové je toto posuzováno v okamžiku vydávání daného konkrétního opatření.

Pro povinnost zajistit dostupnost strategicky významné služby je možno uvést to stejné, co je uvedeno výše, nicméně je možné nad rámec odůvodnění návrhu zákona dodat, že se jedná de facto o rozšíření a nadstavbu povinnosti zavádět a provádět bezpečnostní opatření, která je uložena každému poskytovateli regulované služby v návrhu zákona, zejm. v rámci tzv. řízení kontinuity činností. Toto bezpečnostní opatření má pak vliv na schopnost organizace rychle a účinně reagovat na úmyslné a neúmyslné kybernetické bezpečnostní incidenty (např. sabotáž nebo přírodní katastrofy). Všem poskytovatelům regulovaných služeb v režimu vyšších povinností je tak již bezpečnostními opatřeními uloženo vypracovat politiku řízení kontinuity činností, která nastavuje základní procesy, práva a povinnosti, a dále stanovit cíle řízení kontinuity činností ve smyslu stanovení doby obnovy chodu, minimální úrovně poskytovaných služeb a tzv. bodu obnovy dat. Z tohoto důvodu a z důvodu, že povinnost zajistit dostupnost strategicky významné služby není přímo spojena s povinností provést dodatečné investice, jsou náklady přímo spojené se stanovením nezbytného rozsahu, tedy takové, které budou pro všechny poskytovatele strategicky významné služby stejné, dány v rozsahu administrativní zátěže, která bude provedena přímo v souvislosti s plněním ustanovení o zajištění dostupnosti a nad rámec klasického řízení kontinuity činností. Ve specifických případech pak může některý z poskytovatelů strategicky významné služby dospět k závěru, že pro zajištění dostupnosti strategicky významné služby je v jeho situaci potřeba provést dodatečné investice. Taková situace má mnoho proměnných, protože závisí na povaze jím poskytované služby, technologickém i geografickém rozvržení aktiv, které pro danou službu používá, na tom, jakým způsobem vyhodnocuje požadavky na zajištění kontinuity činností, a v neposlední řadě také na tom, jak přistoupil ke stanovení času a kvality v rámci splnění povinnosti zajištění dostupnosti strategicky významné služby.

10.   Předpokládaný dopad návrhu právního předpisu na práva a povinnosti fyzických a právnických osob

Navrhovaná právní úprava nezakládá fyzickým a právnickým osobám žádná nová práva ani povinnosti. Práva a povinnosti jsou upraveny v návrhu zákona, který zmocňuje k vydání tohoto nařízení. Návrh nařízení představuje návrh prováděcího právního předpisu, na jehož základě vzhledem k jeho povaze nemohou být ukládány povinnosti ani vznikat nová práva.

11.   Předpokládaný dopad návrhu právního předpisu na podnikatelské prostředí České republiky

Samotné nařízení vlády o strategicky významných službách nemá na podnikatelské prostředí žádný vliv, neboť takovéto dopady vyvolává výhradně návrh zákona, k jehož provedení je toto nařízení vlády vydáváno. Hodnocení dopadů návrhu zákona na podnikatelské prostředí je podrobně rozvedeno v rámci hodnocení dopadů návrhu zákona.

12.   Předpokládaný sociální dopad návrhu právního předpisu, včetně dopadu na specifické skupiny obyvatel, především na osoby sociálně slabé, osoby se zdravotním postižením a národnostní menšiny

Nařízení vlády nemá specifický dopad na specifické skupiny obyvatel, zejména osoby sociálně slabé, osoby se zdravotním postižením a národnostní menšiny.

13.   Předpokládaný dopad návrhu právního předpisu na rovnost mužů a žen, upravuje-li návrh právního předpisu postavení fyzických osob nebo se tohoto postavení dotýká

Nařízení vlády je z hlediska zákazu diskriminace a z hlediska rovnosti mužů a žen neutrální, resp. nemá žádný dopad.

14.   Předpokládaný dopad návrhu právního předpisu na životní prostředí

Nařízení vlády nemá specifický dopad na životní prostředí.

15.   Předpokládaný dopad návrhu právního předpisu na ochranu práv dětí

Nařízení vlády nemá specifický dopad na ochranu práv dětí.

16.   Předpokládaný dopad návrhu právního předpisu na bezpečnost nebo obranu státu

Nařízení vlády má v návaznosti na návrh zákona velmi pozitivní dopady na bezpečnost a obranu státu, zejména přispěje k dalšímu posílení zabezpečení klíčových služeb v České republice, čímž dojde k posílení zabezpečení českého kyberprostoru jako celku a rovněž ke snížení míry rizika realizace incidentů, které by mohly ohrozit bezpečnost České republiky jako celku. Vydáním tohoto nařízení vlády dojde nejen ke stanovení strategicky významných služeb, ale také ke stanovení toho, které části strategicky významné služby mají být brány specificky v potaz při stanovování zajištění dostupnosti u strategicky významných služeb.

