Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

DŮVODOVÁ ZPRÁVA

Zákon o kybernetické bezpečnosti – Bezpečnost dodavatelského řetězce

# Obsah

# 1 Obecná část důvodové zprávy

## 1.1 Zhodnocení platného právního stavu

### 1.1.1 Legislativa v oblasti kybernetické bezpečnosti

V českém právním řádu je v současnosti oblast definovaného problému upravena především zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „ZKB“) a jeho prováděcí vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „VKB“).

ZKB v tomto ohledu zejména ukládá v § 5 svým povinným osobám zavádět technická a organizační bezpečnostní opatření, tedy konkrétní kroky k seznámení se s aktivy svých systémů, řízení rizik s nimi spojenými, zavedení minimálních opatření k technickému zabezpečení a jiné. Ve vztahu k dodavatelskému řetězci ukládá stávající právní úprava v oblasti kybernetické bezpečnosti povinným osobám v regulované infrastruktuře toliko znát své významné dodavatele[1], informovat je o tomto jejich postavení, hodnotit rizika s významnými dodavateli spojená a smluvně své dodavatele zavazovat k přijetí některých kybernetických bezpečnostních opatření.[2]

Dalším regulatorním nástrojem v oblasti definovaného problému je institut varování upravený § 12 ZKB (dále jen „varování podle ZKB“) a další opatření podle § 11 ZKB. Varování podle ZKB slouží mimo jiné k upozornění veřejnosti na hrozbu v oblasti kybernetické bezpečnosti, o které se NÚKIB dozvěděl z vlastní činnosti nebo od jiných orgánů či osob. Nejen pro výkon této kompetence je NÚKIB umožněno provádět analýzu a monitoring kybernetických hrozeb a rizik.[3] Vydané varování podle ZKB pak mají povinné osoby podle ZKB v některých případech povinnost zohlednit v rámci řízení rizik spojených se svými systémy.

Právní řád tedy sice umožňuje zjišťovat a vyhodnocovat informace o hrozbách v oblasti kybernetické bezpečnosti, NÚKIB ani ostatním státním orgánům, působícím v oblasti bezpečnosti, ale dává pouze velmi limitovanou možnost seznamovat se s informacemi o dodavatelích v regulované infrastruktuře nebo o dodavatelích, kteří se o zakázky do regulované infrastruktury uchází, způsobem, který by umožňoval odhalit a vyhodnotit hrozbu spojenou s dodavateli ještě před její realizací.

V případě, kdy se ale NÚKIB přesto podaří potřebné informace o současném či budoucím riziku spojenému s dodavatelským řetězcem získat a vyhodnotit, neumožňuje mu zákonná úprava na tato zjištění vhodně reagovat. Možnosti, které NÚKIB v takové situaci má, jsou pouze informovat o hrozbě formou varování podle ZKB nebo vydat reaktivní opatření podle § 13 ZKB – to však cílí už na určitý kybernetický bezpečnostní incident, a tedy na situaci bezprostředního narušení bezpečnosti regulované infrastruktury v konkrétní podobě. Minimalizovat zjištěnou strategickou hrozbu, spojenou s konkrétním dodavatelem



[1] Významným dodavatelem je dle § 2 písm. n) VKB provozovatel informačního nebo komunikačního systému dle ZKB a každý, kdo s povinnou osobou vstupuje do právního vztahu, který je významný z hlediska bezpečnosti systému.
[2] § 8 VKB.
[3] § 22 písm. u) ZKB.

prostřednictvím omezení jeho přítomnosti ve strategicky významné infrastruktuře, se státním orgánům nenabízí.

Možnost omezovat přítomnost rizikových dodavatelů ve strategicky významné infrastruktuře je tak primárně ponechána na povinných osobách podle ZKB. S ohledem na rozdělení pravomocí a povinností mezi státem a soukromým sektorem, jakož i mezi jednotlivými státními orgány, ale tyto povinné osoby nejsou motivovány analyzovat a omezovat hrozby pro větší množinu systémů strategicky významné infrastruktury, než za jaké jsou odpovědné. Nicméně i pokud by se povinná osoba chystala takovou hrozbu ve svém řízení rizik podle VKB reflektovat, nemá zpravidla oprávnění, nástroje ani kapacitu shromažďovat a vyhodnocovat informace k tomu potřebné.

Tzv. strategické hrozby spojené s dodavateli, tedy například možnost nepřezkoumatelných zásahů cizích států do aktivit dodavatele či neformální působení na dodavatele, směřující k poškození jiného státu (viz část 1.3 Vysvětlení nezbytnosti navrhované právní úpravy), vyžadují pro svoji sofistikovanost a komplexitu seznámení se s velkým množstvím informací, často neveřejného či dokonce zpravodajského charakteru. K těmto informacím má z podstaty věci povětšinou přístup pouze stát, resp. jeho bezpečnostní aparát, a neoprávněná dispozice s takovými informacemi, byť subjektem jednajícím v dobré víře (jako například zmiňovaná povinná osoba, mající vůli strategickou hrozbu reflektovat), je právními předpisy přísně sankcionována.[4]

Správci regulované infrastruktury tak stojí před opačným problémem než NÚKIB – mají přehled o užívaných dodavatelích (tzn. informace, které NÚKIB schází), mají možnost omezit v infrastruktuře přítomnost vysoce rizikových dodavatelů, nemají ale možnost získat a vyhodnotit veškeré potřebné informace pro to, aby mohli hrozbu spojenou s dodavatelem účinně minimalizovat. Nezřídka se navíc stává, že identifikovaná hrozba, před níž NÚKIB vydal varování podle ZKB, není v analýze rizik povinných osob podle ZKB dostatečně, či dokonce jakkoliv, reflektována. Podle výstupů z kontrol a auditů povinných osob prováděných podle ZKB je úskalím tohoto přístupu nejčastěji samotná maturita povinných osob v oblasti řízení rizik, kdy povinná osoba nesplňuje samotnou procesní prerekvizitu vykonávání analýzy rizik. V případě, kdy je varování v analýze rizik náležitě zohledněno, často nejsou řízeny následné procesy a alokovány zdroje pro ošetření daného rizika doložitelné formou např. plánu zvládání rizik.

Pro řešení definovaného problému nepostačuje ani současné zmocnění NÚKIB k zajišťování metodické podpory v oblasti kybernetické bezpečnosti podle § 22 písm. j) ZKB. V rámci této pravomoci vydal ve snaze adresovat definovaný problém NÚKIB v únoru 2022 Doporučení pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí v České republice (dále jen „5G Doporučení“).

5G Doporučení představuje podpůrný materiál pro výběr dodavatelů subjektů budujících a provozujících sítě a poskytujících služby elektronických komunikací, které jsou kritickou informační infrastrukturou. Cílem 5G Doporučení je nabídnout operátorům, potažmo celému odvětví elektronických komunikací, pohled NÚKIB, Ministerstva průmyslu a obchodu (dále jen „MPO“), Ministerstva zahraničních věcí (dále jen „MZV“), Bezpečnostní informační



[4] Např. zajištění si přístupu k utajované informaci bez současného splnění zákonných předpokladů je možné potrestat pokutou až do 1 000 000 Kč podle § 148 odst. 4 písm. d) a § 155a odst. 2 zák. č 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

služby (dále jen „BIS“), Úřadu pro zahraniční styky a informace (dále jen „ÚZSI“) a Vojenského zpravodajství (dále jen „VZ“) na základní východiska posuzování důvěryhodnosti dodavatelů technologií do 5G sítí a navrhnout kritéria, která mohou přispět k výběru důvěryhodných dodavatelů.

Přestože však byla vodítka tohoto druhu ze strany správců této infrastruktury dlouhodobě požadována, k reflexi 5G Doporučení jeho adresáty po jeho vydání prakticky nedošlo; mnozí správci kritické informační infrastruktury v sektoru elektronických komunikací nadále uzavírají kontrakty na dodávky technologií do bezpečnostně citlivých částí své infrastruktury s dodavateli, kteří po vyhodnocení kritérií 5G Doporučení na první pohled nevychází jako důvěryhodní.[5]

Na základě této zkušenosti se jeví neregulatorní působení na zohledňování strategické roviny důvěryhodnosti dodavatele v sektoru elektronických komunikací jako nedostatečné. Lze se domnívat, že ani v jiných sektorech hospodářství nebudou podnikatelské subjekty ochotny upřednostňovat strategickou důvěryhodnost dodavatele před bezprostředními ekonomickými aspekty dodávek, jako je například nabídková cena, nebudou-li existovat závazná regulatorní pravidla.

