V l á d n í n á v r h

ZÁKON

ze dne ……. 2020,

kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, a některé další zákony

Parlament se usnesl na tomto zákoně České republiky:

ČÁST PRVNÍ

Změna zákona o Vojenském zpravodajství

Čl. I

V zákoně č. 289/2005 Sb., o Vojenském zpravodajství, ve znění zákona č. 274/2008 Sb., zákona č. 254/2012 Sb., zákona č. 273/2012 Sb., zákona č. 64/2014 Sb., zákona č. 250/2014 Sb., zákona č. 47/2016 Sb., zákona č. 35/2018 Sb. a zákona č. 205/2019 Sb., se za část třetí vkládá nová část čtvrtá, která včetně nadpisu a poznámek pod čarou č. 19 až 22 zní:

„ČÁST ČTVRTÁ

ČINNOSTI VOJENSKÉHO ZPRAVODAJSTVÍ PŘI ZAJIŠŤOVÁNÍ OBRANY ČESKÉ REPUBLIKY

§ 16a
Činnosti Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru

(1) Vojenské zpravodajství za podmínek stanovených tímto zákonem provádí

a) cílenou detekci kybernetických útoků a hrozeb majících původ v zahraničí[12)] a směřujících proti důležitým zájmům státu, jejichž zajišťování je předmětem obrany České republiky podle zákona o zajišťování obrany České republiky[19)] (dále jen „detekce“),
b) identifikaci a vyhodnocování detekovaných kybernetických útoků a hrozeb a jejich dopadů (dále jen „vyhodnocování“) a
c) opatření k odvracení detekovaných kybernetických útoků a hrozeb.

(2) Detekce je Vojenským zpravodajstvím prováděna na základě jím stanovených ukazatelů kybernetických útoků a hrozeb umožňujících odhalit v kybernetickém prostoru definované jevy, které v daném čase byly vyhodnoceny jako skutečnosti ohrožující důležité zájmy státu v kybernetickém prostoru.

(3) Ukazatele kybernetických útoků a hrozeb jsou Vojenským zpravodajstvím stanovovány na základě

a) dat a informací, které Vojenské zpravodajství získává při plnění svých úkolů jako jednotné ozbrojené zpravodajské služby České republiky,
b) dat a informací předaných ostatními zpravodajskými službami, Národním úřadem pro kybernetickou a informační bezpečnost a dalšími státními orgány, nebo
c) dalších skutečností způsobilých ohrozit plnění funkce státu v oblasti zajišťování jeho obrany, které jsou mu předány.

§ 16b

Spolupráce Vojenského zpravodajství při provádění činností, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru

Při provádění činností a opatření vykonávaných v souvislosti se zajišťováním obrany státu v kybernetickém prostoru spolupracuje Vojenské zpravodajství s ostatními zpravodajskými službami a s dalšími státními orgány, ozbrojenými silami České republiky, bezpečnostními sbory a právnickými a fyzickými osobami, pokud působí v oblasti zajišťování kybernetické bezpečnosti nebo obrany státu.

§ 16c

Nástroje detekce a podmínky jejich provozování

(1) Vojenské zpravodajství za účelem včasné a přesné detekce a následného vyhodnocování využívá nástroje detekce, které jsou umisťovány pouze pro tyto účely na určených bodech veřejných komunikačních sítí.

(2) Nástroj detekce zaznamenává metadata[20)]
a) provozu veřejných komunikačních sítí a veřejně dostupných služeb elektronických komunikací, a to pouze v rozsahu souvisejícím s detekovaným kybernetickým útokem nebo hrozbou na základě stanovených ukazatelů,
b) provozu nástroje detekce a
c) o manipulaci s konfigurací nástroje detekce pro potřeby auditu činností vykonávaných Vojenským zpravodajstvím.

(3) Vojenské zpravodajství nesmí využívat nástroje detekce podle odstavce 1 pro provádění odposlechů nebo pro záznam zpráv podle zákona o elektronických komunikacích.

(4) Vojenské zpravodajství provádí detekci výlučně způsobem, který zaručuje, že
a) je zachována důvěrnost komunikací fyzických a právnických osob při poskytování veřejně dostupné služby elektronických komunikací, integrita veřejných komunikačních sítí a dostupnost veřejných komunikačních sítí a služeb elektronických komunikací a
b) není zasahováno nebo ovlivňováno plnění povinností právnické nebo podnikající fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací vůči uživatelům sítě jinak, než v rozsahu odpovídajícím veřejnému zájmu na zajišťování obrany státu.

§ 16d

Zajištění podmínek detekce

(1) Ministerstvo obrany požaduje od právnické nebo podnikající fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací, aby zřídila a zabezpečila v určených bodech jí zajišťované veřejné komunikační sítě rozhraní pro připojení nástroje detekce.

(2) Základní charakteristiky veřejných komunikačních sítí využitelných pro umístění nástrojů detekce z hlediska zajištění důležitých zájmů státu stanoví vláda v ústředním plánu obrany státu[21)].

(3) K plnění povinnosti podle odstavce 1 vydá Ministerstvo obrany na základě návrhu Vojenského zpravodajství vypracovaného jako opatření k zajištění závěrů jím plněných povinností stanovených v § 16a odst. 1 a 2 rozhodnutí, jímž právnické nebo podnikající fyzické osobě zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací uloží povinnost zřídit a zabezpečit rozhraní pro připojení nástrojů detekce v určeném bodě veřejné komunikační sítě a povinnost strpět umístění a provozování těchto nástrojů.

(4) Rozhodnutí podle odstavce 3 musí vedle náležitostí stanovených správním řádem obsahovat také

a) určení doby, po kterou má být nástroj detekce v určeném bodě provozován, a
b) lhůtu, ve které je právnická nebo podnikající fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinna v určených bodech jí zajišťované veřejné komunikační sítě zřídit rozhraní pro připojení nástroje detekce.

(5) Doba podle odstavce 4 písm. a) nesmí být delší než 6 měsíců, Ministerstvo obrany ji však může na návrh Vojenského zpravodajství prodloužit.

(6) Rozklad proti rozhodnutí nemá odkladný účinek.

(7) Před vydáním rozhodnutí podle odstavce 3 je Vojenské zpravodajství povinno posoudit, zda připojení nástroje detekce samo o sobě není bezpečnostním rizikem, popřípadě zda je možné důsledky takového bezpečnostního rizika přijmout jako akceptovatelné vzhledem k účelu připojení konkrétního nástroje detekce. Dokument obsahující závěry takového posouzení je podkladem pro vydání rozhodnutí podle odstavce 3.

§ 16e

Opatření k odvracení detekovaných kybernetických útoků a hrozeb

(1) Vojenské zpravodajství na základě výsledku vyhodnocování přijme opatření k odvrácení detekovaných kybernetických útoků a hrozeb podle odstavce 2 nebo 3.

(2) V případě, že identifikuje konkrétní kybernetický útok nebo hrozbu, pro jejichž odvrácení nejsou naplněny podmínky pro provedení aktivního zásahu podle § 16f, předá neprodleně zjištěné informace k provedení dalších opatření příslušným státním orgánům.

(3) Hrozí-li nebezpečí z prodlení, provede Vojenské zpravodajství za podmínek stanovených v § 16f aktivní zásah k neprodlenému odvrácení detekovaného kybernetického útoku či hrozby.

§ 16f

Oprávnění provést aktivní zásah v kybernetickém prostoru

(1) Vojenské zpravodajství je oprávněno provést aktivní zásah výlučně v případě, že

a) skutečnosti jím zjištěné v kybernetickém prostoru svědčí o existenci ohrožení důležitých zájmů státu ve značném rozsahu,
b) kybernetický útok nebo hrozba směřující proti důležitým zájmům státu trvají nebo bezprostředně hrozí a
c) kybernetický útok nebo hrozbu směřující proti důležitým zájmům státu nelze odvrátit v součinnosti s ozbrojenými silami České republiky a aktivní zásah byl vyhodnocen jako jediný možný účinný způsob jejich odvrácení.

(2) K provedení aktivního zásahu je Vojenské zpravodajství oprávněno pouze po předchozím souhlasu ministra obrany.

(3) O zahájení aktivního zásahu Vojenské zpravodajství bezodkladně informuje vládu, Národní úřad pro kybernetickou a informační bezpečnost a ostatní zpravodajské služby.

(4) Vojenské zpravodajství o provedení aktivního zásahu bezodkladně po jeho provedení informuje ministra obrany a jeho prostřednictvím

a) vládu,
b) náčelníka Generálního štábu Armády České republiky,
c) ředitele Národního úřadu pro kybernetickou a informační bezpečnost a
d) ostatní zpravodajské služby.

(5) Pro obsah předávané informace podle odstavce 4 se využije § 16g odst. 2 obdobně.

(6) Vojenské zpravodajství poskytne v souvislosti s jím prováděnými činnostmi a opatřeními, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru, v této oblasti působnosti součinnost Národnímu úřadu pro kybernetickou a informační bezpečnost nebo Policii České republiky, pokud o to v individuálních případech výlučně pro účely jimi zajišťované bezpečnosti České republiky v kybernetickém prostoru požádají; tím není dotčena součinnost výkonu veškerých činností Vojenského zpravodajství prováděných podle této části zákona vůči ozbrojeným silám České republiky při zajišťování obrany státu.

§ 16g

Záznamy o předání dat a informací nebo aktivním zásahu a jejich uchovávání

(1) Pokud Vojenské zpravodajství v rámci zajištění součinnosti pro provádění činností, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru, předává data a informace, které jsou výstupem jím prováděné detekce a vyhodnocování, zpracuje o tomto předání záznam obsahující charakteristiku předávaných dat a informací v rozsahu skutečností uvedených v odstavci 2 písm. a) až c) a e), účel předání dat a informací a dále údaje o době předání dat a informací a identifikační údaje adresáta jejich předání v rozsahu:

a) název adresáta,
b) adresa, na kterou byly data a informace předány,
c) časový údaj předání dat a informací s přesností na sekundy,
d) časový údaj o potvrzení převzetí dat a informací s přesností na sekundy.

(2) Vojenské zpravodajství je povinno o každém provedeném aktivním zásahu provést záznam, a to minimálně v rozsahu:
a) charakteristika identifikovaného útoku nebo hrozby směřující proti důležitým zájmům státu,
b) závěry posouzení útoku nebo hrozby směřující proti důležitým zájmům státu,
c) závěry posouzení přípustnosti provedení aktivního zásahu,
d) údaje o zdroji útoku nebo hrozby směřující proti důležitým zájmům státu,
e) časový údaj o provedení opatření směřujících k zastavení nebo odvrácení útoku anebo odstranění hrozby s přesností na sekundy,
f) způsob provedení zásahu a popis využitých organizačních a technických opatření,
g) další skutečnosti charakterizující provedení aktivního zásahu.

(3) Záznamy podle odstavců 1 a 2 Vojenské zpravodajství uchovává po dobu 10 let od data jejich zpracování.

§ 16h
Zprávy o činnostech Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru

(1) Vojenské zpravodajství předkládá prezidentu republiky a vládě prostřednictvím ministra obrany jednou ročně podrobnou zprávu o činnostech a opatřeních Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru, a vyhodnocení jejich účinnosti.