17.   Zhodnocení dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů

Návrh se netýká soukromí. Nařízení vlády nemá specifický dopad ve vztahu k ochraně osobních údajů. Okrajově může stanovení strategicky významných služeb a tedy i aktivace dalších zákonných povinností spojených se strategicky významnými službami zvýšit ochranu těch služeb, resp. informačních systémů, které se pro tyto služby využívají a potenciálně tedy i zvýšit ochranu osobních údajů zpracovávaných v těchto systémech.

18.   Zhodnocení, zda návrhem právního předpisu není zakládána veřejná podpora

Navrhovanou právní úpravou není zakládána veřejná podpora. Veřejná podpora je termín vycházející ze Smlouvy o fungování EU, kdy se jí rozumí každá podpora poskytnutá v jakékoli formě státem nebo z veřejných prostředků, která narušuje nebo může narušit hospodářskou soutěž tím, že zvýhodňuje určité podniky nebo určitá odvětví výroby a ovlivňuje obchod mezi členskými státy. Podpora, která splňuje uvedená kritéria, je neslučitelná se společným trhem EU, a tedy zakázaná. Návrh nařízení nepracuje s rozdělováním veřejných prostředků, neobsahuje přímé či nepřímé zvýhodnění určitých podniků či odvětví a nemá selektivní charakter.

19.   Zhodnocení korupčních rizik návrhu právního předpisu

Nařízení vlády nezakládá žádná nová korupční rizika.

20.   Odůvodnění případného návrhu, aby Poslanecká sněmovna vyslovila s návrhem právního předpisu souhlas již v prvém čtení (pokud se navrhuje)

Nařízení vlády neprojednává Poslanecká sněmovna.

21.   Odůvodnění případného návrhu, aby navrhovaná právní úprava nabyla účinnosti dříve než počátkem patnáctého dne následujícího po dni jejího vyhlášení (pokud se navrhuje)

Nenavrhuje se, aby navrhovaná právní úprava nabyla účinnosti dříve než počátkem patnáctého dne následujícího po dni jejího vyhlášení.

22.   Odůvodnění odchylek v postupu projednání návrhu právního předpisu (pokud se navrhují a jsou odlišné od předchozích) (jsou-li navrhovány, může být konzumováno přechozími kapitolami)

Nejsou navrhovány žádné odchylky v postupu projednávání návrhu právního předpisu.

II. Zvláštní část

K § 1

Návrh nařízení vlády navazuje na zákonem o kybernetické bezpečnosti stanovená zmocnění k vydání prováděcího právního předpisu, kterým se stanoví strategicky významné služby. Poskytovatel strategicky významné služby je poskytovatelem regulované služby, kterému nad rámec běžných povinností poskytovatele regulované služby plynou povinnosti také z tzv. mechanismu prověřování bezpečnosti dodavatelského řetězce a povinnost zajištění dostupnosti strategicky významné služby. Nařízení vlády ve své druhé části pak také navazuje na zákonné zmocnění ukládající vládě stanovit tzv. nezbytný rozsah zajištění dostupnosti strategicky významných služeb.

K § 2

Z důvodu větší přehlednosti jsou regulované služby, které splňují podmínky strategicky významné služby podle § 25 zákona uvedeny v příloze č. 1 tohoto nařízení vlády.

K § 3

Z důvodu větší přehlednosti je stanovení a vymezení nezbytného rozsahu strategicky významné služby, tedy částí strategicky významných služeb, jejichž nedostupnost by mohla mít závažný dopad na bezpečnost České republiky nebo vnitřní pořádek uvedeno v příloze č. 2 tohoto nařízení vlády.

K § 4

Zákon a nařízení jsou vzájemně komplementární. Je v zájmu jak normotvůrce, tak adresátů prováděcího právního předpisu, aby zákon a nařízení vstoupily v účinnost ve stejný okamžik. Jelikož zákon, k jehož provedení se nařízení vydává, nemá k okamžiku zahájení meziresortního připomínkového řízení známý pevný okamžik nabytí účinnosti, tak termín účinnosti návrhu nařízení byl po konzultaci se Sbírkou zákonů orientačně dán na datum, které umožňuje zahájit v systému eLegislativa meziresortní připomínkové řízení, nicméně i nadále se počítá s úpravou účinnosti nařízení podle účinnosti zákona.

K označení přílohy č. 1 příloha č. 1

Příloha č. 1 stanovuje, které regulované služby splňují podmínky strategicky významné služby podle § 25 zákona. Strategicky významnou službou je podle § 25 odst. 1 zákona regulovaná služba, jejíž narušení by mohlo mít závažný dopad na bezpečnost České republiky nebo vnitřní pořádek. Podstatné pro stanovení strategicky významných služeb je tedy nejen to, že se musí jednat o takové služby, které mají mít potenciálně závažný dopad na bezpečnost České republiky nebo vnitřní pořádek, ale také se musí jednat o takové služby, které splňují podmínky pro registraci regulované služby podle § 4 nebo § 5 návrhu zákona, resp. že jsou jako takové registrovány. Touto podmínkou je dáno, že nařízení vlády a způsob, jakým jsou v rámci něj stanovena kritéria strategicky významné služby, jsou úzce spjaty s podobou vyhlášky o regulovaných službách vydané Úřadem. Regulované služby splňující podmínky strategicky významné služby jsou vymezeny v řešeném ustanovení a jejich ekvivalenty jsou také uvedeny v příloze vyhlášky o regulovaných službách.