Problematika posuzování subjektů na základě mj. také vyhodnocování kritérií netechnického charakteru je v současnosti již zavedena v právním řádu pro vymezené skupiny subjektů. Jedná se zejména o zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů (dále jen „zákon o IS veřejné správy“), který v § 6m odst. 1 písm. c) stanovuje mezi požadavky na poskytovatele cloud computingu poskytujícího cloud computing orgánu veřejné správy, aby se jednalo o osobu nebo jiné právní uspořádání, která je způsobilá pro poskytnutí cloud computingu orgánu veřejné správy z hlediska veřejného pořádku, bezpečnosti a dodržování práv třetích osob. Poskytovatel cloud computingu musí zákonem definované požadavky splnit, jestliže má být zapsán v katalogu cloud computingu pro orgány veřejné správy (dále jen „katalog cloud computingu“). Pouze poskytovatelé zapsaní v katalogu cloud computingu mohou poskytovat služby cloud computingu orgánům veřejné správy.

### 1.1.2 Legislativa v ostatních oblastech

Kromě nedostatečného zmocnění NÚKIB k řešení definovaného problému nemají ani orgány a osoby v postavení zadavatele podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, (dále jen „ZZVZ“), reálnou možnost zohlednit aspekt strategické bezpečnostní rizikovosti dodavatele v zadávacích podmínkách a při následném hodnocení nabídek. Stanovení a následné posuzování netechnických aspektů dodavatele vyžadují specifickou expertízu a informace, kterými zadavatelé zpravidla nedisponují. V konečném důsledku tak zpravidla dochází k výběru dodavatele veřejné zakázky na základě nabídkové ceny, případně jiných, snadno vyhodnotitelných kritérií.

Další regulací je zákon č. 34/2021 Sb., o prověřování zahraničních investic a o změně souvisejících zákonů (dále jen „zákon o prověřování zahraničních investic“). Podle § 1 písm. a)

[5] T-MOBILE CZECH REPUBLIC, A.S. T-Mobile pokračuje s rozšiřováním 5G sítí – spustil dalších 270 vysílačů. Dostupné z: https://www.t-press.cz/cs/tiskove-materialy/tiskove-zpravy-t-mobile/t-mobile-pokracuje-s-rozsirovanim-5g-siti-spustil-dalsich-270-vysilacu.html; SEDLÁK, Jan. Varování navzdory. Vodafone a T-Mobile budou dál v 5G sítích nasazovat zařízení od Huawei. Dostupné z: https://www.e15.cz/byznys/technologie-a-media/varovani-navzdory-vodafone-a-t-mobile-budou-dal-v-5g-sitich-nasazovat-zarizeni-od-huawei-1389914

zákona o prověřování zahraničních investic (dále jen „zákon o prověřování zahraničních investic“) je předmětem této právní úpravy mj. stanovení pravidel *„prověřování některých zahraničních investic z důvodu ochrany bezpečnosti České republiky a vnitřního či veřejného pořádku“*. Zahraniční investoři do cílových osob definovaných § 7 zákona o prověřování zahraničních investic tak budou podrobeni prověření s cílem získat povolení zahraniční investice, bez nějž tuto investici nebudou moci uskutečnit.

K účelu udržení nebo obnovení mezinárodního míru a bezpečnosti, boje proti terorismu, dodržování mezinárodního práva, ochraně lidských práv a svobod a podpoře demokracie a právního státu směřuje zákon č. 69/2006 Sb., o provádění mezinárodních sankcí (dále jen „zákon o mezinárodních sankcích“). Na základě tohoto zákona je možné nařízením či rozhodnutím vlády při splnění jedné z podmínek vymezených v § 2 uplatnit omezení či zákazy v oblastech stanovených v § 4 odst. 2 zákona o mezinárodních sankcích. K omezení či zákazu využívání ICT produktů na území ČR může dojít na základě:

a) Ustanovení § 5 odstavce 1 písm. a) zákona o mezinárodních sankcích, kdy může dojít k omezení nebo zákazu dovozu anebo koupě zboží, na které se vztahují mezinárodní sankce, jeho prodeje nebo jakéhokoli jiného nakládání s ním.

b) Ustanovení § 7 zákona o mezinárodních sankcích, kdy mohou sankce také v oblasti technické infrastruktury spočívat v omezení či zákazu dodávek energie nebo dodávek surovin, strojů nebo zařízení potřebných k její výrobě subjektu, osobě či celému území, na které se mezinárodní sankce vztahují.

Stávající právní úprava umožňuje omezit či zakázat produkty či služby poskytované určitými osobami, a to z důvodu možnosti existence strategického rizika spojeného s těmito osobami majícího negativní vliv na zajištění ochrany bezpečnosti, veřejného pořádku či bezpečnosti a dodržování práv třetích osob v České republice. Poskytovatelé cloud computingu či zahraniční investoři jsou na základě platné právní úpravy v současnosti regulováni a prověřování mj. i na základě hodnocení tzv. netechnických kritérií. Obdobná regulace je v současnosti potřebná taktéž pro dodavatele ICT do strategicky významné infrastruktury ČR, a to z důvodu nedostatečnosti existující právní úpravy pro řešení problému definovaného v části 1.2. Zákon o mezinárodních sankcích umožňuje dokonce omezení či zákaz dodávek zboží, popř. v oblasti dodávek energií taktéž veškerá zařízení potřebná k její výrobě, a to nejen zboží určitého subjektu či osoby, nicméně celému území, na které se sankce vztahují. Ačkoliv tento sankční režim umožňuje regulovat dodávky mj. také do strategické infrastruktury, z povahy věci jsou omezení spojená s udělováním sankcí především reaktivního charakteru na vývoj na mezinárodní úrovni. Jejich využívání pro potřeby mitigace rizika úmyslného narušení kybernetické bezpečnosti strategicky významné infrastruktury či vzniku strategické závislosti na rizikovém dodavateli tedy není dostačující. Plánovaná regulace dodavatelů nicméně počítá s využitím informací a poznatků těchto existujících mechanismů pro proces hodnocení důvěryhodnosti dodavatelů do strategické infrastruktury státu, a to pro zvýšení efektivnosti tohoto procesu.

V současnosti je na úrovni Evropské unie plánováno zavedení evropského systému certifikace kybernetické bezpečnosti[6], např. certifikační schéma pro 5G sítě. Evropský certifikační systém zahrnuje pouze technickou certifikaci produktů, služeb a procesů a nevyhodnocuje rovinu strategické důvěryhodnosti dodavatele. Prověřování strategické důvěryhodnosti dodavatelů však především nelze aplikovat na úrovni Evropské unie z důvodu

[6] Tento systém je zaváděn na základě nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“).

vyloučení problematiky vnitřní bezpečnosti z úpravy primárního práva Evropské unie[7]. Evropský systém certifikace kybernetické bezpečnosti se tedy v současnosti jeví pouze jako vhodný doplněk k navrhovanému řešení, avšak nemůže a ani nemá ambice jej nahradit.

## 1.2 Odůvodnění hlavních principů navrhované právní úpravy

Mechanismus posuzování dodavatelů vychází z principů a hodnot ZKB a respektuje v maximální možné míře stávající performativní povahu pravidel řízení dodavatelů a jiných ustanovení VKB. Zaměřuje prověřování ze strany státu toliko na ty strategické aspekty důvěryhodnosti dodavatelů, jež správci této strategicky významné infrastruktury z podstaty své činnosti (a vzhledem k monopolizaci určitých pravomocí státem) nemohou provádět. Jedná se zejména o identifikaci a omezení známých případů či existujícího rizika ingerence státních aktérů do produktů, služeb či procesů prostřednictvím dodavatelů či poddodavatelů, s cílem narušení bezpečnosti s ohledem na dostupnost, důvěrnost a integritu strategicky významné informační a komunikační infrastruktury státu. Informace o takových případech či rizicích ingerence vychází v mnohých případech z neveřejných zdrojů a vyžaduji kontextuální analýzu citlivých či jinak režimových informací, kterou je v požadované míře vybaven, schopen a oprávněn provádět pouze stát.

Mechanismus posuzování dodavatelů přitom není pouze službou státu pro stát a jím chráněné informační a komunikační systémy a sítě. Díky již zmíněným unikátním informačním zdrojům a z toho plynoucí komplexitě analýzy přítomnosti hrozeb a z nich plynoucích rizik si mechanismus klade za cíl přinést zvýšenou úroveň důvěry a bezpečnosti také pro samotnou strategicky významnou infrastrukturu. Skutečnost, že mechanismus identifikuje přítomnost strategického rizika důvěryhodnosti dodavatele, významně omezí riziko narušení předmětné dodávky či jí dodávané technologie z neobchodních důvodů, jejichž identifikace a posouzení nemusí být v možnostech a schopnostech správce infrastruktury jakožto odběratele. Prověření a omezení strategických rizik důvěryhodnosti dodavatele je tedy rovněž službou státu pro povinné osoby mechanismu.