(2) Orgán nezávislé kontroly zpravodajských služeb České republiky (dále jen „orgán nezávislé kontroly“) podle zákona o zpravodajských službách České republiky předkládá vládě, Poslanecké sněmovně a ministru obrany podrobnou zprávu o kontrole činností a opatření, jimiž se Vojenské zpravodajství podílí na zajišťování obrany státu v kybernetickém prostoru, a to vždy neprodleně po jejím provedení.

(3) Vojenské zpravodajství předkládá ministru obrany neprodleně po ukončení kalendářního pololetí písemnou zprávu o stavu jím plněných úkolů, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru, za toto období.

§16i
Nepřípustnost použití dat a informací k jiným účelům

Data a informace získané Vojenským zpravodajstvím při provádění detekce mohou být použity výlučně pro účely zabezpečování činností, jimiž se podílí na zajišťování obrany státu, pokud tento zákon nestanoví jinak.

16j

Inspektor pro kybernetickou obranu

(1) Vláda České republiky jmenuje na návrh ministra obrany z příslušníků Vojenského zpravodajství inspektora pro kybernetickou obranu; návrh je vládě České republiky překládán po jeho projednání ve výboru Poslanecké sněmovny příslušném ve věcech bezpečnosti.

(2) Inspektor pro kybernetickou obranu je jmenován na dobu 5 let.

(3) Inspektor pro kybernetickou obranu je příslušníkem Vojenského zpravodajství a je podřízen přímo ministrovi obrany, nestanoví-li tento zákon jinak.

(4) Ve věcech služebního poměru inspektora pro kybernetickou obranu činí právní úkony jménem České republiky ministr obrany, a to včetně provádění služebního hodnocení inspektora pro kybernetickou obranu.

(5) Inspektor pro kybernetickou obranu je při plnění úkolů podle § 16k odst. 1 písm. a) a b) nezávislý a je vázán pouze právním řádem České republiky; je povinen svou funkci vykonávat nestranně, v mezích svého oprávnění a zdržet se při jejím výkonu všeho, co by mohlo ohrozit důvěru v jeho nestrannost a profesionalitu.

(6) Vojenské zpravodajství je povinno zajistit, aby byl inspektor pro kybernetickou obranu náležitě, včas a v potřebném rozsahu zapojen do veškerých záležitostí souvisejících s činnostmi Vojenského zpravodajství, jimiž se podílí na zajišťování obrany České republiky v kybernetickém prostoru, zejména mu poskytuje veškeré potřebné informace o provádění detekce a vyhodnocování. Vojenské zpravodajství zároveň zabezpečuje materiální a personální podmínky výkonu funkce inspektora pro kybernetickou obranu.

(7) Inspektor pro kybernetickou obranu předává ministru obrany vždy neprodleně po ukončení kalendářního pololetí zprávu o jím zjištěných nedostatcích v oblasti zajišťování ochrany dat a informací zpracovávaných Vojenským zpravodajstvím při výkonu činností, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru; zpráva obsahuje rovněž návrhy opatření na zkvalitnění ochrany soukromí a osobních údajů. V případě zjištění závažného nedostatku zprávu předává inspektor pro kybernetickou obranu ministru obrany bezodkladně po jeho zjištění, a to včetně návrhů na jeho odstranění a přijetí preventivních opatření.

(8) Dnem zániku služebního poměru vojáka končí i výkon funkce Inspektora pro kybernetickou obranu.

§ 16k

Úkoly inspektora pro kybernetickou obranu

(1) Inspektor pro kybernetickou obranu vykonává tyto úkoly:

a) prověřuje správnost postupů Vojenského zpravodajství při činnostech, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru, pokud se týkají zabezpečení ochrany dat a informací,
b) ověřuje účinnost opatření přijatých Vojenským zpravodajstvím za účelem zajišťování ochrany dat a informací zpracovávaných při činnostech, jimiž se Vojenské zpravodajství

podílí na zajišťování obrany státu v kybernetickém prostoru, podílí se na jejich zavádění do činnosti Vojenského zpravodajství a navrhuje jejich případnou aktualizaci,
c) při činnostech Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru, poskytuje na vyžádání poradenskou podporu příslušníkům Vojenského zpravodajství v oblasti ochrany dat a informací,
d) za účelem zajištění účinnosti opatření přijímaných k ochraně práv spolupracuje se subjekty, u nichž byly umístěny nástroje detekce podle § 16d.

(2) Osoby se mohou obracet na inspektora pro kybernetickou obranu ve všech záležitostech souvisejících se zajištěním jejich práv, pokud jsou nebo by mohly být ohroženy činností Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru.

(3) Inspektor pro kybernetickou obranu podnět prošetří a na základě zjištěných skutečností vypracuje zprávu, z níž budou zřejmé skutečnosti, na jejichž základě bude možné vyslovit závěr, zda v konkrétním případě byl činností Vojenského zpravodajství porušen zákon a jakým způsobem. Zprávu zašle inspektor pro kybernetickou obranu osobě, která podnět podala, ministru obrany, řediteli Vojenského zpravodajství a orgánu nezávislé kontroly k vyslovení závěru podle věty první. Orgán nezávislé kontroly může před vyslovením závěru požádat ředitele Vojenského zpravodajství o doplnění poskytnutých informací; závěr orgánu nezávislé kontroly o tom, zda byl porušen zákon, se zveřejní způsobem umožňujícím dálkový přístup.

§ 16l

Kontrola činností, jimiž se Vojenské zpravodajství podílí na zajišťování obrany státu v kybernetickém prostoru, a prověřování souvisejících opatření

(1) Provádí-li vláda, Poslanecká sněmovna nebo orgán nezávislé kontroly kontrolu činností a opatření Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru, je Vojenské zpravodajství povinno kontrolujícímu předložit zejména
a) záznamy podle § 16g a
b) další zprávy, které jsou nezbytné pro zjištění skutečného stavu v rozsahu nezbytném pro dosažení účelu kontroly.

(2) Kontrolující podle odstavce 1 jsou oprávněni kdykoliv požádat o
a) přístup k auditním záznamům provozu nástroje detekce,
b) přístup ke spisové dokumentaci vedené ve věci rozhodování o umístění nástroje detekce, nebo
c) poskytnutí dalších dat a informací souvisejících s předmětem kontroly.

(3) Kontrolující je při provádění kontroly povinen šetřit práva a oprávněné zájmy Vojenského zpravodajství, stejně jako třetích osob, kterým byly v souvislosti s prováděním činností Vojenského zpravodajství podle této části zákona uloženy povinnosti.

(4) Orgán nezávislé kontroly může vykonávat kontrolní činnost podle odstavce 1 také na základě podnětu právnické nebo podnikající fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací, jíž byla uložena povinnost zřídit a zabezpečit rozhraní pro připojení nástroje detekce v určeném bodě veřejné komunikační sítě a povinnost strpět umístění a provozování tohoto nástroje, nebo Českého

telekomunikačního úřadu. V případě, že orgán nezávislé kontroly na základě kontroly provedené z podnětu právnické nebo podnikající fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací podle věty první zjistí, že činností Vojenského zpravodajství, jíž se podílí na zajišťování obrany státu, došlo k protiprávnímu zásahu do základních práv a svobod, obdrží jím vypracovanou písemnou zprávu[22)] rovněž tato osoba.

(5) Kontrolní řád se na kontrolu činnosti Vojenského zpravodajství podle této části zákona nepoužije.

(6) Na prověřování opatření přijímaných Vojenským zpravodajstvím v zájmu zabezpečování činností, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru, Ministerstvem obrany se použije ustanovení § 41 zákona o zajišťování obrany České republiky obdobně.

§ 16m

Náhrada škody nebo nemajetkové újmy

(1) Každý, komu vznikla škoda nebo nemajetková újma v souvislosti s činnostmi Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu, má právo na jejich náhradu.

(2) Fyzické nebo právnické osobě se nahrazuje také škoda nebo nemajetková újma, která jí vznikla v důsledku realizace opatření přijatých Vojenským zpravodajstvím v zájmu provedení aktivního zásahu směřujícího k odstranění kybernetického útoku nebo hrozby v rámci zajišťování obrany státu v kybernetickém prostoru.

(3) Povinnost státu k náhradě škody nebo nemajetkové újmy podle odstavců 1 a 2 nevznikne, pokud se jedná o škodu nebo nemajetkovou újmu způsobenou fyzické nebo právnické osobě, která vyvolala útok nebo hrozbu.

(4) Za škodu nebo nemajetkovou újmu způsobenou Vojenským zpravodajstvím odpovídá stát. Náhradu škody nebo nemajetkové újmy poskytuje v zastoupení státu Ministerstvo obrany.

---

19) § 2 odst. 1 zákona č. 222/1999 Sb., o zajišťování obrany České republiky.
20) § 3 odst. 10 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.
21) § 2 písm. a) nařízení vlády č. 139/2017 Sb., o plánování obrany státu.
22) § 12g odst. 4 zákona č. 153/1994 Sb.“.

Dosavadní části čtvrtá až šestá se označují jako části pátá až sedmá.

ČÁST DRUHÁ

Změna zákona o zpravodajských službách České republiky

Čl. II

Zákon č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění zákona č. 118/1995 Sb., zákona č. 53/2004 Sb., zákona č. 290/2005 Sb., zákona č. 530/2005 Sb., zákona č. 342/2006 Sb., zákona č. 80/2006 Sb., zákona č. 250/2008 Sb., zákona č. 274/2008 Sb., zákona č. 218/2009 Sb., zákona č. 227/2009 Sb., zákona č. 357/2011 Sb., zákona č. 254/2012 Sb., zákona č. 186/2013 Sb., zákona č. 170/2013 Sb., zákona č. 64/2014 Sb., zákona č. 219/2015 Sb., zákona č. 51/2016 Sb., zákona č. 204/2015 Sb., zákona č. 325/2017 Sb., zákona č. 35/2018 Sb., zákona č. 251/2017 Sb., zákona č. 205/2019 Sb. a zákona č. 227/2019 Sb., se mění takto:

1. V § 2 se dosavadní text označuje jako odstavec 1 a doplňuje se odstavec 2, který včetně poznámek pod čarou č. 10 a 11 zní:

„(2) Vojenské zpravodajství se v rozsahu a způsobem stanoveným zákonem o Vojenském zpravodajství[10)] podílí[11)] na zajišťování obrany České republiky v kybernetickém prostoru.

[10)] Část čtvrtá zákona č. 289/2005 Sb., ve znění pozdějších předpisů.
[11)] Čl. 3 odst. 2 ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky.“.

2. V § 12 odst. 1 se na konci textu věty první doplňují slova „; kontrole kontrolujícími podléhá rovněž činnost Vojenského zpravodajství, kterou se podílí na zajišťování obrany státu v kybernetickém prostoru podle zákona o Vojenském zpravodajství[10)]“.