V jednotlivých odstavcích řešeného ustanovení jsou kritéria strategicky významné služby rozdělena podle odvětví, obdobně jako je tomu u vyhlášky o regulovaných službách.

K příloze č. 1 odst. 1

První odstavec přílohy č. 1 stanovuje strategicky významné služby v odvětví veřejná správa.

Strategicky významné služby v odvětví veřejná správa jsou vymezeny výkonem svěřených pravomocí vykonávaným těmi orgány nebo osobami, které jsou v nařízení vlády vyjmenovány. Předmětný výčet vychází z obsahu přílohy vyhlášky o regulovaných službách, odvětví 1. Veřejná správa, služby 1.1. Výkon svěřených pravomocí, bod I. písm. a) až l). Jedná se o skupiny organizací v rámci veřejné správy, u kterých by narušení bezpečnosti v jejich aktivech mohlo vést k významnému systémovému omezení služeb pro občany státu a chod státu jako takový, dále pak organizace pracující s největším množstvím osobních údajů, a to i zvláštních kategorií osobních údajů. Ústřední orgány státní správy jsou často těmi, kdo spravují a provozují služby strategického významu, na jejichž funkčnost je navázáno praktické fungování dalších veřejných orgánů. Příklady takových služeb jsou Úřadu známy z jeho předcházející úřední činnosti, a to zejména ve vztahu ke kritické infrastruktuře státu, do které většina vybraných subjektů spadá již nyní. Nefunkčnost těchto strategických služeb by pak představovala v rámci správního fungování státu riziko dominového efektu velkého rozsahu, kdy by nemohly fungovat služby navazující na služby poskytované na ústřední úrovni státu. Rovněž byla zohledněna skutečnost, že stát by měl v rámci naplňování zajištění nedistributivního práva na bezpečnost být tím, kdo pro zajištění bezpečného digitálního prostředí pro občany zajišťuje co nejvyšší míru bezpečnosti, veřejné instituce na ústřední úrovni spravují velké množství informací, které jim často poskytují občané, přičemž občané nemají možnost vybrat si tyto údaje daným orgánům neposkytnout tak, jako tomu je u běžných soukromoprávních vztahů, kde si mohou zvolit jiného poskytovatele plnění, jehož zajišťování bezpečnosti věří více. Stejně tak pokrytí vybraných organizací zabývajících se vymáháním práva a stíháním trestné činnosti je dáno tím, že pokud tyto organizace mají zajišťovat nedistributivní právo na bezpečnost občanů, měly by tak činit prostřednictvím procesů, které jsou samy o sobě bezpečné. Vzhledem k výše uvedenému je významným aspektem i tzv. reputační riziko, kdy státní organizace, které jsou zodpovědné za zajištění nedistributivního práva občanů na bezpečnost, případně neriskují pouze pověst sebe jako organizace, ale i důvěru občanů ve stát a v to, jak zajišťuje jejich právo na bezpečnost. Další subjekty jsou pak mezi strategicky významné zařazeny s přihlédnutím k jejich zvláštnímu významu pro důvěru občanů ve stát, jelikož zajišťují chod ústředních zákonodárných či výkonných institucí. V neposlední řadě je zařazení těchto organizací mezi poskytovatele strategicky významné služby vedeno i zvýšeným výskytem situací tzv. proprietárního uzamčení (*vendor lock-in*) ve veřejnosprávním segmentu regulovaných osob.

K příloze č. 1 odst. 2

Druhý odstavec přílohy č. 1 stanovuje strategicky významné služby v odvětví energetiky.

Jednotlivé níže uvedené služby cílí na nejvýznamnější prvky energetického odvětví v České republice, a to jak v elektřině, ropě, ale i zemním plynu. Níže uvedená kritéria vycházejí jak z podstaty praktického fungování regulovaných služeb, tak i z dosavadní regulace, ať už zákona o kybernetické bezpečnosti nebo krizového zákona.

K písmeni a):

Dle písmene a) se jedná o výrobu elektřiny v rámci výrobny s celkovým instalovaným elektrickým výkonem nejméně 100 MW vykonávanou držitelem licence na výrobu elektřiny podle energetického zákona. Vzhledem ke skutečnosti, že se jedná o síťové odvětví, toto upřesnění výkonu míří na vyčlenění skupiny těch nejvýznamnějších elektráren v České republice. Cílem zahrnutí těchto elektráren mezi poskytovatele strategicky významné služby je, aby se minimalizovalo riziko případného výpadku dodávek elektrické energie (tzv. *blackout*) způsobeného kybernetickým bezpečnostním incidentem, jelikož výroba elektřiny je první službou, od které se další služby (přenos elektřiny, distribuce elektřiny atd.) odvíjí a mohou na ní být závislé.