Problematika komplexního zajištění bezpečnosti nicméně zůstává věcí správce systému či sítě. V souladu se stávajícím nastavením systému zajišťování kybernetické bezpečnosti v České republice je klíčovým prvkem systém řízení rizik podle VKB. Ačkoliv navrhovaný mechanismus přichází s novým vstupem státu do tohoto systému, komplexní analýzu hrozeb a rizik v oblasti kybernetické bezpečnosti ponechává na odpovědnosti povinných osob mechanismu.

Výstup z mechanismu posuzování dodavatelů má sloužit toliko jako jeden ze vstupů do procesu řízení rizik a neměl by pro povinné osoby mechanismu představovat významnou administrativní či jinou zátěž. Navrhovaný mechanismus prověřování je vytvářen s cílem minimalizovat ekonomické náklady pro soukromé subjekty i pro stát na úroveň nezbytnou pro zajištění účelu mechanismu. Účelem je tedy omezení závislosti povinných osob mechanismu na dodavatelích představujících strategickou hrozbu v oblasti informačních a komunikačních technologiích a přispět tak k zajištění dlouhodobě udržitelného zabezpečení a odolnosti, jež je nezbytná pro naplňování základních funkcí státu.

Klíčovým principem mechanismu je i jeho efektivita vycházející z přesvědčení, že rizika v oblasti kybernetické bezpečnosti nelze zcela eliminovat, ale pouze omezovat.



[7] Viz např. čl. 72 Smlouvy o fungování EU.

Mechanismus posuzování dodavatelů tedy bude ve všech částech svého procesu poměřovat náklady a přínosy dané části i mechanismu jako celku. S ohledem na zachování proporcionality zajištění národní bezpečnosti a ochrany svobody podnikání, jakož i s ohledem na minimalizaci státního donucení a ekonomických dopadů navrhovaného řešení na veřejný i soukromý sektor, je nezbytné omezit prověřování pouze na vymezenou strategicky významnou infrastrukturu, a to pouze na její část, která je kritická pro bezpečnost daného prvku vymezené infrastruktury (kritickou část systému). Prověřováni budou také pouze dodavatelé dodávek, které jsou relevantní z hlediska bezpečnosti daného prvku (bezpečnostně významné dodávky).

Se shora uvedeným poměřování nákladů a přínosů souvisí i lhůty v opatřeních vydaných při zjištění rizikovosti konkrétního dodavatele. Byť pro dosažení účelu mechanismu se jeví nejefektivnější ihned omezit plnění takového dodavatele, navržená úprava umožňuje reflektovat i náklady s tím spojené a respektovat životní cyklus ICT produktů, tak aby nebylo disproporčně zasaženo do práva na podnikání osob povinných z mechanismu.

Navrhovaná úprava zohledňuje i skutečnost, že rizikovost dodavatele nelze stanovit binárně, naopak je třeba ji vnímat jako škálu. Z tohoto důvodu ne každý rizikový dodavatel musí být nutně vyřazen z možnosti poskytovat bezpečnostně významné dodávky. U méně rizikových dodavatelů postačí omezení daného rizikového dodavatele nepřímo prostřednictvím vydání varování dle ZKB, jehož cílem je upozornit na hrozbu spojenou s dodavatelem tak, aby ji osoby povinné z mechanismu reflektovaly ve své analýze rizik.

## 1.3 Vysvětlení nezbytnosti navrhované právní úpravy v jejím celku

Návrh zákona zmocní NÚKIB a další organizační složky státu k identifikaci a vyhodnocení hrozeb plynoucí z dodavatelských řetězců pro národní bezpečnost nebo veřejný pořádek. Zda jsou tyto hodnoty v ohrožení bude vyhodnoceno na základě transparentních kritérií stanovených v prováděcím právním předpise – vyhlášce o kritériích rizikovosti dodavatele, k prověřování kritérií bezpečnostní spolehlivosti dodavatelů povinných osob mechanismu, a to skrze vyhodnocování kritérií a případné omezování bezpečnostních rizik spojených s těmito dodavateli. Mechanismus posuzování dodavatelů umožní NÚKIB na základě zákonného zmocnění omezit či vyloučit z vymezených dodávek povinných osob mechanismu takové dodavatele, kteří budou vyhodnoceni jako rizikoví, v důsledku čehož dojde ke snížení dopadu negativních zahraničních vlivů na zajištění základních funkcí státu prostřednictvím dodávek technologií.

Účelem navrhovaného řešení je omezení závislosti strategicky významné infrastruktury státu na dodavatelích, kteří představují strategickou hrozbu v oblasti kybernetické bezpečnosti pro své politické či právní prostředí, ve kterém působí, nebo pro své dosavadní jednání proti zájmům ČR. Prověřování bude založeno na hodnocení naplnění netechnických kritérií konkrétním dodavatelem (resp. dodavatelským řetězcem) a zhodnocení dalších informací (vč. zpravodajských) o možných strategických hrozbách a rizicích spojených s konkrétním dodavatelem. Jedná se tedy o kritéria, která není schopen adekvátně vyhodnotit správce strategicky významné infrastruktury.

Bezpečnost a odolnost organizačních složek státu a dalších orgánů a osob, jež poskytují služby stěžejní pro chod státu, jsou předpoklady pro zajištění bezpečnosti ČR. Podle Bezpečnostní strategie ČR existuje řada hrozeb, kterým ČR čelí, a to vč. kybernetických útoků, ohrožení funkčnosti kritické infrastruktury či přerušení dodávek strategických surovin nebo energie. Všechny zmíněné hrozby lze realizovat také v kyberprostoru. Útoky státních aktérů na systémy kritické pro chod státu se stávají běžnou realitou ovlivňující život a fungování

mnoha obyvatel a institucí. Bezpečnost strategicky významné infrastruktury pro ČR je ohrožena nejen kybernetickými útoky, ale i prostřednictvím dodavatelů a dodavatelských řetězců, spadajících do sféry vlivu zejména státních aktérů, jejichž zájmy a mezinárodní působení jsou v konfliktu se zájmy ČR. Dodavatelé se tak mohou stát prostředkem k prosazování politických cílů.

Jelikož ČR v rámci plnění svých základních funkcí povětšinou spoléhá na infrastrukturu vlastněnou, dodávanou či spravovanou třetími osobami, vzniká státu na těchto dodavatelích závislost (dále také „strategická závislost“). Pokud vznikne závislost na rizikovém dodavateli, plynou z toho pro stát významná rizika. Možné dopady takových rizik ukázal např. vývoj související s vojenskou invazí Ruské federace na Ukrajinu, která byla zahájena 24. února 2022. Válka na Ukrajině měla a má kromě nezměrných humanitárních, bezpečnostních a geopolitických dopadů také značné dopady na evropskou ekonomiku, což se nejhmatatelněji projevuje v energetice. Razantní zvýšení cen energií, zejména plynu,[8] bylo způsobeno právě onou strategickou závislostí, jež si ČR na dovozu plynu z Ruska vytvořila.[9]

Obdobná situace strategické závislosti státu na dodavatelích může nastat, a v mnoha sektorech již nastává, v oblasti informačních a komunikačních technologií (dále jen „ICT“). V ICT je kromě již identifikovaných problémů strategické závislosti potřeba vyhodnocovat také rizika související s narušením důvěrnosti, integrity i dostupnosti dat a informací přenášených dodávanými technologiemi ze strany dodavatele.

Strategicky významná infrastruktura je přitom na ICT značně závislá. Společně se zvyšující se mírou přenosu odpovědnosti za zajištění důvěrnosti, integrity a dostupnosti informací přenášených informačními systémy (dále jen „IS“) na dodavatele ICT a zvyšující se mírou složitosti jednotlivých prvků technologických systémů závislost strategicky významné infrastruktury na těchto dodavatelích dále narůstá.

Dodavatelé mají v ICT infrastruktuře výsadní postavení. Hardwarová a softwarová řešení ICT jsou již natolik komplexní a v infrastrukturách povinných osobo mechanismu tak četně zastoupená, že je nelze technicky komplexně včas a efektivně prověřovat.

I s ohledem na časté aktualizace je technické testování ICT produktů ve velkém měřítku vysoce neefektivní. Problematika bezpečnostních záplat taktéž ztěžuje správcům infrastruktury technicky ověřit implementovaná softwarová řešení od svých dodavatelů, jelikož v případě odhalení (i zcela neúmyslných) slabin je potřeba co nejrychleji vydat softwarové aktualizace, než jich využijí útočníci (tzv. zranitelnosti nultého dne[10]). Takové aktualizace proto nemohou být podrobeny důkladné analýze, a nelze tak vyloučit riziko, že budou obsahovat například zadní vrátka[11] (tzv. backdoors), nebo jiný škodlivý kód. Klíčovým faktorem zabezpečení ICT je proto důvěra v dodavatele, že nezneužije své výsadní postavení ve prospěch svůj, státu, který má na dodavatele vliv, či jiného aktéra.