ČÁST TŘETÍ

Změna zákona o elektronických komunikacích

Čl. III

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění zákona č. 290/2005 Sb., zákona č. 361/2005 Sb., zákona č. 186/2006 Sb., zákona 235/2006 Sb., zákona č. 310/2006 Sb., zákona č. 110/2007 Sb., zákona č. 261/2007 Sb., zákona č. 304/2007 Sb., zákona č. 124/2008 Sb., zákona č. 177/2008 Sb., zákona č. 189/2008 Sb., zákona č. 247/2008 Sb., zákona č. 384/2008 Sb., zákona č. 227/2009 Sb., zákona č. 281/2009 Sb., zákona č. 153/2010 Sb., nálezu Ústavního soudu, vyhlášeného pod č. 94/2011 Sb., zákona č. 137/2011 Sb., zákona č. 341/2011 Sb., zákona č. 375/2011 Sb., zákona č. 420/2011 Sb., zákona č. 457/2011 Sb., zákona č. 468/2011 Sb., zákona č. 18/2012 Sb., zákona č. 19/2012 Sb., zákona č. 142/2012 Sb., zákona č. 167/2012 Sb., zákona č. 273/2012 Sb., zákona č. 214/2013 Sb., zákona č. 303/2013 Sb., zákona č. 181/2014 Sb., zákona č. 234/2014 Sb., zákona č. 250/2014 Sb., zákona č. 258/2014 Sb., zákona č. 318/2015 Sb., zákona č. 378/2015 Sb., zákona č. 222/2016 Sb., zákona č. 298/2016 Sb., zákona č. 183/2017 Sb., zákona č. 194/2017 Sb., zákona č. 225/2017 Sb.,

zákona č. 252/2017 Sb., zákona č. 287/2018 Sb., zákona č. 277/2019 Sb. a zákona č. 311/2019 Sb., se mění takto:

1. Za § 98 se vkládá nový § 98a, který včetně poznámek pod čarou č. 70 a 71 zní:

„§ 98a

(1) Právnická nebo podnikající fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna na základě rozhodnutí vydaného Ministerstvem obrany podle zákona o Vojenském zpravodajství[70)] zřídit a zabezpečit v určených bodech jí zajišťované veřejné komunikační sítě rozhraní pro připojení nástroje detekce umožňujícího provádět cílenou detekci jevů nasvědčujících existenci kybernetického útoku nebo hrozby a jejich identifikaci podle zákona o Vojenském zpravodajství[71)].

(2) Rozhraní pro připojení nástroje detekce musí být technicky uzpůsobeno tak, že neumožňuje předávat obsah detekovaných jevů provozu veřejné komunikační sítě ani komunikaci nástroje detekce s veřejnou komunikační sítí v opačném směru.

(3) Osoba uvedená v odstavci 1 není bez souhlasu Vojenského zpravodajství oprávněna zasáhnout do jím připojeného nástroje detekce nebo jakkoliv omezit jeho funkčnost; to neplatí, pokud provedení zásahu do nástroje detekce nebo omezení jeho funkčnosti je nutné vzhledem k tomu, že v souvislosti s jeho připojením a provozováním je vyvolán stav ohrožující samotný provoz veřejné komunikační sítě, poskytování veřejně dostupné služby elektronických komunikací nebo ohrožující zdraví anebo životy fyzických osob, hrozí-li nebezpečí z prodlení.

(4) Osoba uvedená v odstavci 1 je povinna umožnit Vojenskému zpravodajství na požádání přístup k nástroji detekce umístěnému na jí zajišťované veřejné komunikační síti, přičemž Vojenské zpravodajství musí postupovat tak, aby jeho činností nebyly porušovány podmínky výkonu povinností této osobě uložené zákonem.

(5) Za plnění povinností podle odstavce 1 náleží právnické nebo podnikající fyzické osobě od Vojenského zpravodajství úhrada efektivně vynaložených nákladů. Způsob určení výše efektivně vynaložených nákladů, postup jejich uplatnění a způsob jejich úhrady stanoví prováděcí právní předpis.

(6) Osoba uvedená v odstavci 1, jakož i jiné osoby podílející se na plnění povinnosti podle odstavce 1, jsou povinny zachovávat mlčenlivost o všech skutečnostech souvisejících s připojením a užíváním nástroje detekce. Tato povinnost trvá i poté, kdy tato osoba přestane být osobou podle odstavce 1 nebo osobou podílející se na plnění povinnosti podle věty první.

(7) Povinnost zachovávat mlčenlivost podle odstavce 5 se nevztahuje na podávání informací kontrolujícím, kteří provádějí kontrolu činností Vojenského zpravodajství podle části čtvrté zákona o Vojenském zpravodajství.

[70)] § 16d zákona č. 289/2005 Sb., ve znění pozdějších předpisů.
[71)] § 16a odst. 2 zákona č. 289/2005 Sb., ve znění pozdějších předpisů.“.

2. V § 118 se za odstavec 22 vkládá nový odstavec 23, který zní:

„(23) Právnická nebo podnikající fyzická osoba se jako osoba zajišťující veřejnou komunikační síť nebo veřejně dostupnou službu elektronických komunikací dopustí přestupku tím, že

a) v rozporu s § 98a odst. 1 nezřídí nebo nezabezpečí v určených bodech jí zajišťované veřejné komunikační sítě rozhraní pro připojení nástroje detekce podle rozhodnutí vydaného Ministerstvem obrany,
b) neumožní Vojenskému zpravodajství přístup k nástroji detekce,
c) neoprávněně zasáhne do nástroje detekce nebo omezí jeho funkčnost, nebo
d) poruší povinnost zachovávat mlčenlivost podle § 98a odst. 6.“.

Dosavadní odstavec 23 se označuje jako odstavec 24.

3. V § 118 odst. 24 písm. a) se slova „nebo odstavce 14 písm. ae)“ nahrazují slovy „, odstavce 14 písm. ae) nebo odstavce 23 písm. d)“.

4. V § 118 odst. 24 písm. b) se slova „nebo odstavce 15“ nahrazují slovy „, odstavce 15 nebo odstavce 23 písm. b) anebo c)“.

5. V § 118 odst. 24 písm. c) se slova „nebo 22“ nahrazují slovy „, 22 nebo 23 písm. a) “.

6. V § 119 se za odstavec 6 vkládá nový odstavec 7, který zní:

„(7) Fyzická osoba podílející se na plnění povinností právnické nebo podnikající fyzické osoby zajišťující veřejnou komunikační síť nebo veřejně dostupnou službu elektronických komunikací se dopustí přestupku tím, že poruší povinnost zachovávat mlčenlivost podle § 98a odst. 6.“.

Dosavadní odstavec 7 se označuje jako odstavec 8.

7. V § 119 odst. 8 větě první se číslo „6“ nahrazuje číslem „7“.

8. V § 150 se doplňuje odstavec 7, který zní:

„(7) Ministerstvo obrany vydá vyhlášku k provedení § 98a odst. 5.“.

ČÁST ČTVRTÁ

ÚČINNOST

Čl. IV

Tento zákon nabývá účinnosti patnáctým dnem po jeho vyhlášení.

DŮVODOVÁ ZPRÁVA

OBECNÁ ČÁST

Poznámka k obecné části:
V souladu s čl. 9 odst. 3 Legislativních pravidel vlády jsou dále uvedené kapitoly I. až III. a V. až IX. obsahově rozpracovány v Závěrečné zprávě z hodnocení dopadů regulace k návrhu zákona, následující text je proto nutné vnímat jako základní informaci o vztahu přípravy a stavu předkládaného normativního textu o oblastech, jež jsou označeny názvy příslušných kapitol obecné části důvodové zprávy; tyto kapitoly jsou tedy shrnutím zpracovatelského přístupu a obecným odůvodnění návrhu zákona, kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, a některé další zákony (dále jen „návrh zákona“).

I. Zhodnocení platného právního stavu, včetně zhodnocení současného stavu ve vztahu k zákazu diskriminace a ve vztahu k rovnosti mužů a žen

I. 1 Zhodnocení východisek pro předložení návrhu zákona

Vláda České republiky svým usnesením ze dne 25. května 2015 č. 382 schválila Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020. Jedná se o strategii státu pro zajišťování kybernetické bezpečnosti, v rámci které byl Vojenskému zpravodajství jako součásti Ministerstva obrany uložen úkol připravit návrh normativního řešení vytvoření podmínek kybernetické obrany České republiky

Strategie přisuzuje odpovědnost za plnění Vojenskému zpravodajství v případě 8 úkolů (na dalších 20 se spolupodílí). Základní úkol spočíval ve vytvoření Národního centra kybernetických operací (NCKO) – původní název byl Národní centrum kybernetických sil, které má provádět široké spektrum operací v kyberprostoru a aktivity nutné pro zajištění kybernetické obrany ČR. Stěžejní úkol pro Vojenské zpravodajství však spočívá v plném zajišťování kybernetické obrany skrze kooperaci NCKO s Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB), který vykonává i roli vládního CERT[1)], národním CERT a ostatními pracovišti typu CERT/CSIRT. Pro potřeby plné funkčnosti NCKO byl pro Vojenské zpravodajství stanoven i úkol připravit návrh nutných legislativních změn.

Před stanovením těchto úkolů se důkladně vyhodnotil stávající i žádoucí právní a skutkový stav. Těchto jednání se účastnili představitelé NBÚ (dnešního NÚKIB), zpravodajských služeb a ostatních relevantních institucí. Výsledkem byla koncepce systému kybernetické bezpečnosti ČR v gesci nově vzniklého NÚKIB a jako nejvhodnější institucí pro zajišťování kybernetické obrany bylo určeno právě Vojenské zpravodajství.

Na plnění jednotlivých úkolů začalo Vojenské zpravodajství pracovat již v průběhu roku 2015 vytvořením studie proveditelnosti vybudování NCKO (samotné centrum následně vzniklo v roce 2016) a prvním návrhem nutných legislativních a organizačních změn.

Výsledný legislativní návrh Ministerstva obrany byl v roce 2016 připraven ve spolupráci s MV, NBÚ, ÚZSI, BIS a ČTÚ. Prošel připomínkovým řízením a vláda jej schválila na svém jednání dne 5. října 2016 usnesením č. 870. V rámci Poslanecké sněmovny byl tento návrh ve

[1)] Computer Emergency Response Team – „Skupina pro reakci na počítačový stav nouze“.

druhém čtení výbory pro obranu i bezpečnost navržen ke schválení (ve znění pozměňovacích návrhů). Z důvodu předčasného rozpuštění sněmovny však nebyl zákon přijat.

Legislativní proces k návrhu doprovázela široká diskuze, neboť vyvstaly otázky ohledně dostatečných záruk pro ochranu soukromí a osobních údajů fyzických osob. Jako problémový pak byl shledán rovněž způsob řešení svěření provádění kybernetické obrany do výlučné působnosti Vojenskému zpravodajství mimo rámec jemu svěřené působnosti zpravodajské služby, tedy mimo rámec činností prováděných podle § 2 zákona č. 153/1994 Sb., o zpravodajských službách České republiky, jímž je stanoveno, že zpravodajské služby jsou státní orgány pro „získávání, shromažďování a vyhodnocování informací důležitých pro ochranu ústavního zřízení, významných ekonomických zájmů, bezpečnost a obranu České republiky“.

Stávající návrh zákona je proto v zájmu splnění úkolu uloženého Ministerstvu obrany usnesením vlády České republiky ze dne 25. května 2015 č. 382, ale především k naplnění vládou stanovené koncepce zajišťování obrany České republiky v kybernetickém prostoru, za níž nese odpovědnost, předkládán opakovaně, avšak významně přepracován; rovněž na tomto vypracování znění předkládaného návrhu zákona se podílely všechny zpravodajské služby, NÚKIB a NBÚ.