K písmeni b):

Dle písmene b) se jedná o provoz přenosové soustavy elektřiny vykonávaný držitelem licence na přenos elektřiny podle energetického zákona – jak již bylo zmíněno výše, jedná se o síťové odvětví a nelze tak na činnosti související s elektřinou pohlížet jako na samostatné bloky, ale na soustavu vzájemně se ovlivňujících prvků. Služba provoz přenosové soustavy tvoří páteř elektrizační soustavy, zajišťuje propojení elektrizační soustavy se zahraničními soustavami a dále slouží pro vyvedení výkonu z velkých systémových elektráren. Toto kritérium tak má za cíl zahrnout poskytovatele výše uvedené regulované služby mezi poskytovatele strategicky významné služby, jelikož se jedná o strategicky významný subjekt a kybernetický bezpečnostní incident by mohl způsobit fatální důsledky.

K písmeni c):

Dle písmene c) se jedná o provoz regionální distribuční soustavy elektřiny v rámci celé distribuční soustavy elektřiny vykonávaný držitelem licence na distribuci elektřiny podle energetického zákona. Regionální distribuční soustava je v energetickém zákoně v § 2 odstavci 2 písmeni a) bodě 24 vymezena jako distribuční soustava, která je přímo připojena na přenosovou soustavu. Ustanovení skrze omezení na regionální distribuční soustavu míří na nejvýznamnější distributory elektřiny v České republice, jejichž výpadek by mohl přímo ovlivnit přenosovou soustavu. Cílem zahrnutí těchto provozovatelů distribuční soustavy mezi poskytovatele strategicky významné služby je, aby se minimalizovalo riziko případného výpadku dodávek elektrické energie způsobeného kybernetickým bezpečnostním incidentem, který by mohl vést k zasažení velkého množství obyvatel a chodu významných podniků v České republice.

K písmeni d):

Dle písmene d) se jedná o provoz ropovodu vykonávaný provozovatelem ropovodu podle zákona o nouzových zásobách ropy. Toto ustanovení míří na dva vnitrostátní ropovody, které by v případě kybernetického bezpečnostního incidentu mohly ovlivnit celou Českou republiku. Z tohoto důvodu toto kritérium řadí právě tyto subjekty mezi poskytovatele strategicky významné služby.

K písmeni e):

Dle písmene e) se jedná o provoz produktovodu vykonávaný provozovatelem produktovodu podle zákona o nouzových zásobách ropy. Tato služba je strategicky významnou službou z důvodu, že produktovody se používají pro potrubní přepravu ropných produktů. V případě kybernetického bezpečnostního incidentu u produktovodů by tak mohlo dojít k ovlivnění přepravy motorových paliv a tím následně k ovlivnění velkého množství obyvatel i chodu významných podniků České republiky.

K písmeni f):

Dle písmene f) se jedná o provoz přepravní soustavy zemního plynu vykonávaný držitelem licence na přepravu plynu podle energetického zákona. Tato služba je zřizována ve veřejném zájmu a slouží k přepravě plynu mimo jiné i se zahraničními plynárenskými soustavami. Daná služba je v České republice vykonávána prostřednictvím jediného nezávislého podniku. V případě kybernetického bezpečnostního incidentu u tohoto poskytovatele regulované služby by tak mohlo dojít k ovlivnění přepravy plynu a tím následně k ovlivnění důležitých společenských činností, např. distribuce plynu koncovým odběratelům, mezi nimiž jsou nejen fyzické, ale i právnické osoby.

K písmeni g):

Dle písmene g) se jedná o provoz distribuční soustavy zemního plynu v rámci celé distribuční soustavy plynu s licencovanou přenosovou kapacitou nejméně 1 000 MW vykonávaný držitelem licence na distribuci plynu podle energetického zákona. Jak již bylo zmíněno výše, i u plynárenství se jedná o síťové odvětví a služby vykonávané jednotlivými poskytovateli na sebe mnohdy bezprostředně navazují. Upřesnění přenosové kapacity míří na vyčlenění nejvýznamnějších distributorů plynu v České republice, kteří zajišťují i činnosti související se zabezpečením spolehlivého a bezpečného provozu distribuční soustavy a kteří by tak měli patřit mezi poskytovatele strategicky významné služby.

K písmeni h):

Dle písmene h) se jedná o činnost Elektroenergetického datového centra podle energetického zákona vykonávanou držitelem licence na činnost Elektroenergetického datového centra podle energetického zákona. Mezi hlavní služby Elektroenergetického datového centra patří řízení dat pro účely zajištění sdílení, akumulace, flexibility nebo agregace elektřiny na celém území České republiky. Neposkytování těchto služeb by mohlo způsobit výkyvy v celé přenosové soustavě elektřiny, což by mohlo vést dominovému efektu a ke kolapsu celé přenosové soustavy elektřiny v České republice. Z těchto důvodů je nezbytné, aby technologie používané k řízení těchto dat byly bezpečné, a proto by Elektroenergetické datové centrum mělo patřit mezi poskytovatele strategicky významné služby.