[8] ČESKÁ NÁRODNÍ BANKA. Vývoj na evropském trhu se zemním plynem. Dostupné z: https://www.cnb.cz/cs/o_cnb/cnblog/Vyvoj-na-evropskem-trhu-se-zemnim-plynem/

[9] Eurostat uvádí 75–100% závislost ČR na ruském plynu pro první pololetí roku 2021. (Viz EUROSTAT. File:Share of Russia in national extra EU imports of each Member State, first semester 2021.png. Dostupné z: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Share_of_Russia_in_national_extra_EU_imports_of_each_Member_State,_first_semester_2021.png)

[10] Dle Zprávy o stavu kybernetické bezpečnosti za rok 2021 se jedná o typ zranitelnosti, který bývá často využíván např. státem podporovanými skupinami.

[11] V informatice se jedná o název metody umožňující obcházení autentizačních opatření a neoprávněné užívání počítačového systému. Zadní vrátka mohou být zabudována jak do softwarových, tak i hardwarových komponent.

Dodavatelé ze zemí majících např. nestandardní legislativní prostředí, umožňující ingerenci státních aktérů do produktů, služeb či procesů dodavatelů, a jejichž zájmy jsou v konfliktu se zájmy ČR a jejích spojenců, lze považovat za rizikové. Ačkoliv výrobci či dodavatelé ICT produktů a služeb (dále jen „dodavatelé ICT“) mají s ohledem na generování zisku zájem o prodej kvalitních a bezpečných produktů, ne vždy se musí jednat o jejich jediný zájem.

Dodavatelé ICT mají sídla v různých zemích a podléhají rozličným právním řádům, mocenským strukturám a jiným neobchodním vlivům. Zvýšené riziko představují primárně dodavatelé ICT z autoritářských států, které mají silný vliv na své domácí společnosti a neváhají jej zneužít pro prosazování svých geopolitických cílů, jež mohou být v rozporu se zájmy ČR či jejích spojenců. Dodavatel ICT může být natolik ovlivněný a propojený se státním a politickým aparátem své domovské země, že může nezřídka činit i ekonomicky kontraproduktivní rozhodnutí v souladu se zájmy režimu, který mu potenciální reputační škodu může kompenzovat, případně jej za jednání v rozporu se svými zájmy potrestat. Navíc, vzhledem k obtížnému odhalení, a ještě obtížnější atribuci (přičitatelnosti) kybernetických útoků,[12] mohou tyto aktivity představovat pro výrobce přijatelné riziko, které mu zajistí výhodné postavení v domovském státě a výrazněji neohrozí jeho zisk.

V řadě států mohou být společnosti také nuceny ke spolupráci se zpravodajskými službami státu na základě legislativy, jež na ně dopadá. V Čínské lidové republice (dále také „ČLR“) ukládá legislativa povinnost jednotlivcům i společnostem spolupracovat s čínskými státními orgány. Jedná se např. o mechanismus, který je začleněný do zákona o společnostech z roku 2013, jež ukládá všem společnostem povinnost ustanovit uvnitř svých struktur stranickou organizaci Komunistické strany ČLR (dále jen „KS ČLR“), pokud ve společnosti pracují nejméně tři členové Strany. V praxi to znamená přímý dosah této strany na dění v jakékoliv významné společnosti. KS ČLR vykonává skrze stranické organizace přímou kontrolu nad společnostmi a zajišťuje, že beze zbytku plní, co se od nich očekává, včetně požadavků v oblasti státní bezpečnosti[13].

Taktéž Ruská federace (dále jen „RF“) přijala během poslední dekády několik zákonů s významným dopadem v oblasti kybernetické a informační bezpečnosti, které zásadním způsobem zasahují do fungování soukromých společností.[14] Zákon o Federální službě bezpečnosti (FSB) RF (40-FZ) poskytuje státu právní nástroje k donucení ke spolupráci formálně soukromé entity, a to včetně globálně působících výrobců ICT.[15] § 15 tohoto zákona umožňuje FSB instalovat dodatečný software a hardware do ICT produktů ruských společností[16], stejně tak jako dosazovat důstojníky FSB do struktur soukromých firem.[17] Přestože i v ČR, stejně tak jako v dalších zemích Evropské unie a spojeneckých zemích ČR,



[12] Atribuce dle vyjádření NÚKIB představuje proces, během něhož dochází k určení pravého zdroje útoku a samotného útočníka (Viz NÚKIB. Bezpečnější zdravotnictví i řešení rizikových dodavatelů - Vláda schválila Akční plán ke strategii kybernetické bezpečnosti. Dostupné z: https://www.nukib.cz/cs/infoservis/aktuality/1735-bezpecnejsi-zdravotnictvi-i-reseni-rizikovych-dodavatelu-vlada-schvalila-akcni-plan-ke-strategii-kyberneticke-bezpecnosti/)

[13] Law Bridge. 28.12.2013. Dostupné z: http://www.lawbridge.org/zhong-hua-ren-min-gong-he-guo-gong-si-fa-2013-nian-xiu-ding/

[14] Human Rights Watch. 2020. Russia: Growing Internet Isolation, Control, Censorship. Dostupné z: https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship

[15] Peter B. Maggs. 2018. Report of Peter B. Maggs. Dostupné z: https://assets.documentcloud.org/documents/4386053/Report-of-Peter-B-Maggs-Russian-Surveillance-Law.pdf

[16] Федеральный закон от 03.04.1995 N 40-ФЗ (ред. от 02.12.2019) "О федеральной службе безопасности" (Federal Law on the Federal Security Service of the Russian Federation); Venice Commission. 2012. Federal Law on the Federal Security Service of the Russian Federation.

[17] FSB Dossier. 2020. Аппарат прикомандированных сотрудников. Dostupné z: https://fsb.dossier.center/prikom/

existuje legislativa regulující vztah státu a soukromých společností pro potřeby zajišťování obrany státu a národní bezpečnosti[18], pravomoci státu jsou ve srovnání s těmi čínskými či ruskými nepoměrně nižší. Případné zásahy státu musejí být řádně odůvodněny, přičemž podléhají soudnímu přezkumu a usilují o co nejmenší rozsah získávaných informací.

Dodavateli (či s jejich asistencí) úmyslně způsobené narušení kybernetické bezpečnosti strategicky významné infrastruktury, a to zejména nejzávažnější případy jako je narušení dostupnosti systému ve velkém rozsahu, představuje podstatný problém pro významné ekonomické a jiné zájmy ČR a její bezpečnost, jelikož mohou výrazně narušit fungování státu, ekonomiky, společnosti a v krajním případě ohrozit zdraví a životy obyvatel.

Identifikovaná rizika současného stavu spojená s nečinností jsou:

a. Vytvoření strategické hrozby státu v podobě závislosti na rizikových dodavatelích. V případě realizace hrozby by došlo k ohrožení strategicky významné infrastruktury, jejíž narušení by mohlo mít dopad na fungování celé ČR.

b. Existence nepředvídatelného prostředí a nejistota povinných osob mechanismu, kteří ačkoliv mají přehled z ostatních států o rizikovosti vybraných dodavatelů, mohou při výběru i nadále upřednostňovat jiné, zejména ekonomické, aspekty nabízeného řešení, což je podněcováno zejména obavou z nekonkurenceschopnosti na trhu a taktéž podmínkami, které jim jsou v ČR nabízeny.

c. Reputační dopad ČR, kdy absence regulatorního rámce dodavatelů do strategicky významné infrastruktury bude řadit ČR mezi státy, jež v této oblasti zaostávají. Proto je důležité zachovat dobré jméno ČR a budovat strategicky významnou infrastrukturu na bezpečném základu s adekvátně nastavenou regulací. Absence regulace bezpečnosti dodavatelského řetězce by tak v budoucnu mohla vést ke zhoršení pozice podnikatelských subjektů působících v ČR, které by nemohly nabídnout stejnou míru bezpečnosti svého produktu či služby jako subjekty ve státech, které obdobnou regulaci přijaly. Nepřijetí předmětné právní úpravy by tedy mohlo vyvolat nucené odmítání dodávek českých společností zahraničními odběrateli kvůli bezpečnostním a strategickým hrozbám plynoucím z dodávek subdodavatelů. České společnosti by se tím de facto staly nespolehlivými dodavateli pro zahraniční obchodní partnery, kteří by byli v takovém případě nucení svým národním legislativním systémem upřednostnit dodavatele ze zemí, které rizika dodavatelského řetězce legislativně ošetřují.

d. Vznik strategické hrozby v podobě závislosti na rizikových dodavatelích či přítomnosti technologií vysoce rizikových dodavatelů ICT ve strategické infrastruktuře. Může také dojít k omezení volnosti strategického rozhodování ČR, kdy bude nutné vzít v potaz možnost zneužití přítomnosti rizikových dodavatelů cizím státem.

e. Může docházet k výskytu vícero závažných zranitelností a tím k navýšení počtu kybernetických incidentů a útoků ze strany států, které mohou zneužívat svého vlivu nad dodavateli operujícími ve sféře jejich vlivu. Tito dodavatelé poskytující hardware či software do strategické infrastruktury ČR mohou cíleně narušit důvěrnost, integritu a dostupnost dat.