V souvislosti s přípravou návrhu zákona byla velká pozornost věnována také ochraně základních lidských práv a svobod a možnostem provedení krátkodobých a přiměřených zásahů do nich v případě zabezpečování obrany České republiky v kybernetickém prostoru, resp. pro případy provádění cílené detekce jevů nasvědčujících existenci kybernetického útoku nebo hrozby, jejich identifikace a vyhodnocování. Návrh zákona zohledňuje požadavky na ochranu ústavně garantovaných práv na ochranu soukromí a informačního sebeurčení, stejně jako na ochranu před neoprávněnými zásahy do osobních údajů. V tomto smyslu byly návrhem zákona vytvořeny potřebné záruky fyzickým osobám tak, aby možnost případného zásahu do této sféry vždy odpovídala ústavně aprobovanému veřejnému zájmu na zajišťování obrany České republiky, kterému koneckonců odpovídá také jedna ze základních povinností státu (k tomu viz čl. 1 ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky - „Zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot je základní povinností státu.“). Ve spolupráci s Ministerstvem spravedlnosti byl návrh zákona podroben pečlivému vyhodnocení jeho souladu s existující judikaturou Evropského soudu pro lidská práva v této oblasti, stejně jako byla zohledněna judikatura, jejímž zdrojem jsou soudy české a pro danou oblast zejména pak soud ústavní.

Vypracovaný návrh v nutném rozsahu doplňuje systém obecné (kybernetické) bezpečnosti a obecné obrany státu takovým způsobem, že se jedná o řešení navazující na limity působnosti ostatních státních orgánů, především NÚKIB, armády, zpravodajských služeb a Policie ČR. To vše bez nutnosti vyhlášení mimořádných stavů či omezení běžného života občanů.

Pro zhodnocení východisek pro potřeby předložení navrhovaného zákona je vhodné zdůraznit, že kybernetická bezpečnost představuje aktivitu státu, kterou chrání informační a komunikační systémy (sítě, systémy, počítače, databáze, datová centra atd.) napříč nejrůznějšími odvětvími společnosti. V tomto smyslu je koncept kybernetické bezpečnosti obecného charakteru a zahrnuje velké množství preventivních, proaktivních a reaktivních činností, které provádí především gestor kybernetické bezpečnosti v ČR – NÚKIB.

V některých případech však může docházet k tak závažným kybernetickým incidentům, resp. útokům (např. sofistikované útoky ze zahraničí cíleně určené k poškození státu), že na ně nemůže NÚKIB adekvátně reagovat. V takových případech je mnohdy potřeba aktivovat prvky obrany, potažmo nasazení aktivních kybernetických kapacit i vojenského charakteru, které NÚKIB, jakožto ústřednímu správnímu úřadu nepřísluší.

NÚKIB a jeho specializované pracoviště vládní CERT má v těchto krizových situacích odlišnou roli, analogickou se zdravotnickými zařízeními v dobách válečného konfliktu. Vládní CERT se zaměřuje na oběti kybernetických útoků a incidentů v České republice a snaží se jim v dobách krize pomáhat a podporovat je v opětovném zabezpečení svých informačních a komunikačních systémů. Při boji s kybernetickými hrozbami se tedy nezaměřuje přímo na útočníka. Působí proti němu především pomocí přijímání bezpečnostních opatření u subjektů, které chrání.

Činnosti, které by mělo NCKO vykonávat oproti tomu budou značně rozdílné od nastavování bezpečnostních standardů, kontrolního dozoru, ale i administrativně-právního vynucování jejich dodržování. Obrana státu v kybernetickém prostoru musí být komplexním systémem opatření, která umožňují, aby stát byl schopen aktivně odvrátit nejzávažnější kybernetické útoky ohrožující jeho základní fungování a podstatu. Zásadní roli zde hrají schopnosti umožňující aktivně zasáhnout proti kybernetickému útoku, přičemž za současného stavu žádná státní instituce pro to nedisponuje adekvátními oprávněními. Bylo proto nutné připravit legislativní podmínky umožňující odhalit, identifikovat a vyhodnotit kybernetický útok a v případě nutnosti aktivně odvrátit ty nejzávažnější z nich.

I. 2 Zhodnocení platného právního stavu

Cílem návrhu zákona je i v tomto případě umožnit splnění úkolu C. 9.01 uvedeného Akčního plánu, tedy zajistit podmínky výkonu kybernetické obrany, kterou doposud ve svém důsledku žádný státní orgán nevykonává, což bylo vyhodnoceno jako systémový nedostatek, a vybudování Národního centra kybernetických sil v rámci Vojenského zpravodajství.

Po vyhodnocení právního a skutkového stavu možností implementace sledovaného cíle do právního řádu České republiky bylo konstatováno, že normativní řešení vládou České republiky představuje promítnutí předmětného zadání do těchto právních předpisů:

- zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, a
- zákon č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů.
- zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

Při přípravě návrhu zákona bylo nutné zejména uspokojivě vyřešit postavení Vojenského zpravodajství jako jedné ze zpravodajských služeb České republiky, jemuž vláda České republiky přiznala roli při zajišťování obrany České republiky, přestože nepatří mezi ozbrojené síly České republiky.

Podle § 5 odst. 4 zákona č. 153/1994 Sb. sice zpravodajské služby mohou plnit také další úkoly, pokud tak stanoví zvláštní zákon nebo mezinárodní smlouva, jíž je Česká republika vázána, je však zřejmé, že i takto ukládané úkoly nemohou překročit zákonný rámec účelu, k němuž jsou zpravodajské služby České republiky zřizovány (viz § 2 zákona č. 153/1994 Sb.).

Tento stav však neznamená, že úkol zadaný vládou České republiky je neřešitelný a že – aniž by byly porušeny požadavky na dodržení ústavnosti právního řádu – by bylo nemožné předpokládanou zákonnou úpravu zpracovat a předložit ji k posouzení do legislativního procesu.

K tomu, aby bylo možné při dodržení ústavnosti realizovat vládou České republiky uložené úkoly, je nutné detailně vyhodnotit existující právní rámec zajišťování obrany České republiky jako jedné ze základních funkcí státu a určení subjektů, které jsou k výkonu souvisejících činností zmocněny.

Základní – a pro řešení zcela rozhodující – je úprava podmínek zajišťování bezpečnosti České republiky, provedená ústavním zákonem č. 110/1998 Sb., o bezpečnosti České republiky, ve znění ústavního zákona č. 300/2000 Sb. Podle čl. I tohoto ústavního zákona je „zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot základní povinností státu". Podle čl. 3 odst. 1 citovaného ústavního zákona jsou výkonem této povinnosti státu pověřeny ozbrojené síly, ozbrojené bezpečnostní sbory, záchranné sbory a havarijní služby, čímž je provedena limitace postavení Vojenského zpravodajství pro zajišťování „kybernetické obrany", neboť ustanovení § 3 odst. 1 a 2 zákona č. 219/1999 Sb., o ozbrojených silách České republiky, stanoví, že „k zajišťování své bezpečnosti vytváří Česká republika ozbrojené síly, které se člení na armádu, Vojenskou kancelář prezidenta republiky a Hradní stráž".

Pro předkládanou úpravu pak bylo důležité vyhodnotit také to, že „kybernetická obrana" v rámci zajišťování obrany (tedy vnější bezpečnosti) České republiky není specifická, souběžně působící struktura nad standardní obranou státu, ale její nedílná součást, byť vlivem rozvoje moderních komunikačních technologií a služeb součást novější a specificky technologicky vybavená a zejména působící v nestandardním prostředí sítí a služeb elektronických komunikací. I přes tato specifika je však na kybernetickou obranu nutno pohlížet jako na standardní součást obrany státu ve smyslu § 2 odst. 1 zákona č. 222/1999 Sb., o zajišťování obrany České republiky, tedy jako na součást „souhrnu opatření k zajištění svrchovanosti, územní celistvosti, principů demokracie a právního státu, ochrany života obyvatel a jejich majetku před vnějším napadením". Obrana státu zahrnuje výstavbu účinného systému obrany státu, přípravu a použití odpovídajících sil a prostředků a účast v kolektivním obranném systému a v tomto smyslu rovněž kybernetická obrana musí podléhat jednotnému koncepčnímu řízení, plánování a strategii, stejně jako platí, že v uvedeném smyslu za její přípravu a zajišťování odpovídá vláda České republiky (§ 4 zákona č. 222/1999 Sb.).

Současný právní řád však umožňuje, aby se Vojenské zpravodajství na zajišťování „obrany státu v kybernetickém prostoru" podílelo, navzdory tomu, že není ozbrojenou silou a že rámec účelu zřízení zpravodajských služeb jako státních orgánů pro „získávání, shromažďování a vyhodnocování informací důležitých pro ochranu ústavního zřízení, významných ekonomických zájmů, bezpečnost a obranu České republiky" by mohl sám o sobě aktivní podíl na zajišťování obrany České republiky vylučovat. Nositelem této možnosti je ustanovení čl. 3 odst. 2 ústavního zákona č. 110/1998 Sb., které stanoví, že „státní orgány, orgány územních samosprávných celků a právnické a fyzické osoby jsou povinny se podílet na zajišťování bezpečnosti České republiky; rozsah povinností a další podrobnosti stanoví zákon.". **Navrhovaná právní úprava tedy není ničím jiným, než provedením již platné zákonné úpravy tím, že stanoví rozsah povinností Vojenského zpravodajství, kterými se do budoucna bude podílet na zajišťování obrany státu, a to s konkrétním vymezením tohoto podílu vzhledem k zajišťování obrany státu v kybernetickém prostoru.** Stejně tak jsou

návrhem zákona stanovovány podrobnosti, jimiž se upřesňují podmínky výkonu takto Vojenskému zpravodajství ukládaných povinností, a to včetně stanovení vnějších vazeb garantujících začlenění kybernetické obrany do celého kontextu zajišťování obrany a bezpečnosti České republiky, stanovení garancí pro ochranu soukromí a osobních údajů pro oblast detekování a vyhodnocování definovaných jevů v oblasti veřejných komunikačních sítí a veřejně dostupných služeb elektronických komunikací a kontrolních mechanismů poskytujících záruky proti zneužití takto Vojenskému zpravodajství svěřených pravomocí nebo případnému zabránění svévolného jednání tam, kde je nutné důsledně zvažovat proporcionalitu mezi prosazením bytostného zájmu státu a mezi ústavně garantovanými základními právy a svobodami fyzických osob.

Pokud tedy bylo zajištěno právní řešení předpokladů pro to, aby Vojenské zpravodajství bylo plně legitimováno pro výkon činností, jimiž se podílí na zajišťování obrany České republiky v kybernetickém prostoru, je zřejmé, že veškeré další legislativní práce jsou směřovány nikoliv využitím analogií s postupy Vojenského zpravodajství jako zpravodajské služby, ale jsou přímo určeny „zmocněním" pro stanovení podmínek, jimiž se má příslušný státní orgán podílet na zajišťování obrany České republiky, obsaženém v čl. 3 odst. 2 ústavního zákona č. 110/1998 Sb. v tomto znění: „*Státní orgány, orgány územních samosprávných celků a právnické a fyzické osoby jsou povinny se podílet na zajišťování bezpečnosti České republiky. Rozsah povinností a další podrobnosti stanoví zákon*.".