K písmeni i):

Dle písmene i) se jedná o činnost nominovaného organizátora trhu s elektřinou podle přímo použitelného předpisu Evropské unie, jímž je nařízení Evropského parlamentu a Rady (EU) 2019/943 ze dne 5. června 2019 o vnitřním trhu s elektřinou, v platném znění. Výkon činnosti nominovaného organizátora trhu s elektřinou, která je v současné době svěřena operátorovi trhu podle § 20a energetického zákona a odpovídá výlučné licenci pro celé území České republiky, spočívá především v organizaci trhu s elektřinou, včetně vyhodnocování odchylek za celé území České republiky, a jako taková je z hlediska významu pro trh s elektřinou nezastupitelná. Je proto nezbytné, aby byl také nominovaný organizátor trhu s elektřinou zařazen mezi poskytovatele strategicky významné služby.

K příloze č. 1 odst. 3

Třetí odstavec přílohy č. 1 stanovuje strategicky významné služby v odvětví dopravy - letecké a drážní. Níže uvedené strategicky významné služby jsou toho typu, že mají plošný vliv fungování daného odvětví napříč Českou republikou.

K písmeni a):

Dle písmene a) se jedná o řízení letového provozu (ATC) ve vzdušném prostoru České republiky vykonávané provozovatelem služby řízení letového provozu v převážné části vzdušného prostoru České republiky podle přímo použitelného předpisu Evropské unie. Poskytovatel regulované služby je v tomto případě zodpovědný za řízení letového provozu nad celým územím státu a narušení bezpečnosti ve vztahu k jeho aktivům by tak mohlo mít dopady na samotné fungování státu a významně ohrozit bezpečnost obyvatelstva.

K písmeni b):

Dle písmene b) se jedná o meteorologické služby (MET) podle čl. 2 bodu 29 Nařízení Evropského parlamentu a Rady (ES) č. 549/2004 ze dne 10. března 2004 , kterým se stanoví rámec pro vytvoření jednotného evropského nebe (rámcové nařízení) vykonávané poskytovatelem letových navigačních služeb podle téhož předpisu Evropské unie, v případě, že je určeným a osvědčeným poskytovatelem meteorologických služeb podle téhož předpisu Evropské unie s působností pro poskytování meteorologických informací pro potřeby letectví v celé České republice. Tento poskytovatel regulovaných služeb dodává nepostradatelné podklady pro řízení letového provozu nad vzdušným prostorem ČR a narušení jejich bezpečnosti by tak mohlo vést dominovým efektem k dopadům obdobným těm uvedeným výše u služby dle písmene a) tohoto odstavce.

K písmeni c):

Dle písmene c) se jedná o provozování železniční dopravní cesty (v rámci předchozího zákona č. 181/2014 Sb., o kybernetické bezpečnosti označované také jako stavění vlakových cest) vykonávané osobou poskytující službu stavění vlakových cest na celostátní úrovni. Tato služba je specifická v tom ohledu, že existuje pouze omezené množství železniční infrastruktury a tato síť není tak rozsáhlá jako například infrastruktura silniční dopravy. Z toho plyne základní omezení. V případě, že by došlo ke kybernetickému bezpečnostnímu incidentu a následné nehodě na některém z úseků železniční tratě, není možné ho jednoduše a rychle nahradit jinou trasou. Tato skutečnost s sebou přináší riziko, že v případě scénáře, během něhož by došlo k uzavření větší části železniční infrastruktury, by takové omezení mohlo mít závažné dopady.

K příloze č. 1 odst. 4

Čtvrtý, poslední odstavec přílohy č. 1 stanovuje strategicky významné služby v odvětví digitální infrastruktury a služeb.

K písmeni a):

Dle písmene a) se jedná o poskytování veřejně dostupné služby elektronických komunikací v rozsahu služeb přístupu k internetu a interpersonálních komunikačních služeb vykonávané osobou poskytující veřejně dostupnou službu elektronických komunikací podle zákona o elektronických komunikacích skrze nejméně 350 000 aktivních mobilních SIM karet nebo nejméně 100 000 aktivních pevných internetových přípojek na území České republiky. Narušení bezpečnosti informací těchto subjektů by mělo s ohledem na počet a významnost odběratelů této služby potenciálně dominový efekt ovlivňující významně chod státu a poskytování služeb pro občany.

K písmeni b):

Dle písmene b) se jedná o zajišťování veřejné komunikační sítě elektronických komunikací vykonávané osobou poskytující veřejně dostupnou službu elektronických komunikací podle zákona o elektronických komunikacích skrze nejméně 350 000 aktivních mobilních SIM karet nebo nejméně 100 000 aktivních pevných internetových přípojek na území České republiky. Narušení bezpečnosti informací těchto subjektů by mělo s ohledem na počet a významnost odběratelů této služby potenciálně dominový efekt ovlivňující významně chod státu a poskytování služeb pro občany.

K písmeni c):

Dle písmene c) se jedná o správu a provoz registru domény nejvyšší úrovně vykonávanou osobou spravující a provozující registr domény nejvyšší úrovně. Správce a provozovatel registru domén nejvyšší úrovně je tím, kdo zajišťuje funkčnost domén s doménovým jménem nejvyšší úrovně pro Českou republiku, tedy „.cz“. Narušení bezpečnosti informací v jeho aktivech by tak opět vedlo k významnému dominovému efektu a mělo dopad jak na poskytování služeb občanům státu, tak i na chod státu jako takový.