f. Vznik nepřiměřených finančních dopadů pro ČR. Sanace kybernetických incidentů s sebou může přinášet náklady pohybující se v řádech desítek miliónů až miliard



[18] V České republice se jedná zejména o Zákon č. 289/2005 Sb., o Vojenském zpravodajství.

korun. Dále je nutné zmínit nežádoucí finanční dopady spojené se situací, kdy může být nezbytné produkty bezpečnostně rizikových dodavatelů bezodkladně nahradit až ve chvíli, kdy se již hrozba bezprostředně realizovala. A to navíc pouze v případě, že by takové odstranění bylo po technické, finanční a legislativní stránce proveditelné. Časový rámec potřebný pro nahrazení infrastruktury pak navíc může násobně překračovat lhůtu pro efektivní reakci, což jen podtrhuje potřebu včasného a proaktivního řešení, nikoli až reakci ex post.

g. Sekundárně dochází k nepřímému financování států, které mohou tyto prostředky následně využívat pro narušování zájmů ČR a jejích spojenců. Tuto situaci lze nyní pozorovat například při nákupu plynu či ropy pocházejících z RF, kdy jsou získané finanční prostředky vynakládány na vedení ozbrojeného konfliktu na Ukrajině.

Přestože jsou popsaná rizika spojená s dodavateli známá, v současnosti neexistuje v ČR komplexní mechanismus, který by umožnil rizika plynoucí z těchto strategických hrozeb pro strategicky významnou infrastrukturu cíleně a účinně vyhodnocovat a mitigovat. Stát by neměl rezignovat na svoji základní povinnost tím, že ji přenese na třetí, často soukromé, osoby. Stát proto nemůže ponechat výhradní výběr potenciálně rizikového dodavatele tak strategicky významné infrastruktury státu zcela v rukou soukromých společností, které nemusí být dostatečně vybaveny nebo motivovány k ochraně bezpečnosti ČR. Ačkoliv mají soukromé společnosti zájem o poskytování kvalitních a bezpečných produktů a služeb, jejich primárním cílem je dosažení zisku, přičemž tyto dva aspekty (bezpečnost versus výše zisku prostřednictvím minimalizace nákladů) mohou být v určitých případech v přímém rozporu a společnosti mohou upřednostnit vyšší zisk na úkor bezpečnosti. V souladu s čl. 1 ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky, ve znění pozdějších předpisů, dle kterého je základní povinností státu: *„zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot“* musí stát ze své podstaty na takové riziko reagovat a usilovat o jeho mitigaci. Akceptace existující míry rizika je nepřijatelná a cílem tohoto zákona je umožnit státu disponovat takovými nástroji, které toto riziko sníží na akceptovatelnou úroveň.

Díky kontinuálnímu prověřování dodavatelů ve strategicky významné infrastruktuře bude docházet také ke zvyšování povědomí NÚKIB, jakožto ústředního správní orgánu pro oblast kybernetické bezpečnosti, o aktuálních trendech a hrozbách pro kybernetickou bezpečnost v regulovaných sektorech. Získané poznatky následně bude NÚKIB dále využívat v mezích svých pravomocí stanovených § X zákona o kybernetické bezpečnosti, i mimo oblast strategicky významné infrastruktury, a to směrem ke všem provozovatelům regulovaných služeb dle prováděcího právního předpisu, vyhlášky o regulovaných službách. Tato nová právní úprava tak přispěje k navýšení bezpečnosti a odolnosti České republiky.

## 1.4 Zhodnocení souladu navrhované právní úpravy s ústavním pořádkem České republiky

Předkládaný návrh zákona je v souladu s ústavním pořádkem České republiky a nevytváří podmínky vedoucí k nerovnému postavení mužů a žen.

Předkládaný návrh zákona je v souladu s článkem 2 odst. 3 ústavního zákona č. 1/1993Sb., Ústava České republiky (dále jen „Ústava“), 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.

Navrhovaná právní úprava je rovněž v souladu s Usnesením předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky (dále jen „Listina“). Konkrétně se jedná o článek 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 článku 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 či veřejného pořádku, kdy 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 subjektů zajišťuje přiměřená lhůta k výměně produktu či služby vysoce rizikového dodavatele, která v maximální možné míře respektuje životní cyklus produktů.

Článek 17 odst. 4 Listiny stanoví, že svobodu projevu a právo vyhledávat a šířit informace lze omezit zákonem, jde-li o opatření v demokratické společnosti nezbytná pro ochranu práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost, ochranu veřejného zdraví a mravnosti. V souladu s tímto ustanovením předkládaný návrh zákona omezuje dostupnost informací např. podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, neboť v procesu prověřování bezpečnosti dodavatelského řetězce

budou zohledňovány citlivé informace o osobě dodavatele (včetně jeho vazeb, majetkové struktury, podnikatelské činnosti) a zákonem chráněné informace, typicky utajované informace podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, poskytnuté zpravodajskými službami a jinými státními orgány, nebo informace čerpané z neveřejných zdrojů. Zveřejnění takových informací by mohlo ohrozit zájmy ČR, bezpečnost, vnitřní či veřejný pořádek, případně zásadním způsobem poškodit zájmy jiné osoby nebo zájmy jiných členských států EU a NATO. Předkladatel proto rovněž navrhuje, aby utajované a důvěrné části písemností a záznamy byly vedeny odděleně od správního spisu, a aby byla omezena možnost nahlížení do spisu.

Navrhovaná právní úprava nijak nesnižuje práva dotčených subjektů a nejsou jí diskriminovány žádné specifické skupiny adresátů právních norem. Respektuje obecné zásady ústavního pořádku České republiky a není v rozporu s nálezy Ústavního soudu.

## 1.5 Zhodnocení slučitelnosti navrhované právní úpravy s předpisy Evropské unie

Navrhovaný zákon je v souladu se směrnicí Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 („směrnice NIS 2“). Směrnice NIS 2 ukládá členským státům povinnost zohlednit problematiku dodavatelského řetězce v rámci národní strategie kybernetické bezpečnosti [čl. 7 odst. 2 písm. a) směrnice NIS 2] a také povinnost zajistit, aby základní a důležité subjekty přijaly vhodná a přiměřená technická a organizační opatření k řízení bezpečnostních rizik, které zahrnují opatření k zajištění bezpečnosti dodavatelského řetězce těchto subjektů [čl. 21 odst. 1 a odst. 2 písm. d) směrnice NIS 2]. Směrnice NIS 2 také v čl. 22 předpokládá provádění koordinovaných posouzení bezpečnostních rizik kritických dodavatelských řetězců na unijní úrovni. Dle bodu 91 preambule směrnice NIS 2 by se při posuzování rizik kritických dodavatelských řetězců s ohledem na charakteristické rysy dotčeného odvětví měly zohlednit jak technické, tak případné netechnické faktory včetně faktorů vymezených v doporučení Komise (EU) 2019/534, v koordinovaném posouzení rizik pro bezpečnost sítí 5G v celé EU a v souboru opatření EU pro kybernetickou bezpečnost sítí 5G, na němž se dohodla skupina pro spolupráci. V doporučení Komise (EU) 2019/534 jsou jako relevantní faktory zmíněné i regulační nebo jiné požadavky kladené na dodavatele zařízení informačních a komunikačních technologií nebo jiná rizika vlivu třetí země jako např. model správy věcí veřejných, neexistence dohod o spolupráci v oblasti bezpečnosti nebo podobných ujednání apod. (bod 20 preambule doporučení). Význam právních a politických faktorů vyplývá i z odst. 15 bodu a) doporučení.

Další legislativní iniciativou, která je nyní ve fázi vyjednávání v unijním legislativním procesu a má také ambici zvýšit bezpečnost dodavatelského řetězce, je návrh nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020. Ačkoli návrh tohoto nařízení není zaměřen na strategicko-politické aspekty bezpečnosti výrobků, nýbrž na ty technické, problematika bezpečnosti dodavatelského řetězce je v něm taktéž zohledněna. Konkrétně v čl. 10 odst.4 návrhu nařízení je stanovena povinnost výrobců při začleňování součástí pocházejících od třetích stran do produktů s digitálními prvky postupovat s náležitou péčí tak, aby nebyla ohrožena bezpečnost daného produktu. V čl. 6 odst. 5 návrhu nařízení, který

svěřuje Evropské komisi pravomoc upřesňovat kategorie vysoce kritických produktů s digitálními prvky, je odolnost dodavatelského řetězce uvedena v písm. b) tohoto ustanovení jako relevantní hodnotící kritérium, které se má při určování těchto specifických kategorií zohlednit. Zájem na pečlivém přístupu k problematice bezpečnosti dodavatelského řetězce lze vypozorovat i z bodu 33 preambule návrhu nařízení, dle kterého technické požadavky nařízením stanovené nezabraňují členským státům přijímat další opatření zohledňující netechnické faktory ve vztahu k bezpečnosti produktu. Dále bod 25 preambule návrhu nařízení k bezpečnosti dodavatelského řetězce upozorňuje na fakt, že zranitelnosti v jednom produktu mohou vést k šíření problémů v celém dodavatelském řetězci. Je tedy nutné eliminovat riziko u každého jednotlivého produktu, aby došlo k celkovému navýšení odolnosti dodavatelských řetězců. Z výše uvedeného lze tedy dojít k závěru, že z pohledu unijního práva jsou tendence zajistit kybernetickou bezpečnost dodavatelského řetězce holistickým přístupem.