I. 3 Zhodnocení současného stavu ve vztahu k zákazu diskriminace a ve vztahu k rovnosti mužů a žen

Právní úprava podmínek zajišťování jedné ze základních povinností státu při zajištění svrchovanosti a územní celistvosti České republiky, ochrany jejích demokratických základů a ochrany životů, zdraví a majetkových hodnot je v současné době upravena systémem právních předpisů souhrnně označovaných jako tzv. „systém branné legislativy", který byl pro každou ze svých součástí, ale i jako celek, podroben důkladné analýze, zda jím nastavované instituty a procesy odpovídají zásadám vyloučení diskriminace a zachování principů rovnosti žen a mužů. To se týká podmínek zajišťování obrany státu s tím, že ve vztahu k Vojenskému zpravodajství platí nepochybně to samé, avšak pro existující právní úpravu, která se zabývá regulací činnosti Vojenského zpravodajství jako zpravodajské služby, nikoliv jako státního orgánu, který se podílí na zajišťování obrany státu - v této oblasti se navrhuje právní úprava zcela nová, která však princip nediskriminace důsledně dodržuje, přičemž je třeba konstatovat, že nebyly zjištěny důvody, které by objektivně ospravedlňovaly porušení této zásady.

II. Odůvodnění hlavních principů navrhované úpravy, včetně dopadů navrhovaného řešení ve vztahu k zákazu diskriminace a ve vztahu k rovnosti mužů a žen

Základním zpracovatelským principem pro tento návrh je vytvořit právní úpravu zcela odpovídající zásadám demokratického právního státu, tedy při dosažení sledovaného účelu stanovení rozsahu činností Vojenského zpravodajství, jimiž se bude podílet na zajišťování obrany České republiky v kybernetickém prostoru, a to při zachování záruk ochrany jednotlivce před projevy libovůle ze strany veřejné moci tak, jak je uvedeno v kapitole I. 2 části I. obecné důvodové zprávy. Návrhem zákona je tak předkládána právní úprava zcela ústavně slučitelná, jednoznačná a pro uživatele předvídatelná, která vytváří jak potřebné podmínky významné podpory zajišťování kybernetické obrany České republiky a potřebné vazby mezi státními

orgány tam, kde detekované a identifikované jevy v kybernetickém prostoru budou vypovídat o přesahu oblasti obrany České republiky a oblasti zajišťování její vnitřní bezpečnosti, ale také dostatečné záruky pro stanovení povinností a ochranu práv třetích osob. V této oblasti je v potřebném rozsahu a při využití vhodných a nejméně invazivních prostředků právní úprava navržena tak, aby respektovala práva a právem chráněné zájmy jak provozovatelů veřejných komunikačních sítí a veřejně dostupných služeb elektronických komunikací, tak ochrany základních práv a svobod fyzických osob pro oblast ochrany soukromí a osobních údajů, a to při zachování základního účelu navrhované regulace, tedy vytvořit pro stát dostatečně efektivní podmínky, jejichž prostřednictví naplňuje svoji základní povinnost, tedy zajišťování obrany České republiky.

Návrh zákona se přitom významně odklonil od koncepce návrhu zákona, který projednala a schválila vláda České republiky dne 5. října 2016 usnesením č. 870, a to především v postavení Vojenského zpravodajství při výkonu činností, k nimž bylo pověřeno za účelem zajišťování obrany České republiky v kybernetickém prostoru. Návrh zákona již nestaví Vojenské zpravodajství do role „nestandardní součásti" systému zajišťování obrany státu, když plně respektuje zákonnou úpravu provedenou zákonem č. 219/1999 Sb., o ozbrojených silách České republiky, ve znění pozdějších předpisů, která jeho ustanovením § 3 odst. 1 stanoví, že „k zajišťování své bezpečnosti (*v daném kontextu vnější bezpečnosti, tedy obrany)* vytváří Česká republika ozbrojené síly"; v odstavci 2 téhož ustanovení je pak uvedeno, že „ozbrojené síly České republiky se člení na armádu, Vojenskou kancelář prezidenta republiky a Hradní stráž". Návrh zákona svou koncepcí vylučuje, že by mohl být považován za nepřímou novelizaci zákona č. 219/1999 Sb., když jednoznačně určuje, jaké je postavení Vojenského zpravodajství v rámci zajišťování obrany České republiky v kybernetickém prostoru.

V této souvislosti bylo nutné se vypořádat s tím, že provádění kybernetické obrany svou povahou přesahuje obecně vymezené úkoly Vojenského zpravodajství jako zpravodajské služby, neboť provádění kybernetické obrany by alespoň v určitém rozsahu bylo aktivní činností přesahující rámec zabezpečování informací. Zákon o zpravodajských službách sice těmto službám umožňuje výkon dalších činností, pokud je ukládá jiný zákon, avšak tyto činnosti nesmí překročit rámec činností zpravodajských obecně vymezených v zákoně o zpravodajských službách, tedy rámec „*získávání, shromažďování a vyhodnocování informací důležitých pro ochranu ústavního zřízení, významných ekonomických zájmů, bezpečnost a obranu České republiky"*. K tomu je využito čl. 3 odst. 2 ústavního zákona č. 110/1998 Sb. tak, jak je uvedeno v kapitole I. Toto řešení postavení Vojenského zpravodajství koresponduje s účelem zadání vyplývajícím z usnesení vlády České republiky ze dne 25. května 2015 č. 382, kterým vláda schválila Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 a současně uložila Ministerstvu obrany úkol předložit návrh normativního řešení vytvoření podmínek kybernetické obrany České republiky.

S uvedenou úpravou je pak nedílně spojená úprava začlenění zajišťování obrany státu v kybernetickém prostoru do celkového systému obrany a bezpečnosti České republiky, a to jednak v rámci plánování obrany státu Ministerstvem obrany, jednak v nastavení vazeb vůči dalším nositelům povinností při zajišťování obrany a bezpečnosti státu tak, aby byla zajištěna komplexní ochrana kybernetického prostoru ve všech sledovaných aspektech a za tímto účelem využito synergického účinku společného působení sil a prostředků Armády České republiky a Národního úřadu pro kybernetickou a informační bezpečnost.

Navrhovaná úprava pak v sobě při zajištění věcných aspektů kybernetické obrany současně vychází z nezbytnosti zajistit proporcionalitu mezi svěřenými nástroji a opatřeními

jejího výkonu a dostatečnými zárukami proti jejich zneužití (pro jiné účely nebo proti nežádoucímu osobnímu nebo časovému rozsahu jejich účinků). Připravovaný právní rámec proto poskytuje záruky bránící jejímu zneužití, a to jednak v rámci jejího začlenění do podmínek a systému zajišťování obrany České republiky, jednak jednoznačným a předvídatelným nastavením rozsahu a podmínek detekování a vyhodnocování definovaných jevů v kybernetickém prostoru, pro které platí přísnější mantinely a právní limity, než je tomu u zpravodajské činnosti.

Navrhovaná úprava s vědomím toho, že se jedná o oblast mimořádně citlivou z hlediska nastavení vztahů mezi státem a provozovateli sítí a služeb elektronických komunikací, ale především z hlediska případných zásahů do soukromí nebo práva na ochranu osobních údajů, řeší jednoznačným, předvídatelným způsobem také pravidla pro ukládání povinností uvedeným podnikatelům i zásady, jimiž musí být zajištěna garance uvedených lidských práv, popřípadě na jejichž základě mohou být tato práva prolomena v zájmu zajištění plnění základních povinností státu s přihlédnutím k proporcionalitě těchto zájmů a ochraně demokratických principů a vyloučení svévole užití svěřených oprávnění nad stanovený zákonný rámec.

Návrhem zákona je prováděna úprava, jejímž účelem není přímo zasahovat do základních lidských práv a svobod, ale v kontextu závěrů Evropské soudu pro lidská práva skýtá potenciál pro to, že by se tak v některých případech mohlo stát (k tomu viz výše – omezení základních lidských práv a svobod v zájmu zajišťování obrany státu). Návrh zákona proto pro tyto případy jednoznačně respektuje nároky, které jak judikatura Ústavního soudu České republiky, tak judikatura Evropského soudu pro lidská práva klade na zpracování právních předpisů, u kterých se předpokládá nebo lze dovodit případný zásah do základních lidských práv a svobod. Navrhovaná legislativní opatření omezující rozsah ochrany základních lidských práv a svobod, v daném případě práva na soukromí a informační sebeurčení a práva na ochranu osobních údajů, vychází ze skutečnosti, že toto omezení je objektivně nezbytné, přiměřené a úměrné opatření pro zajištění obrany České republiky, přičemž je vždy využito v nejnižší možné míře.

Navrhovaná úprava proto striktně pro tato omezení sleduje vládou České republiky zadaný účel zajišťování obrany České republiky v kybernetickém prostoru a vymezuje rozsah opatření, a to včetně doby jejich působení, přezkumu skutečností vedoucích k zásahu do základních práv a stanovením několikastupňové kontroly na úrovni vládních institucí, ale i na nich nezávislého subjektu.

III. Vysvětlení nezbytnosti navrhované právní úpravy v jejím celku

Formálním důvodem zpracování návrhu zákona je – jak je již uvedeno v kapitole I. – usnesení vlády České republiky ze dne 25. května 2015 č. 382, kterým vláda schválila Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 a současně uložila Ministerstvu obrany úkol předložit návrh normativního řešení vytvoření podmínek kybernetické obrany České republiky. Tento úkol i přes ukončený legislativní proces k původnímu návrhu zákona trvá, a to s akcentací veřejného zájmu na zajištění kompletní bezpečnosti kybernetického prostoru, v němž spolu s dynamickým nárůstem technologií vzrůstá jednak rozsah služeb a nabídek uživatelského prostředí, ale současně také rizika jeho zneužití. Vláda České republiky svým usnesením současně do jisté míry určila jednoho z hlavních nositelů zajišťování kybernetické obrany, i když je jí beze sporu stále nutné vnímat jako součást obrany státu jako takové, včetně uplatnění zásad odpovědnosti za její přípravu a zajišťování (*podle § 4 zákona č. 222/1999 Sb. je jejím nositelem vláda České republiky*) nebo její plánování [*podle § 6 odst. 1 písm. b) a c) zákona č. 222/1999 Sb. je jejím nositelem*

Ministerstvo obrany, které „odpovídá za proces plánování obrany státu a koordinuje jeho přípravu a za plánování a zabezpečení operační přípravy státního území, doplňování ozbrojených sil a mobilizaci ozbrojených sil“].