K písmeni d):

Dle písmene d) se jedná o poskytování služby cloud computingu nejvyšší bezpečnostní úrovně vykonávané poskytovatelem státního cloud computingu podle zákona o informačních systémech veřejné správy. Provozovatel tzv. státního cloudu je osobou, která agreguje data nejdůležitějších systémů státu v rámci infrastruktury, kterou za tímto účelem provozuje, a jeho dopad na fungování veřejné správy tak může mít významný dominový efekt.

K označení přílohy č. 2 příloha č. 2

Příloha obsahuje návrh stanovení nezbytného rozsahu dostupnosti strategicky významných služeb.

Určení nezbytného rozsahu podle § 33 odst. 4 návrhu zákona je zásadní pro fungování povinnosti stanovující zajištění dostupnosti strategicky významné služby. Povinnost zajištění dostupnosti, na kterou navazuje toto ustanovení, se vztahuje pouze na strategicky významné služby, nikoliv na všechny regulované služby podle návrhu zákona.

Zajištění dostupnosti strategicky významné služby je v § 33 návrhu zákona koncipováno následujícím způsobem. Poskytovatel strategicky významné služby je povinen z území České republiky zajišťovat její dostupnost 1) v nezbytném rozsahu, 2) ve stanoveném čase a 3) ve stanovené kvalitě. Body 2) a 3), tedy čas a kvalitu služby, stanoví poskytovatel strategicky významné služby sám. Provede tak zejména s ohledem na charakter a specifika jím poskytované strategicky významné služby, účel, pro nějž je poskytována, a závažnost dopadů narušení jejího řádného poskytování na uživatele strategicky významné služby. O stanovení času a kvality služby je poskytovatel strategicky významné služby povinen vyhotovit záznam. Aby však mohl čas a kvalitu stanovit, musí také znát rozsah toho, v jaké šíři má zajištění dostupnosti dané služby z území České republiky uvažovat. Pokud by i stanovení rozsahu zajištění dostupnosti bylo ponecháno na poskytovateli regulované služby, mohl by teoreticky zvolit tuto množinu nulovou. Z tohoto důvodu a z důvodu zajištění a zvýšení bezpečnosti strategicky významných služeb v rámci České republiky stanovuje návrh zákona, že nezbytný rozsah zajištění dostupnosti strategicky významných služeb stanoví vláda nařízením.

Cílem této přílohy je stanovit části strategicky významných služeb tvořící nezbytný rozsah strategicky významných služeb a způsob jejich vymezení, tedy jsou v ní stanovena kritéria pro určení tohoto nezbytného rozsahu dostupnosti pro všechna aktiva strategicky významných služeb, na která toto ustanovení dopadá. Rozsah byl stanoven tak, aby byla v dostačující míře zajištěna dostupnost strategicky významné služby, přičemž zároveň byl kladen důraz na minimalizaci nadměrné administrativní zátěže povinných subjektů. V odůvodnění přílohy č. 2 je u jednotlivých odvětví nezbytné vycházet z odůvodnění dotčených odvětví v příloze č. 1, neboť na sebe tyto přílohy přímo navazují.

K příloze č. 2 odst. 1

V oblasti veřejná správa vychází jednotlivá kritéria pro určení nezbytného rozsahu dostupnosti strategicky významné služby z úrovně dopadu kritická podle přílohy vyhlášky č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci, která je souběžně s navrhováním tohoto předpisu pro účely nového zákona o kybernetické bezpečnosti transformována do vyhlášky o bezpečnostních úrovních informačních systémů veřejné správy. Návrh kritérií v tomto ohledu reflektuje relevantní požadavky ze zmíněné vyhlášky a z připravované vyhlášky pro určení nezbytného rozsahu dostupnosti strategicky významné služby.

K písmeni a):

Narušení dostupnosti služby může způsobit zranění 2 501 a více osob. Hranice 2 501, resp. 2 500 osob odpovídá průřezovému kritériu nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury stejně jako kritérium ztráty života 250 osob. Navázáním na současnou podobu „dopadového“ kritéria pro identifikaci kritické infrastruktury by mělo být zajištěno, že se jedná o organizaci a službu se skutečně zásadním dopadem na stát.

K písmeni b):

Narušením dostupnosti služby u orgánů veřejné správy, které jsou orgány činnými v trestním řízení, může vytvořit takové podmínky, že může dojít k závažnému a dlouhodobému narušení jejich řádných činností. U trestního řízení je přitom dostupnost dat, která jsou pro jeho vedení potřeba klíčová k včasnému objasnění trestných činů, stejně tak je nezbytné míst přístup k důkazům, které mohou být vedeny v elektronické podobě. Narušení vyšetřování trestné činnosti pak může vést k nedůvěře občanů ve stát jako takový. Narušením dostupnosti určité služby může dojít až ke zpochybnění zákonnosti soudního procesu v trestní věci.