Návrh zákona je dále v souladu s nařízením Evropského parlamentu a Rady (EU) 2019/452 ze dne 19. března 2019, kterým se stanoví rámec pro prověřování přímých zahraničních investic směřujících do Unie, dle kterého členské státy mohou mít zavedeny, měnit nebo zavádět mechanismy k prověřování přímých zahraničních investic na svém území z důvodu bezpečnosti nebo veřejného pořádku, přičemž tyto investice mohou členské státy dokonce i zakázat (čl. 2 odst. 3 a 4 a čl. 3 nařízení). Nařízení explicitně uvádí, že členské státy mohou v souvislosti s bezpečností a veřejným pořádkem zohlednit potenciální dopady investice na kritickou infrastrukturu, kritické technologie, dodávky kritických vstupů (např. energie nebo suroviny), přístup k citlivým informacím včetně osobních údajů a schopnost takové informace kontrolovat nebo také na svobodu a pluralitu sdělovacích prostředků (čl. 4 odst. 1 nařízení). Podle nařízení je rovněž vhodné zohledňovat, zdali je daný zahraniční investor přímo či nepřímo kontrolovaný vládou třetí země, zdali již daný investor byl zapojen do činností ovlivňujících bezpečnost nebo veřejný pořádek v některém členském státě či zdali existuje vážné riziko, že je daný zahraniční investor zapojen do protiprávní nebo trestné činnosti (čl. 4 odst. 2 nařízení). Stejně tak směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace, obsahuje ustanovení umožňující členským státům přijímat opatření za účelem zajištění veřejného pořádku a veřejné bezpečnosti, jakož i za účelem obrany (čl. 1 odst. 3 písm. c) směrnice). Tyto právní předpisy tedy umožňují přijímání restriktivních opatření z důvodu bezpečnosti státu.

Navrhovaný zákon je v souladu s příslušnými ustanoveními o volném pohybu osob, služeb a kapitálu Smlouvy o fungování Evropské unie (dále jen „SFEU“) – konkrétně s ustanoveními o svobodě usazování, ve které je zahrnut přístup k samostatně výdělečným činnostem a jejich výkon, jakož i zřizování a řízení podniků, zejména společností (čl. 49 SFEU), v návaznosti na ustanovení o pohybu kapitálu umožňující členským státům, mimo jiné, učinit opatření odůvodněná veřejným pořádkem či veřejnou bezpečností (čl. 63 a čl. 65 odst. 1 písm. b) SFEU). Neméně důležitý je i soulad se Smlouvou o Evropské unii (dále jen „SEU“), který je dán skutečností, že Evropská unie dle této smlouvy respektuje základní funkce státu, zejména ty, které souvisejí se zajištěním územní celistvosti, udržením veřejného pořádku a ochranou národní bezpečnosti. Zejména národní bezpečnost zůstává výhradní odpovědností každého členského státu (čl. 4 odst. 2 SEU).

Navrhovaná právní úprava je v souladu také s Listinou základních práv Evropské unie (dále jen „Listina EU“). Svoboda podnikání je Listinou EU garantována, avšak musí

být vykonávána v souladu s právem Unie a vnitrostátními zákony a zvyklostmi (čl. 16 Listiny EU). Navrhovaný zákon taktéž nezakládá nerovnost (čl. 20 Listiny EU) ani diskriminaci mezi adresáty (čl. 21 Listiny EU), jelikož nastavuje obecná kritéria vztahující se na všechny adresáty a počítá i s právem na soudní ochranu (čl. 47 Listiny EU). Vzhledem k tomu, že hlavním účelem návrhu zákona je posílení celkové národní bezpečnosti státu a zvýšení ochrany demokratického zřízení, návrh zákona přispěje k zajištění práva na svobodu a osobní bezpečnost (čl. 6 Listiny EU). Zvýšením bezpečnostních standardů dojde v konečném důsledku, také k efektivnější ochraně osobních údajů (čl. 8 Listiny EU).

Navrhovaný zákon není v rozporu s judikaturou soudních orgánů Evropské unie a je v souladu s předpisy Evropské unie a obecnými právními zásadami práva Evropské unie.

## 1.6 Zhodnocení souladu navrhované právní úpravy s mezinárodními smlouvami

Předkládaný návrh zákona je v souladu s mezinárodními smlouvami, jimiž je ČR vázána, stejně jako s obecnými pravidly a zásadami mezinárodního práva.

### 1.6.1 Lidskoprávní závazky

*Evropská úmluva o ochraně lidských práva (EÚLP)*

Relevantními ustanoveními EÚLP majícími potenciál se uplatnit ve vztahu k předmětu úpravy předkládaného návrhu zákona jsou čl. 6 – Právo na spravedlivý proces a čl. 1 Dodatkového protokolu č. 1 – Ochrana vlastnictví.

Právo na spravedlivý proces je zajištěno možností přezkoumat opatření obecné povahy opravnými prostředky dle zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů, a soudním přezkumem podle zákona č. 150/2002 Sb., soudní řád správní, ve znění pozdějších předpisů.

Ochrana vlastnictví dle EÚLP chrání již nabytý majetek, existující nárok nebo legitimní očekávání nabytí majetku. Nevztahuje se na v budoucnu učiněné investice a dodávky. Předkládaný návrh omezuje 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 kybernetické bezpečnosti státu. Minimalizaci zásahu do vlastnictví povinných subjektů zajišťuje přiměřená lhůta k výměně produktu či služby vysoce rizikového dodavatele, která v maximální možné míře respektuje životní cyklus produktů. Předkládaný návrh je tudíž v souladu s právem na ochranu vlastnictví dle EÚLP.

*Mezinárodní pakt o občanských a politických právech (Pakt)*

Mezinárodní pakt o občanských a politických právech zakotvuje v článku 2 odst. 3 právo domáhat se ochrany před případným zásahem do práv garantovaných Paktem. S předkládaným návrhem souvisí právo na spravedlivý proces dle článků 14 a 15 Paktu, jehož obsah lze pro účely předkládaného návrhu považovat za shodný s obsahem čl. 6 EÚLP. S odkazem na výše uvedené tedy předkládaný návrh není s Paktem v rozporu.

### 1.6.2 Obchodní a investiční závazky

*Světová obchodní organizace (WTO)*

Předkládaný návrh je v souladu 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 1947 (GATT 1947) 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 1947 i GATS, a proto neodporuje závazkům ČR přijatým v rámci WTO.

*Bilaterální dohody o podpoře a ochraně investic (BITs)*

Dohody o podpoře a ochraně investic stejně jako GATT či GATS přiznávají investorům smluvních stran podmínky ne méně příznivé než investorům ze třetích států. Jednou z podmínek investic dle BITs (vyjma BIT s USA) 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 BITs.

Ochrana stávajících investic podle BITs 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. Jedná se tudíž o minimální možný zásah k dosažení účelu předkládaného návrhu, zajištění bezpečnosti dodavatelského řetězce strategicky významné infrastruktury.

V neposlední řadě obsahuje většina BITs s doložku se základními bezpečnostními zájmy smluvních stran. Doložka opravňuje strany přijmout taková opatření, která považují

za nezbytná pro ochranu svých základních bezpečnostních zájmů.[19,20,21] 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.

BITs také řadí mezi základní bezpečnostní zájmy smluvní strany 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 demonstrativním výčtu minima nutných opatření (čl. 21 odst. 2. písm. d) směrnice NIS 2).

Předkládaný návrh zákona tedy není v rozporu s bilaterálními dohodami o ochraně investic, jimiž je ČR vázána.

## 1.7 Předpokládaný hospodářský a finanční dopad navrhované právní úpravy na státní rozpočet, ostatní veřejné rozpočty na podnikatelské prostředí České republiky, dále sociální dopady, včetně dopadů na rodiny a dopadů na specifické skupiny obyvatel, zejména osoby sociálně slabé, osoby se zdravotním postižením a národnostní menšiny, a dopady na životní prostředí

### 1.7.1 Dopady na státní rozpočet

Do procesu prověřování dodavatelů budou zapojeny relevantních státních orgány, které budou z oblasti svojí působnosti NÚKIB poskytovat relevantní informace k posuzovaným dodavatelům. Z toho důvodu bude pro účely zavedení a realizaci mechanismu posuzování dodavatelů nutné vyčlenit nízké desítky pracovníků. Mechanismus posuzování dodavatelů je ovšem navržen tak, aby v maximální možné míře využíval již stávajících kapacit jednotlivých státních orgánů.