Právním důvodem pro zcela nevyhnutelné zajištění účelu sledovaného usnesení vlády České republiky ze dne 25. května 2015 č. 382 formou přijetí zákona je provedená věcná a právní analýza možností řešení dané věci tak, jak je nastíněna v kapitole I., která prokázala, že pro splnění všech věcných a organizačních nároků na splnění vládou České republiky zadaného úkolu je naprosto nevyhnutelné zohlednit také veškeré aspekty legitimity výkonu předpokládaných činností, a to včetně mantinelů možností omezení základních práv a svobod, což nelze provést jinak, než provedením zákonné úpravy *(k tomu viz čl. 3 odst. 2 ústavního zákona č. 110/1998 Sb. a § 53 odst. 6 zákona č. 222/1999 Sb.).* Nezbytnost přijetí právní úpravy je tedy vyvolána požadavkem na její provedení vyplývající z jiných právních předpisů, v daném případě ústavním zákonem č. 110/1998 Sb. a zákonem č. 222/1999 Sb., a to s využitím možnosti „pověření“ Vojenského zpravodajství jako státního orgánu s postavením jednotné ozbrojené zpravodajské služby České republiky podílením se na zajišťování obrany České republiky výlučně za podmínek stanovených v čl. 3 odst. 2 ústavního zákona č. 110/1998 Sb.; návrhem zákona jsou tedy ukládány související povinnosti a stanovován jejich rozsah, stejně jako podrobnosti jejich výkonu, a rovněž jsou stanovována opatření k zajištění ochrany základních lidských práv a svobod.

IV. Zhodnocení souladu navrhované právní úpravy s ústavním pořádkem České republiky

Potřeba navrhované úpravy vyplývá ze skutečností uvedených v kapitole I., když je zřejmé, že návrh zákona je zákonem vydávaným za účelem sledovaným v čl. 3 odst. 2 ústavního zákona č. 110/1998 Sb. a formálně sleduje i zmocnění pro naplnění tohoto účelu stanovené týmž ustanovením. Soulad s právními předpisy souboru tzv. branné legislativy byl zajištěn analýzou vztahu návrhu zákona k zákonu č. 222/1999 Sb. a k zákonu č. 219/1999 Sb.

Při zpracování návrhu byla rovněž důsledně respektována zásada, že státní moc lze uplatňovat jen v případech, v mezích a způsoby, které stanoví zákon.

Je nicméně nezbytné, aby samotný výkon takové obrany, tedy výkon státní moci, byl normován zákonem, a to zejména v případech, kdy by při výkonu takové obrany bylo zasahováno do základních lidských práv a svobod. Ústava České republiky vyžaduje, aby působnost správních úřadů, a obecně vzato i jiných státních orgánů, byla stanovena zákonem. Z tohoto důvodu jsou návrhem zákona Vojenskému zpravodajství pro činnosti vykonávané ve prospěch zajišťování kybernetické obrany stanovovány meze, které garantují vyloučení svévole při užití svěřených pravomocí; navrhovanou úpravu je také nutné vnímat v kontextu důsledného oddělení výkonu zpravodajské činnosti a činností, jimiž se Vojenské zpravodajství bude podílet na zajišťování obrany České republiky v kybernetickém prostoru, s jediným překryvem využíváním informací, které díky své zpravodajské činnosti získá a které vypovídají o skutečnostech ohrožujících důležité zájmy státu.

V zájmu zajištění jednoznačných a odpovídajících předpokladů pro provádění detekce a identifikace vytipovaných jevů v rámci provozování veřejných sítí elektronických komunikací nebo poskytování veřejně dostupných služeb elektronických komunikací jsou návrhem zákona stanovena pravidla, která umožní Ministerstvu obrany na návrh Vojenského

zpravodajství ukládat povinnosti provozovatelům veřejných komunikačních sítí nebo poskytovatelům veřejně dostupných služeb elektronických komunikací; takto ukládaná povinnost je však provázaná s předcházející analytickou činností Vojenského zpravodajství, ale také komunikací s příslušnou podnikající fyzickou nebo právnickou osobou provozující veřejnou síť elektronických komunikací nebo poskytující veřejně dostupnou službu elektronických komunikací tak, aby ukládaná povinnost byla v co nejmenší kolizi s právy a povinnostmi těchto osob.

I v tomto případě je úprava provedena tak, aby respektovala ústavní zásady, v daném případě zásadu, „že nikdo nesmí být nucen činit, co zákon neukládá“; proto je zákonem upraveno, jaké povinnosti budou právnickým a fyzickým osobám v souvislosti s plněním úkolů kybernetické obrany uloženy a pravidla pro stanovení, za jakých podmínek a v jaké lhůtě má být povinnost splněna, stejně jako časové období, ve kterém je povinna činnost Vojenského zpravodajství, jíž se bude podílet na zajišťování obrany České republiky, strpět. Formálně má uložení povinnosti podobu rozhodnutí vydaného ve správním řízení a uvedené skutečnosti jsou stanoveny jako nedílné součásti jeho obsahu.

Navrhovaný zákon nemá umožnit Vojenskému zpravodajství zasáhnout do základních práv a svobod a soukromé sféry osob ve větší míře, než je to nezbytné pro plnění funkce státu zajistit jeho obranu, a to navíc s přihlédnutím k tomu, že pro tyto případy nebude vykonávat působnost zpravodajské služby. Vojenské zpravodajství nově vystupuje v roli státního orgánu podílejícího se na zajišťování obrany České republiky v kybernetickém prostoru. V kontextu uvedeného je třeba vnímat návrhem zákona konstituované činnosti Vojenského zpravodajství jako nedílnou součást zajišťování obrany České republiky, a tedy režimově podřízené zákonu č. 222/1999 Sb. se stanovením úpravy specifické úpravy tam, kde se jedná o zcela mimořádné podmínky zajišťování obrany České republiky vzhledem ke zvláštnostem kybernetického prostoru.

Návrh zákona primárně nepřepokládá trvalé ani průběžné zasahování do základních lidských práv a svobod, chráněných zejména ustanoveními čl. 7 a čl. 10 odst. 2 a 3 Listiny základních práv a svobod, čl. 8 Evropské úmluvy o ochraně lidských práv a základních svobod a čl. 17 Mezinárodního protokolu o občanských a politických právech, i když ve smyslu dynamicky se vyvíjející judikatury Evropského soudu pro lidská práva nelze potenciální možnost takového zásahu spolehlivě vyloučit (viz zejména *Benedik proti Slovinsku*, č. 62357/14, rozsudek ze dne 24. dubna 2018, kde ESLP dovodil, že také informace spjaté s IP adresou obsahují řadu informací o osobě, která ji využívá, a proto spadají pod široký pojem soukromého života ve smyslu čl. 8 Evropské úmluvy).

Evropský soud pro lidská práva však současně připustil, že jím stanovené přísné standardy, které se uplatňují v případech tajného sledování osob prostřednictvím telefonních odposlechů (viz zejména *Lambert proti Francii*, č. 23618/94, rozsudek ze dne 24. srpna 1998; *Amann proti Švýcarsku*, č. 27798/95, rozsudek ze dne 16. února 2000; *Malone proti Spojenému království*, č. 8691/79, rozsudek ze dne 2. srpna 1984; *Huvig proti Francii*, č. 11105/84, rozsudek ze dne 24. dubna 1990; *Pruteanu proti Rumunsku*, č. 30181/05 a další, rozsudek ze dne 3. února 2015), prostorové odposlechy (*Khan proti Spojenému království*, č. 35394/97, rozsudek ze dne 12. května 2000; *Bykov proti Rusku*, č. 4378/02, rozsudek velkého senátu ze dne 10. března 2009; *Savovi proti Bulharsku*, č. 7222/05, rozsudek ze dne 27. listopadu 2012; *P.G. a J.H. proti Spojenému království*, č. 44789/98, rozsudek ze dne 25. září 2001) či prolamováním listovního tajemství a zásahy do elektronické korespondence (*Klass a další proti Německu*, č. 5029/71, rozsudek pléna ze dne 6. září 1978; *Copland proti Spojenému království*,

č. 62617/00, rozsudek ze dne 3. dubna 2007; *Kennedy proti Spojenému království*, č. 26839/05, rozsudek ze dne 18. května 2010) se neuplatní se stejnou tvrdostí na jiné techniky sledování, které svou povahou zasahují do soukromého života dotčených osob v nesrovnatelně nižší intenzitě (viz zejména *Uzun proti Německu*, č. 35623/05, rozsudek ze dne 2. září 2010, § 66, kde se ESLP zabýval sledováním vozidla prostřednictvím GPS). V těchto případech bude proto zpravidla postačovat, pokud právní úprava stanoví nižší úroveň záruk proti svévoli (srov. *a contrario Szabó a Vissy proti Maďarsku*, č. 37138/14, rozsudek ze dne 12. ledna 2016; *Roman Zakharov proti Rusku*, č. 47143/06, rozsudek velkého senátu ze dne 4. prosince 2015).

Cílem detekce a identifikace definovaných jevů v kybernetickém prostoru v žádném případě není narušovat soukromí nebo tajemství zpráv a – to je třeba zdůraznit – rozhodně neopravňují Vojenské zpravodajství sledovat obsah komunikace konkrétních osob (pro tento typ jednání nadále a výhradně platí pravidla pro použití zpravodajské techniky), ale pouze signalizovat určité přesně definované negativní jevy související s kybernetickým prostorem (k nástrojům detekce blíže viz zvláštní část důvodové zprávy). Ve smyslu shora citované judikatury ESLP proto právní úprava detekce a identifikace definovaných jevů v kybernetickém prostoru nemusí splňovat všechny přísné požadavky, na nichž by bylo třeba bezvýhradně trvat v případě jiných skutečně invazivních prostředků tajného sledování. Bylo-li by na základě těchto signálů nutné zaměřit se na konkrétní osoby a jejich chování v kybernetickém prostoru, bude tak činěno v rozsahu povolení na zpravodajskou techniku tak jako dosud. Platná právní úprava přitom skýtá záruky proti svévoli, které lze ve světle citované judikatury považovat za dostatečné. Provádění detekce a identifikace definovaných jevů je přitom zásadní pro zajišťování činností, jimiž se Vojenské zpravodajství má podílet na zajišťování obrany České republiky v kybernetickém prostoru, protože není jiná možnost včas a v potřebném rozsahu identifikovat určité jevy, jež mohou nasvědčovat přípravě kybernetického útoku či dokonce již jeho průběhu.

Pro každý zásah do základních práv a svobod platí obecná zásada, že k němu může dojít pouze za podmínky, že ochrany tohoto jiného zájmu nelze dosáhnout šetrnějším způsobem. Omezení, resp. zásah do těchto práv může být připuštěn pouze za účelem ochrany jiného zájmu, který bude shledán v konkrétní věci důležitějším. Evropská úmluva dovoluje zásahy do práva na respektování soukromého a rodinného života, obydlí a korespondence v případech, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.

Ústavní soud České republiky používá k poměření těchto zájmů tzv. test proporcionality (viz např. nález Ústavního soudu České republiky Pl. ÚS 24/10 ze dne 23. března 2011 nebo Pl. ÚS 45/17 ze dne 22. května 2019). Při něm jsou postupně posuzována tři kritéria. Prvním je **kritérium vhodnosti**, tj. odpověď na otázku, zdali institut, omezující určité základní právo, umožňuje dosáhnout sledovaný cíl (ochranu jiného základního práva). Zde je potřeba si uvědomit, že návrh zákona tak, jak je formulován, nepochybně povede ke zvýšení míry bezpečnosti České republiky a jejích občanů, a to při deklarování jednoznačných, předvídatelných a vymahatelných pravidel v souvislosti s tím vytvářeného systému ochrany základních lidských práv a svobod, včetně stanovených mantinelů pro případy, kdy tato nedistributivní[2)] práva a mezinárodní závazky České republiky mohou být omezeny.