K písmeni c):

Narušením dostupnosti služby může dojít k narušení veřejného pořádku s celostátními dopady. Celostátními dopady se myslí negativní dopad na více místech České republiky. Celostátní dopad není nezbytně spjat se skutečností, že je veřejný pořádek narušen na celém území státu, ale je naplněn i tím, že nepokoje budou soustředěny pouze na jednom místě, ovšem jejich důvod bude celorepublikový (např. demonstranti z různých částí státu budou demonstrovat v Praze).

K písmeni d):

Narušením dostupnosti služby může dojít k takovým dopadům, které mohou ovlivnit diplomatické vztahy České republiky. Může se především jednat o služby podporované specializovanými systémy týkající se výhradně nebo z části mezinárodního působení České republiky, a případný incident způsobující jejich nedostupnost negativně ovlivní postavení České republiky ve světě.

K písmeni e):

Narušení dostupnosti služby může mít vliv na vztahy s jinými organizacemi nebo veřejností a negativní následky mohou být dlouhodobé a s mezinárodním prvkem. Dlouhodobé dopady s mezinárodním prvkem pak představují vyšší intenzitu daného dopadu směrem do zahraničí, tedy možnost poškodit mezinárodní zájmy ČR.

Krátkodobým dopadem jsou myšleny situace, kdy pro službu existuje alternativa. Alternativou se nerozumí opatření zajišťující business kontinuitu, ale ekvivalentní substitut. Dlouhodobý dopad by mohl nastat v situacích, kdy pro službu neexistuje alternativa a není možné ji zajistit jiným způsobem.

Mezinárodní dopady mohou mít například systémy zajišťující nebo podporující vydávání víz, čerpání fondů z EU, mezinárodní obchod a platební styk s ostatními státy, daňové systémy nebo katastr nemovitostí.

K písmeni f):

Narušením dostupnosti služby může dojít k finančním ztrátám, které budou tvořit více než 10 % běžných výdajů ročního rozpočtu, které však musí být nejméně 10 000 000 Kč. Kritérium je stanoveno s ohledem na menší subjekty s menšími rozpočtovými kapitolami kumulativně, tedy pokud u menší organizace daný dopad je vyšší než 10 % jejich běžných výdajů ročního rozpočtu, ale zároveň nedosahuje 10 000 000 Kč, kritérium naplněno není.

K písmeni g):

Narušením dostupnosti služby může dojít k naplnění hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu. Hranice 0,5 % hrubého domácího produktu, která v tomto případě musí být překročena, odpovídá průřezovému kritériu nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění pozdějších předpisů. Navázáním na současnou podobu „dopadového“ kritéria pro identifikaci kritické infrastruktury by mělo být zajištěno, že se jedná o organizaci a službu se skutečně zásadním dopadem na stát.

K písmeni h):

Narušení dostupnosti služby může narušit kvalitu plnění zákonných povinností organizací, což se projeví na kvalitě služeb poskytovaných pro více než 125 000 osob. Hranice 125 000 osob odpovídá průřezovému kritériu pro určení kritické informační infrastruktury podle nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění pozdějších předpisů. Navázáním na současnou podobu „dopadového“ kritéria pro identifikaci kritické infrastruktury by mělo být zajištěno, že se jedná o organizaci a službu se skutečně zásadním dopadem na stát. Přičemž 125 000 osob jako relevantní počet ovlivněných občanů ČR byl na úrovni jmenovaného nařízení vlády dovozen z průměrného počtu obyvatel žijících v jednom kraji.

K příloze č. 2 odst. 2

K písmeni a):

Nezbytný rozsah strategicky významné služby je vymezen výrobou ve výrobně s celkovým instalovaným elektrickým výkonem nejméně 100 MW. Toto vymezení směřuje na nejvýznamnější elektrárny v České republice, u nichž by případný výpadek způsobený kybernetickým bezpečnostním incidentem mohl způsobit významné omezení poskytování dalších nezbytných služeb, jejichž fungování je závislé na dostupnosti elektrické energie. Výklad pojmu „výrobna“ elektřiny a jeho interakce s pojmem „zdroj“ či „provozovna“ je v českém právním prostředí dlouhodobě problematický. Při výkladu tohoto pojmu navrhovatel předpokládá, že jsou jednotlivé výrobny obsaženy v licencích vyhledatelných na stránkách Energetického regulačního úřadu, přičemž více výroben může být součástí jedné provozovny. V oblasti elektroenergetiky nelze pouze na základě výkonu určit nejdůležitější elektrárny, neboť v případě výpadku jedné velké elektrárny nastupuje více menších (například záložních) elektráren, je kritérium stanoveno tak, aby by reflektovalo elektrárny s nejvyšším výkonem, u kterých je pro běžný chod elektroenergetiky žádané, aby jejich dostupnost byla zachována.

K písmeni b):

Přenos elektřiny je nezastupitelná část řetězce poskytování elektřiny. Z tohoto důvodu by narušení provozu přenosové soustavy elektřiny mohlo způsobit masivní *blackout*. Jak je uvedeno výše, služba provozu přenosové soustavy tvoří páteř elektrizační soustavy, zajišťuje propojení elektrizační soustavy se zahraničními soustavami, slouží pro vyvedení výkonu z velkých systémových elektráren a jsou na ni přímo napojené regionální distribuční soustavy.