Ve vztahu k návrhu zákona bude nutné vyhradit jednotky až nízké desítky tabulkových míst u zapojených státních orgánů a rozšíření stávajících či připravovaných informačních systémů k technické obsluze procesu prověřování. Na straně NÚKIB a spolupracujících institucí budou muset být vynaloženy náklady, aby mohlo docházet k systematickému a koordinovanému prověřování dodavatelů do strategicky významné infrastruktury. V souladu s principem efektivity a cílem minimalizace ekonomických nákladů se bude maximálně využívat fungující synergie s již existujícími agendami a procesy, jakými jsou kupříkladu prověřování žadatelů o zápis do katalogu poskytovatelů služeb cloud computingu orgánům

[19] Nejčastější doložka (např. BIT s Ázerbájdžánem čl. 13) je v podstatě opsaný čl. XXI GATT s přidanou výjimkou ve vztahu k trestným činům (v některých případech také ke správním deliktům) a k bezpečnostním zájmům vyplývajícím z členství v EU. GATT obsahuje výjimku pro opatření k ochraně bezpečnostních zájmů týkajících se i) štěpných materiálů, ii) obchodu se zbraněmi, střelivem, válečným materiálem nebo iii) učiněných za války.
Nejjistější cesta k naplnění výjimky by vedla přes EU závazky (čl. 21 odst. 2. písm. d) NIS 2), ale vzhledem k tomu, že zatím není v platnosti, šel jsem přes obecné bezpečnostní zájmy.

[20] Alternativně existuje obecnější doložka, která se neuplatňuje v takové míře. Příkladem budiž BIT s Makedonií (čl. 10 po protokolu z roku 2010), který umožňuje smluvním stranám použít opatření nezbytná pro udržení veřejného pořádku, …, nebo ochranu jejich základních bezpečnostních zájmů. BIT s touto doložkou proto v rozporu s návrhem nejsou.

[21] Některé BIT také žádnou doložku o bezpečnostních výjimkách nestanovují. Bohužel často v případech rizikových států jako Bělorusko, Čína, Rusko (viz tabulka Země a typ dohody.xlsx)

veřejné moci či prověřování zahraničních investorů dle zákona o prověřování zahraničních investic, a to včetně účelného využívání informačních systémů, které tyto agendy podporují.

Vzhledem k tomu, že navrhovaná právní úprava nevyžaduje ex ante prověření všech dodavatelů, resp. dodavatelských řetězců do strategicky významné infrastruktury, minimalizuje také nároky na personální a administrativní kapacity státu, a tedy na státní rozpočet.

### 1.7.2 Dopady na ostatní veřejné rozpočty

Povinné osoby mechanismu jsou jak soukromoprávními, tak veřejnoprávními subjekty či orgány, přičemž obě kategorie jsou zastoupeny zhruba 50 % z odhadovaného počtu 150 povinných osob mechanismu. Nové povinnosti povinných osob mechanismu budou sestávat z povinnosti NÚKIB hlásit přímé dodavatele bezpečnostně relevantních dodávek, vynaložit přiměřené úsilí ke zjišťování nepřímých dodavatelů bezpečnostně relevantních dodávek a zjištěné nepřímé dodavatele taktéž hlásit NÚKIB. Tyto nové povinnosti generují na straně povinných osob mechanismu minimální administrativní náklady.

Potenciální významnější náklady povinným osobám mechanismu generuje povinnost dodržovat opatření vydaná NÚKIB. V případě upozornění na riziko spojené s dodavatelem se bude jednat o reflexi identifikované hrozby v analýze rizik, což je opět proces, který je u povinných osob mechanismu již nastavený a fungující.

Na povinné osoby mechanismu má potenciálně vysoký dopad případný zákaz dodavatele. Pokud by povinná osoba mechanismu identifikovaného zakázaného vysoce rizikového dodavatele využívala v bezpečnostně relevantní dodávce, bude muset takového dodavatele ze své infrastruktury vyloučit. Dle výsledků dotazníkového šetření[22] lze tedy předpokládat, že případné omezení či vyloučení dodávek dodavatele, které veřejné subjekty a orgány povinné z mechanismu posuzování dodavatelů využívají, bude znamenat zvýšené finanční náklady také pro veřejné rozpočty. Maximální náklady spojené s vyloučením významného dodavatele mohou být až ve výši[23] jednotek milionů Kč (3 % respondentů), desítek milionů Kč (34 % respondentů) i stovek milionů Kč (16 % respondentů). 25 % respondentů uvedlo náklady vyšší než 1 miliarda Kč, nicméně náklady byly vyčísleny do takové výše z důvodu, že dané orgány či osoby uvažovaly o vyloučení dodavatelů, kteří jako jediní jsou schopni dané plnění poskytnout. Do kalkulace nákladů tak započítávali mj. dopady ukončení či omezení poskytování regulované služby, vč. ušlého zisku. Jelikož je podle navrhovaného mechanismu prověřování dodavatelů možné udělit výjimku z vyloučení dodavatele, a to v případě, pokud by mohlo být podstatným způsobem ohroženo poskytování regulované služby, takto vysoké náklady překladatel nepředpokládá. Vyloučení dodavatele ovšem může



[22] Dotazníkové šetření bylo adresovaného všem orgánům a osobám dle § 3 c), d), f) a g) zákona o kybernetické bezpečnosti (odesláno prostřednictvím datové schránky 1. 11. 2022 s žádostí o sdílení vyplněného dotazníku do 30. 11. 2022). Následně NÚKIB vyhodnotil odpovědi orgánů a osob, kteří se stanou poskytovateli regulované služby v režimu vyšších povinností, kterým plynou povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce, přičemž některé orgány či osoby spravující či provozující více systémů poskytli odpovědi za každý takový systém zvlášť. NÚKIB obdržel 65 takových odpovědí (dále jen „respondenti“).

[23] Na otázku uvedení maximálního finančního dopadu na zastupovanou organizaci v případě zákazu využívání plnění nejvýznamněji zastoupeného významného dodavatele dle § 2 písm. n) vyhlášky o kybernetické bezpečnosti po uplynutí ekonomické životnosti poskytovaného aktiva obdržel NÚKIB 32 odpovědí, které lze kvantifikovat.

mít na povinnou osobu mechanismu při aplikaci přechodné lhůty odpovídající ekonomické životnosti aktiva také dopad nulový, jak uvedlo 22 % respondentů.

Přesnější vyčíslení nákladů není možné, protože do něj vstupuje řada neznámých proměnných, a to zejména jak často bude nutné přistoupit k omezení některého z dodavatelů, v jakém rozsahu bude omezovaný dodavatel ve strategické infrastruktuře zastoupen a jaký způsob reakce na dané omezení přijme konkrétní povinná osoba mechanismu.

### 1.7.3 Dopady na podnikatelské prostředí

Mechanismus posuzování dodavatelů zřízený předkládaným návrhem zákona přispěje ke zvýšení povědomí podnikatelské sféry o bezpečnostních rizicích, která mohou být spojena se spoluprací s rizikovým dodavatelem. Pro domácí podnikatelské subjekty (a to nejen pro strategickou infrastrukturu státu) tak vzniká prostředek, kterým mohou získat informace o zahraničním dodavateli potřebné pro minimalizaci rizika plynoucího z dodávek, které nejsou učiněny v dobré víře.

Mechanismus posuzování dodavatelů bude mít další dopady na povinné osoby mechanismu. S ohledem na návaznost procesů spojených s mechanismem prověřování na stávající procesy, které povinné osoby dle zákona o kybernetické bezpečnosti mají již v současnosti povinnost provádět, jako je identifikace a hodnocení aktiv, analýza rizik apod., dochází k minimálnímu zásahu, a tedy i k minimálnímu vzniku dodatečných nákladů při zavádění nové regulace do právních předpisů. Nové povinnosti povinných osob mechanismu budou sestávat z povinnosti NÚKIB hlásit přímé dodavatele bezpečnostně relevantních dodávek, vynaložit přiměřené úsilí ke zjišťování nepřímých dodavatelů bezpečnostně relevantních dodávek a zjištěné nepřímé dodavatele taktéž hlásit NÚKIB. Tyto nové povinnosti generují na straně povinných osob mechanismu minimální administrativní náklady.

Potenciální významnější náklady povinným osobám mechanismu generuje povinnost dodržovat opatření vydaná NÚKIB. V případě upozornění na riziko spojené s dodavatelem se bude jednat o reflexi identifikované hrozby v analýze rizik, což je opět proces, který je u povinných osob mechanismu již nastavený a fungující. Případný zákaz dodavatele má potenciální vysoký dopad na povinné osoby. Pokud by povinná osoba identifikovaného zakázaného vysoce rizikového dodavatele využívala v bezpečnostně relevantní dodávce, bude muset takového dodavatele ze své infrastruktury vyloučit.