[2)] Srov. oponentní posudek Pavla Holländera k nálezu pléna Ústavního soudu ze dne 3.4.1996, č.j. Pl.ÚS 32/95, 112/1996 Sb., N 26/5 SbNU 215, dostupný z: www.nalus.usoud.cz: „Ústavní úprava postavení jedince ve společnosti obsahuje ochranu individuálních práv a svobod, jakož i ochranu veřejných statků (public goods,

Dosavadní zkušenosti ukazují, že kybernetické útoky se stávají stále závažnější hrozbou, přičemž je nezbytné, aby stát byl pokud možno připraven jim čelit, což lze v případě nejzávažnějších kybernetických útoků zajistit jen předběžným budováním kapacit schopných se s takovými útoky vypořádat. Návrh zákona vychází z aktuálního vývoje v oblasti budování orgánů pro zabezpečování kybernetické obrany a vybírá tak ty nejefektivnější nástroje obrany kybernetického prostoru při zachování minimální zátěže směrem k osobám soukromého práva. Lze proto konstatovat, že určení jednoho státního orgánu odpovědným za zajišťování kybernetické obrany a jeho vybavení nezbytnými prostředky pro plnění tohoto úkolu, při poměrně malém omezení základních práv a svobod výměnou za ochranu jiných, významných práv a svobod, je vhodné řešení.

Druhým kritériem poměřování základních práv a svobod je **kritérium potřebnosti**, spočívající v porovnávání legislativního prostředku, omezujícího základní právo resp. svobodu, s jinými opatřeními, umožňujícími dosáhnout stejného cíle, avšak nedotýkajícími se základních práv a svobod. Návrh zákona bude omezovat, byť ne více než dosud, právo vlastnit majetek a právo na soukromí, to ale v zájmu zajištění výkonu práva na informační sebeurčení a práva na osobní bezpečnost. V tomto případě má návrh zákona jasně vymezený účel, který spočívá v zabezpečení kybernetického prostoru, tj. v zabezpečení fungování služeb informační společnosti, ať soukromých nebo veřejných. Právě prostřednictvím těchto služeb, tj. jejich dostupnosti, spolehlivosti a bezpečnosti, lze v době rostoucího významu informační společnosti svobodně realizovat právo na informační sebeurčení. Obecným cílem zákona pak je zajistit prostřednictvím obrany kybernetického prostoru fungování státu ve všech jeho aspektech a jeho bezpečnost, což je povinností státu a což samozřejmě umožňuje občanům faktický výkon jejich práva na informační sebeurčení, ale i dalších práv a svobod. Jelikož je nezpochybnitelné, že kybernetické útoky se stávají stále závažnější hrozbou, je potřebnost opatření kybernetické obrany a tím zajištění fungování státu i jeho občanů v kybernetickém prostoru zřejmá. Vedle závazků České republiky plynoucích z členství v mezivládních organizacích představuje zásadní důvod k úpravě kybernetické bezpečnosti (to i včetně shora uvedeného omezení vlastnického práva) základní princip mezinárodního práva, tj. povinnost bdělosti (due diligence). Je v tomto směru jen otázkou času, kdy začne Mezinárodní soudní dvůr řešit odpovědnost státu za jednání, kterého se sice stát sám neúčastní, ale které je mu přičitatelné, neboť má původ v jeho suverénní doméně. Typicky tak může dojít k situaci, kdy budou zneužity počítače na území České republiky k útoku na cizí stát (takové případy se u rozsáhlých útoků vyskytují běžně) – Česká republika, přestože útok neorganizuje ani se na něm nepodílí, může být pohnána k odpovědnosti za to, že takovému útoku, byť k tomu měla prostředky (nebo je měla mít), účinně nezabránila.

Třetím kritériem je **porovnání závažnosti** obou v kolizi stojících základních práv. V posuzovaném případě jedním z nich je právo na soukromí a na tajemství dopravovaných zpráv, na druhé straně pak právo na informační sebeurčení a na bezpečnost. Ke střetu obdobných práv se vyjádřil Ústavní soud v nálezu sp. zn. Pl. ÚS 11/2000 takto: „Ústavní soud zastává názor, že při střetu uvedených dvou hodnot nelze přirozeně abstrahovat

kolektive Gütter). Rozdíl mezi nimi spočívá v jejich distributivnosti. Pro veřejné statky je typické, že prospěch z nich je nedělitelný a lidé nemohou být vyloučeni z jeho požívání. Příklady veřejných statků jsou národní bezpečnost, veřejný pořádek, zdravé životní prostředí. Veřejným statkem se tudíž určitý aspekt lidské existence stává za podmínky, kdy není možno jej pojmově, věcně i právně rozložit na části a tyto přiřadit jednotlivcům jako podíly. (-) Pro základní práva a svobody je, na rozdíl veřejných statků, typická jejich distributivnost. Aspekty lidské existence, jakými jsou např. osobní svoboda, svoboda projevu, účast v politickém dění a s tím spjaté volební právo, právo zastávat veřejné funkce, právo sdružovat se v politických stranách atd., lze pojmově, věcně i právně členit na části a tyto přiřadit jednotlivcům.“.

od bezpečnostních zájmů státu, které je třeba respektovat. Je totiž zřejmé, že výše definovaný státní zájem představuje zájem existenční, který legitimizuje určité omezení privátní sféry jedince; ostatně ve svém důsledku je to stát, jenž postavení jedince chrání. Jestliže Ústavní soud judikoval, že ústava moderního demokratického právního státu představuje společenskou smlouvu, založenou na minimálním hodnotovém a institucionálním konsensu (srov. nález sp. zn. Pl. ÚS 33/97, in: Ústavní soud ČR: Sbírka nálezů a usnesení, sv. 9, str. 407), lze pod tímto pojmem mimo jiné chápat jak zájem státu, tak i jím chráněných osob na jeho vlastní bezpečné existenci; k ochraně tohoto zájmu musí stát disponovat příslušnými nástroji. Jedním z nich je i oblast ochrany utajovaných skutečností.“. Nález se týkal ochrany utajovaných informací, ale lze jej použít i při obdobném střetu v předmětné oblasti zajišťování kybernetické obrany. I zde může docházet k obdobnému střetu práva jedince s právem státu a jeho občanů. Stát musí mít možnost disponovat též nástroji k zajištění své obrany.

Navrhovaná úprava bezprostředně nezasahuje negativně do práva na informační sebeurčení člověka, neboť primárně nezasahuje do obsahové stránky komunikace a nezakládá ani přímé pravomoci státu direktivně zasahovat do běžného života informační společnosti – návrh zákona tedy nepředpokládá žádný státní zásah do soukromí uživatelů při zajišťování kybernetické obrany a v zásadě ani do jejich možností komunikovat prostřednictvím služeb informační společnosti. Právo na informační sebeurčení člověka je naopak návrhem zákona zpracováno jako hodnota, k jejíž ochraně návrh zákona primárně směřuje.

Výše zmíněný zásah do vlastnického práva soukromoprávních subjektů je ve struktuře proporcionality odůvodněn z hlediska vhodnosti, a to jako jediné možné řešení kybernetické obrany, dané nutností umístění nástrojů detekce na určených bodech veřejných sítí elektronických komunikací. Toto řešení je však spojeno jednak se stanovením doby působení zásahu, možnostmi dovolat se přezkoumání takového zásahu, refundací souvisejících vynaložených nákladů, ale také právním nárokem na náhradu škody způsobené činností Vojenského zpravodajství, jíž se podílí na zajišťování obrany České republiky, nebo v souvislosti s ní, a to ve zvláštním procesním režimu, který poskytuje záruky jeho věcné i časové efektivnosti.

Pokud jde o potřebnost, provedenými studiemi a konzultacemi nebylo zjištěno alternativní řešení, které by mohlo naplnit základní cíl záměru, tj. obranu kybernetického prostoru. Byť je většina provozovatelů veřejných sítí elektronických komunikací a poskytovatelů veřejně dostupných služeb elektronických komunikací nepochybně sama vedena zájmem na existenci opatření, díky nimž je garantována bezpečnost České republiky, včetně zabezpečení její obrany v kybernetickém prostoru, tedy bezpečnost „jejich podnikatelského prostředí“. Návrh zákona provozovatele veřejných sítí elektronických komunikací a poskytovatele veřejně dostupných služeb elektronických komunikací dále k nezbytné součinnosti motivuje ekonomickými stimuly (jen fungující síť může generovat ekonomický efekt), a to včetně finanční úhrady vynaložených nákladů.

Zásah do vlastnického práva je tedy co do své intenzity ve zřejmém nepoměru s rizikem zásahu do distributivních i nedistributivních práv, k jejichž ochraně zákon vzniká. Povinnost umožnit nasazení nástrojů detekce, nad to za náhradu, tak zdaleka nedosahuje intenzity rizik ekonomických ztrát, společenských otřesů nebo ztráty mezinárodní důvěryhodnosti České republiky, ani hrozby případného narušení např. právě práva na informační sebeurčení osob. Povinnosti zamýšlené tímto zákonem jsou tedy plně odůvodněny chráněnými zájmy a omezují své adresáty jen v naprosto nezbytně nutné míře. Lze tedy konstatovat, že navrhovaná úprava je vyvážená.

Vzhledem k tomu, že návrh zákona, jak je uvedeno shora, přináší jen minimum povinností osobám soukromého práva, nezatěžuje jejich právo na informační sebeurčení (tj. předkládaný návrh nedává státním orgánům nové právo zasahovat do soukromí ani do aktivní komunikace uživatelů služeb informační společnosti) a naopak zvyšuje míru ochrany základních práv (včetně práva na informační sebeurčení) a nedistributivních veřejných statků (např. kybernetické bezpečnosti), lze konstatovat, že vyhovuje požadavkům ústavní proporcionality, a je tedy ústavně konformní.

Právní úprava je navrhována tak, aby byla v souladu se zásadami zákonnosti, legitimity cílů a přiměřenosti zásahu do základních práv a svobod. Předkládaný návrh zákona směřuje k tomu, aby stát zajistil informace o činnostech, které ohrožují jeho bezpečnost, aby byl připraven detekovat aktivity, jež ohrožují jeho bezpečnost, a v rámci možností byl schopen se jim bránit nebo alespoň minimalizovat následky.

Lze tedy konstatovat, že navrhovaná právní úprava je v souladu s ústavním pořádkem České republiky.

V. Zhodnocení slučitelnosti navrhované právní úpravy s právem Evropské unie, judikaturou soudních orgánů Evropské unie nebo obecnými právními zásadami práva Evropské unie

Poznámka ke kapitole V.: V zájmu komplexnosti posuzování návrhu zákona z hlediska účelu této kapitoly obecné části důvodové zprávy a postižení potřebných souvislostí je dále provedeno vyhodnocení také ve vztahu k judikatuře ESLP, které věcně náleží pod obsah kapitoly VI. Z hlediska komplexnosti vyhodnocení a posouzení dané problematiky je proto nutné vnímat kapitoly V. a VI. obecné části důvodové zprávy jako zpracovatelsky propojené.

Základní právním aktem EU regulujícím kyberprostor je směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, která je plně transponovaná do vnitrostátního právního řádu, a to zejména prostřednictvím zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů.