K písmeni c):

Narušení dostupnosti provozu regionální distribuční soustavy elektřiny by, obdobně jako u předchozí služby, mohlo negativně přímo ovlivnit přenosovou soustavu a následně způsobit výpadek elektrické energie, na jejíž dostupnosti jsou závislé další nezbytné služby.

K písmeni d):

Vymezení míří na dva konkrétní ropovody v České republice, narušení jejichž dostupnosti by mohlo způsobit nedostatek přísunu ropy a v důsledku toho i ropných produktů s negativními následky pro odvětví, která jsou na jejich dostupnosti závislá a zároveň potenciální komplikace v případě krizového stavu. Vymezení ropovodů na tranzitní a vnitrostátní ropovod, včetně jejich jmenovitých průměrů, vychází z aktuálního nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění pozdějších předpisů.

K písmeni e):

V případě narušení dostupnosti provozu produktovodu lze analogicky odkázat na odůvodnění uvedené u ropovodů. Analogicky lze zároveň odkázat na jmenovitý průměr, který rovněž vychází z aktuálního znění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

K písmeni f):

Služba provozu přepravní soustavy zemního plynu je zřizována ve veřejném zájmu a slouží k přepravě plynu mimo jiné i se zahraničními plynárenskými soustavami. Narušením dostupnosti této služby by mohlo dojít k ovlivnění přepravy plynu a tím následně k ovlivnění důležitých společenských činností, např. distribuce plynu koncovým odběratelům, mezi nimiž jsou nejen fyzické, ale i právnické osoby.

K písmeni g):

Narušení dostupnosti služby provozu distribuční soustavy plynu v rámci vysokotlakého a středotlakého plynu by, s ohledem na síťový charakter odvětví plynárenství, mohlo mít za následek ovlivnění dalších navazujících služeb. Vymezení na vysokotlaký a středotlaký plynovod vychází z aktuálního znění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění pozdějších předpisů.

K písmeni h):

Narušení dostupnosti služeb poskytovaných Elektroenergetickým datovým centrem by mohlo mít za následek narušení provozu přenosové soustavy elektřiny, tak jak je uvedeno výše v bodech b) a c).

K písmeni i):

Narušení dostupnosti služeb poskytovaných nominovaným organizátorem trhu s elektřinou by mohlo mít za následek přinejmenším podstatné ztížení organizace trhu s elektřinou, včetně vyhodnocování odchylek za celé území České republiky, jak bylo uvedeno výše, tedy přímý závažný dopad na provoz soustavy elektřiny na přenosové a distribuční úrovni.

K příloze č. 2 odst. 3

V případě vymezení nezbytného rozsahu strategicky významných služeb v odvětví doprava lze v plném rozsahu analogicky odkázat na odůvodnění k stanovení strategicky významných služeb v první příloze tohoto nařízení, neboť je nezbytný rozsah vymezen celou strategicky významnou službou.

K příloze č. 2 odst. 4

K písmeni a):

Jedná se o poskytování veřejně dostupné služby elektronických komunikací podle § 2 odst. 3 písm. a) bodů 1 a 2 zákona o elektronických komunikacích. Jde o službu přístupu k internetu a o interpersonální komunikační službu.

K písmeni b):

Jedná se o zajišťování veřejné komunikační sítě elektronických komunikací. Tato síť je definovaná v § 2 odst. 2 písm. d) zákona o elektronických komunikacích jako síť elektronických komunikací, která slouží zcela nebo převážně k poskytování veřejně dostupných služeb elektronických komunikací a která podporuje přenos informací mezi koncovými body sítě, nebo síť elektronických komunikací, jejímž prostřednictvím je poskytovaná služba šíření rozhlasového a televizního vysílání.

K písmeni c)

Jedná se o správu a provoz registru internetových domén nejvyšší úrovně. Tato služba obsahuje správu domén nejvyšší úrovně, včetně registrace doménových jmen v rámci domén nejvyšší úrovně a technického provozu domén nejvyšší úrovně, včetně provozu jejích jmenných serverů, vedení jejích databází a distribuce souborů zón domén nejvyšší úrovně mezi jmennými servery, bez ohledu na to, zda kteroukoli z těchto operací provádí subjekt sám nebo je zajišťována externě, avšak s výjimkou situací, kdy jsou jména domén nejvyšší úrovně používána registrem pouze pro vlastní potřebu.

K písmeni d)

Jedná se o poskytování služby cloud computingu v nejvyšší bezpečnostní úrovni poskytovatelem státního cloud computingu. Státní poskytovatel cloud computingu je vymezen v § 6i odst. 1 písm. a) zákona č. 365/2000 Sb., o informačních systémech veřejné správy. Kybernetické bezpečnostní incidenty zasahující informační systémy veřejné správy, jejichž provoz je zajišťován prostřednictvím státního cloud computingu, mohou mít kritické dopady na fungování státu.