Dopady vyloučení dodavatele bezpečnostně významné dodávky jsou přiblíženy v kapitole 1.7.2. Dopady na ostatní veřejné rozpočty a analogicky lze tyto dopady aplikovat také na podnikatelské prostředí, včetně omezení vyčíslení nákladů v důsledku velkého množství neznámých vstupů.

56 % respondentů dotazníkového šetření navíc jako nejzávažnější možný dopad na poskytování služby identifikuje omezení či ukončení poskytování služby.[24] Právě riziko ohrožení poskytování regulované služby podstatným způsobem také umožňuje poskytovateli

[24] Na dotaz odhadu nejhorších možných dopadů na poskytování služby, pro kterou jsou respondenti regulováni ZKB, v případě že by bylo zakázáno využívat plnění významného dodavatele, který dodává vysoká a kritická technická aktiva pokud by lhůta pro vyloučení dodavatele byla stanovena na ekonomickou životnost aktiva odpovědělo 50 respondentů.

regulované služby zažádat o výjimku ze zákazu plnění identifikovaného vysoce rizikového dodavatele. Pro dalších 32 % respondentů jsou nejzávažnější dopady finanční. 12 % respondentů v případě aplikace lhůty respektující ekonomickou životnost daného aktiva pro vyloučení stávajícího dodavatele neidentifikuje žádné vícenáklady kromě těch, které jsou s obnovou technologie a přechodem na alternativní technologická řešení standardně spojena.

V případě, že povinná osoba vysoce rizikového dodavatele v současnosti nevyužívá, nicméně v budoucnu by o bezpečnostně relevantních dodávkách tohoto dodavatele uvažovala, z důvodu vyloučení možnosti bezpečnostně relevantní dodávku od vysoce rizikového dodavatele pořídit, může čelit dalším dopadům. Ty souvisejí především s možnou vyšší cenou od alternativních dodavatelů. Tento přístup a zvýšené náklady se mohou objevit obzvláště v případě, že na trhu není dostatečná konkurence a danou dodávku poskytuje pouze omezený počet dodavatelů.

V neposlední řadě přináší navrhovaná regulace dodatečné nepřímé náklady taktéž dodavatelům bezpečnostně relevantních dodávek. V případě vyloučení vysoce bezpečnostně rizikového dodavatele z možnosti poskytovat bezpečnostně relevantní dodávky do strategicky významné infrastruktury dojde k omezení hospodářské soutěže. Toto omezení se ovšem bude zakládat na transparentním a přezkoumatelném rozhodnutí NÚKIB, který vyhodnotí veškeré informace, které jsou relevantní vzhledem k vyhodnocování kritérií definovaných ve vyhlášce o kritériích rizikovosti dodavatele, které má k danému dodavateli k dispozici, a to jak ze svého vlastního šetření či na základě informací obdržených od ostatních státních orgánů zapojených do procesu posuzování dodavatelů. V případě, že NÚKIB neidentifikuje riziko spojené s posuzovaným dodavatelem, takový dodavatel nebude na svém právu podnikat v ČR jakkoliv omezen. I dodavatelé, kteří budou rozhodnutím NÚKIB omezeni ovšem budou moci i nadále poskytovat ostatní dodávky do strategické infrastruktury, stejně tak jako dalším subjektům v ČR.

Možné omezení okruhu subjektů na trhu z důvodu omezení rizikových dodavatelů může vést k nárůstu cen dodávaných technologií, a tedy i ke zvýšení nákladů na straně regulovaných subjektů. Vzhledem k možnému snížení počtu dodavatelů technologií může dojít k alespoň dočasnému poklesu vzájemného konkurenčního tlaku, a tím pádem i ke snížení motivace k vytváření inovací.[25] Omezení rizikových dodavatelů je ovšem odůvodněno prevencí ohrožení bezpečnosti České republiky či veřejného pořádku. Touto novou regulací dále dojde ke zvýšení celkové úrovně bezpečnosti služeb a produktů, čímž dojde ke snížení investičních rizik spojených s dodavatelským řetězcem pro potenciální investory, obzvláště ze zemí, které bezpečnost dodavatelského řetězce již právně regulují.

Vzhledem k tomu, že navrhovaná právní úprava nevyžaduje ex ante prověření všech dodavatelů, resp. dodavatelských řetězců do strategicky významné infrastruktury, minimalizuje také zásah prověřování do podnikatelských procesů, nehrozí tedy zdržení investic a zpomalení rozvoje z důvodu zpomalení výběrových řízení.



[25] Podobné obavy měli např. v Dánsku (viz FOLKETINGET. L 190 Forslag til lov om leverandørsikkerhed i den kritiske teleinfrastruktur. Dostupné z: https://www.ft.dk/samling/20201/lovforslag/l190/20201_l190_som_fremsat.htm

### 1.7.4 Sociální dopady

Navrhovaná právní úprava nebude mít žádné sociální dopady. Z povahy věci nepředpokládáme žádné dopady na rodiny či specifické skupiny obyvatel (zejména osoby sociálně slabé, osoby se zdravotním postižením a národnostní menšiny).

### 1.7.5 Dopady na životní prostředí

Navrhovaná právní úprava nebude mít z povahy věci žádné dopady na životní prostředí.

## 1.8 Zhodnocení dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů

Navrhovaná právní úprava je v souladu s ochranou soukromí a osobních údajů. Je zajištěna jejich standardní ochrana v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

Účelem navrhované právní úpravy je mimo jiné dosáhnout vyšší úrovně zabezpečení kriticky významných ICT produktů prostřednictvím omezení či zákazu plnění od rizikových dodavatelů. Důsledkem posílení zabezpečení bude i posílení ochrany případných osobních údajů uložených a zpracovávaných danými ICT produkty.

## 1.9 Zhodnocení korupčních rizik

Při zpracování předkládaného zákona zohlednil předkladatel kritérium omezení korupčních příležitostí při aplikaci navrhovaného zákona.

Návrh zákona může mít potenciálně zásadní dopady na poptávku po zboží a službách některých dodavatelů do strategicky významné infrastruktury ČR. Tato skutečnost může vyvolat korupční tlak na změnu způsobu prověřování kritérií nebo úpravu celkového zhodnocení rizikovosti dodavatele. Obdobně mohou i někteří správci regulované infrastruktury usilovat o to, aby nebyl konkrétní poskytovatel v důsledku posouzení důvěryhodnosti omezen, jelikož by to pro ně znamenalo zvýšené náklady. Někteří správci mohou naopak usilovat o omezení konkrétního dodavatele za účelem zhoršení postavení svého konkurenta, který takového dodavatele využívá ve své infrastruktuře.

Jako pojistku proti možnému korupčnímu jednání vnímá předkladatel zejména to, že spolupráce na konkrétních případech prověřování dodavatelů bude probíhat v širokém okruhu na sobě nezávislých institucí, které budou poskytovat stanoviska a informace vycházející z vlastních zdrojů. Případné pochybení jedince by ve většině případů nemělo mít dopad na výsledek procesu.

V této souvislosti je rovněž vhodné upozornit na to, že fyzické osoby zapojené do fungování prověřovacího mechanismu mohou přicházet do kontaktu s utajovanými informacemi, a bude tedy nutné, aby byly držiteli adekvátního oprávnění pro přístup k utajovaným informacím. V rámci žádosti o vydání osvědčení a během doby, po kterou budou jeho držiteli, jsou povinny dokládat relevantní informace o svých majetkových poměrech a stát

má možnost jim osvědčení o bezpečnostní způsobilosti odebrat, čímž by byly vyřazeni z možnosti seznamovat se s utajenými informacemi.

## 1.10 Zhodnocení dopadů na bezpečnost nebo ochranu státu

Mechanismus posuzování dodavatelů bude mít pozitivní vliv na národní bezpečnost a obranu. Budování odolné strategicky významné infrastruktury bez rizikových dodavatelů přispěje k její odolnosti. Právě odolná strategicky významná infrastruktura je klíčovým předpokladem pro zajištění národní bezpečnosti a obrany. S tímto předpokladem pracuje jak aktuálně platná Bezpečnostní strategie ČR, tak i Národní strategie pro čelení hybridnímu působení a Národní strategie kybernetické bezpečnosti ČR. Vazbu na odolnou a bezpečnou infrastrukturu jako integrální součást národní bezpečnosti rovněž zdůrazňují strategické dokumenty NATO[26].

Zavedením mechanismu posuzování dodavatelů se navíc podstatně sníží riziko vzniku závislosti strategické infrastruktury na jednotlivých rizikových dodavatelích.



[26] Strategická koncepce NATO 2022, článek 26.