Cíle předloženého návrhu zákona se však týkají oblasti zajišťování obrany České republiky, a to jak v rámci stanovení jednoho z opatření definičně tvořících pojem „obrana České republiky“, tak, jak je stanoven v § 2 odst. 1 zákona č. 222/1999 Sb. Toto opatření je pak účelem zaměřeno na kybernetický prostor, v němž – i přes jeho specifičnost – musí být na stejné úrovni jako v ostatních případech – zajištěna svrchovanost, územní celistvost a demokratické základy České republiky, tedy její obrana (viz § 16a odst. 1 návrhu zákona). Tuto oblast je nutné podřadit pod pojem národní bezpečnosti, jak ho zná právo EU. Klíčovým ustanovením je čl. 4 odst. 2 Smlouvy o Evropské unii, který stanoví, že Unie *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.*

Uvedený koncept odpovědnosti členského státu za oblast národní bezpečnosti nachází svůj odraz také v sekundárním právu EU. Z oblasti ochrany údajů lze zmínit například nařízení 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), které se nevztahuje na národní bezpečnost, jak stanoví bod 16. preambule a čl. 2 odst. 2 písm. a) nařízení. Obdobně směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích), v konsolidovaném znění, v bodě 11. preambule a v čl. 1 odst. 3 vylučuje použitelnost na oblast národní bezpečnosti (zde „bezpečnosti státu“). Pro návrh zákona proto pro případy zpracovávání osobních údajů plně dopadá hlava IV - OCHRANA OSOBNÍCH ÚDAJŮ PŘI ZAJIŠŤOVÁNÍ OBRANNÝCH A BEZPEČNOSTNÍCH ZÁJMŮ ČESKÉ REPUBLIKY - zákona č. 110/2019 Sb., o zpracování osobních údajů, když návrh zákona je pro tyto účely doplněn pouze o výslovné stanovení nemožnosti slučovat zpracovávané údaje pro jiné účely, než je zajišťování činností, jimiž se Vojenské zpravodajství podílí na zajišťování obrany České republiky v kybernetickém prostoru.

Jak je již uvedeno v předcházejících částech obecné části důvodové zprávy k návrhu zákona, návrh zákona nepředpokládá pro zajišťování předmětných činností Vojenských zpravodajstvím průběžné zpracovávání osobních údajů, taková situace by však mohla vzniknout v souvislosti s vyhodnocováním sledovaných jevů v kybernetickém prostoru. Doba uchovávání takových údajů je pak přesně určena účelem jejich zpracování a ten je zase určen ochranou veřejného zájmu na zajištění obrany státu, v daném případě v kybernetickém prostoru. I na tento omezený rozsah zpracování lze uplatnit pravidla, jež lze dovodit na úrovni EU ze směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených a zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES, jimiž je poskytovatelům veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí uloženo uchovávat údaje – provozní a lokalizační údaje o právnických a fyzických osobách – s cílem zajistit jejich dostupnost pro účely vyšetřování, odhalování a stíhání závažných trestných činů.

Byť činnosti Vojenského zpravodajství, jimiž se budou podílet na zajišťování obrany České republiky v kybernetickém prostoru, nemají stejný účel, jako uložená povinnost uchovávat provozní a lokalizační údaje, neboť jsou určeny k přímému, aktivnímu vyhodnocení předem deklarovaného jedinečného účelu, kterým je zajišťování obrany České republiky, bylo nutné při zpracování jednotlivých ustanovení návrhu zákona pozorně přihlížet také k tomu, že uvedená směrnice byla Soudním dvorem EU v rozsudku ze dne 8. dubna 2014 ve věcech C-293/12 a C-594/12 *Digital Rights Ireland Ltd* shledána neplatnou pro rozpor s čl. 7 a 8 Listiny základních práv EU. Uvedený rozsudek upozorňuje na limity úpravy uchovávání provozních a lokalizačních údajů, jak vyplývají z Listiny základních práv EU, a z Evropské úmluvy o ochraně lidských práv. Uvedený rozsudek poukazuje například na vyhodnocení odůvodněnosti zásahu do zaručených práv (zejména do práva na ochranu osobních údajů a do práva na respektování soukromého života), nezbytnosti a přiměřenosti zásahu, na potřebu jasných a přesných pravidel pro rozsah a použití dotčeného opatření s cílem poskytnout dostatečné záruky umožňující účinně se chránit proti zneužití údajů a protiprávnímu přistupování a využívání, rozporuje globální osobní rozsah působnosti opatření a jeho bezvýjimečnost, neomezení počtu osob, které mají oprávnění k přístupu a využití uchovávaných údajů či absenci povinnosti uchovávat údaje na území Unie *(k tomu viz vyhodnocení provedené v kapitole I. 2 části I. obecné části důvodové zprávy).*

Navrhovaná úprava z hlediska práva Evropské unie spadá pod pojem tzv. národní bezpečnosti, o němž Smlouva o Evropské unii výslovně stanoví v čl. 4 odst. 2 větě poslední, že „zejména národní bezpečnost zůstává výhradní odpovědností každého členského státu“. Pojem

národní bezpečnosti se dotýká ochrany samotných základů státu, tedy ochrany před činnostmi ohrožujícími nebo narušujícími takové hodnoty jako jsou ústavní zřízení, významné ekonomické zájmy, bezpečnost a obrana státu. Tento pojem je třeba považovat za zvláštní vůči obecnému pojmu bezpečnosti, který je součástí prostoru svobody, bezpečnosti a práva a který se týká předcházení trestným činům nebo správním deliktům, jejich odhalování a objasňování (srov. hlavu V Smlouvy o fungování Evropské unie – Prostor svobody, bezpečnosti a práva) – v této oblasti Evropská unie naopak s členskými státy část pravomocí sdílí [čl. 4 odst. 2 písm. j) Smlouvy o fungování Evropské unie].

Smlouva o EU se obrany členských států dotýká v čl. 42 a následujících, týkajících se společné bezpečnostní a obranné politiky. Příprava členských států k obraně, včetně obrany v kybernetickém prostoru, bude-li v souladu se společnou obrannou a bezpečnostní politikou EU, nemůže v takovém případě být v rozporu s právem EU. V tomto smyslu lze o návrhu zákona učinit první dílčí závěr, že návrh je s právem EU slučitelný.

Současně je však třeba zkoumat, zda navrhovaná úprava poskytuje dostatečné jistoty pro to, aby mohla být označena za plně slučitelnou s čl. 7 (respektování soukromého a rodinného života) a čl. 8 (ochrana osobních údajů) Listiny základních práv EU. Soudní dvůr Evropské unie rozsudkem Digital Rights Ireland Ltd ze dne 8. 4. 2014 prohlásil v případě stanovení směrnice o data retention za neplatnou, že „samotná efektivní úprava cíle sledovaného ve veřejném zájmu (v případě směrnice harmonizace úpravy data retention na poli boje proti závažné trestné činnosti), ani takový cíl sám o sobě nemůže odůvodnit, aby opatření týkající se všech prostředků elektronické komunikace a spočívající v uchovávání údajů téměř celé evropské populace bylo považováno za nezbytné. Soudní dvůr Evropské unie vyslovil požadavek cílené souvislosti mezi uchovávanými údaji a ohrožením veřejné bezpečnosti (údaje vztahující se k určitému časovému období, určité zeměpisné oblasti nebo okruhu určitých osob, jež mohou být jakýmkoli způsobem zapojeny do závažné trestné činnosti, anebo k osobám, které by prostřednictvím uchovávání jejich údajů mohly z jiných důvodů přispívat k boji proti závažné trestné činnosti). Návrh zákona v tomto smyslu požadavek Soudního dvora Evropské unie respektuje, když vylučuje plošné uchovávání údajů nijak nevymezeného okruhu fyzických osob. Návrh zákona naopak nepředpokládá, že by detekcí a identifikací kybernetického prostoru byly sledovány údaje o fyzických osobách, popřípadě obsahy jejich zpráv, nýbrž stanoví, že detekovány budou jevy, které nasvědčují ohrožení důležitých zájmů státu, tedy výlučně jen zadané charakteristiky sledovaných jevů. V případě, že by tyto charakteristiky vedly ve svých souvislostech ke konkrétní fyzické osobě, pak by Vojenské zpravodajství přestalo působit jako státní orgán, který se podílí na zajišťování obrany státu, ale pro shromažďování informací by plnilo standardní úkoly zpravodajské služby, a to s využitím standardních postupů a techniky, tedy s nutným přivolením soudu k takovému shromažďování údajů na základě existující právní úpravy.

Při posuzování slučitelnosti navrhované právní úpravy s právem Evropské unie, judikaturou soudních orgánů Evropské unie nebo obecnými právními zásadami práva Evropské unie pak byl využit také rozsudek Soudního dvora Evropské unie ve věci Tele2 Sverige AB ze dne 21. 12. 2016, jímž byly zodpovězeny předběžné otázky Velké Británie a Švédska ohledně výkladu čl. 15 odst. 1 e-privacy směrnice v souvislosti se zneplatněním směrnice o data retention a z toho plynoucích důsledků pro vnitrostátní právní úpravy členských států. Podle čl. 15 odst. 1 e-privacy směrnice členské státy mohou přijmout legislativní opatření omezující rozsah ochrany osobních údajů ve smyslu směrnice, představuje-li omezení v demokratické společnosti nezbytné, přiměřené a úměrné opatření pro zajištění národní bezpečnosti (tj. bezpečnosti státu), obrany, veřejné bezpečnosti a pro prevenci, vyšetřování, odhalování

a stíhání trestných činů nebo prevenci neoprávněného použití elektronického komunikačního systému. Soudní dvůr Evropské unie uvedl, že citované ustanovení, umožňující členským státům výjimku z pravidla poskytování ochrany osobním údajům, je třeba vykládat restriktivně, tedy nelze akceptovat stav, kdy se z výjimky stane pravidlo, jako je tomu v případě plošného a nevýběrového uchovávání velkého množství dat. Vnitrostátní právní úprava musí podle SDEU účinně **vymezovat vztah mezi údaji, které mají být uchovávány, a sledovaným účelem**, tj. musí umožňovat účinné vymezení rozsahu opatření (okruh osob z řad veřejnosti, jejichž údaje mohou vykázat minimálně nepřímou souvislost se závažnou trestnou činností, nebo mohou přispívat k boji proti ní a k předcházení závažného ohrožení veřejné bezpečnosti). Pro tyto případy je návrh zákona koncipován zcela jednoznačně, a to způsobem provádění detekce a identifikace s využitím nástroje detekce, jehož funkčnost je limitována ukazateli útoků a hrozeb; účel – tedy zajišťování kybernetické obrany České republiky pak při poměřování veřejného zájmu na plnění základní funkce státu vymezuje ty případy, kdy by mohlo dojít také ke zpracování předmětných údajů, nikoliv však jako „bezbřehá" činnost, ale jako výsledek vyhodnocení detekovaných a identifikovaných jevů s charakteristikami zadání ukazatelů hrozeb nebo útoku.

Při přípravě návrhu zákona bylo ve světle shora uvedeného a v souladu s nálezem Ústavního soudu České republiky Pl.ÚS 45/217 ze dne 22. května 2019 nutné posoudit, zda a jakým způsobem bude probíhat detekce a identifikace jevů ohrožujících důležité zájmy státu v kybernetickém prostoru. Návrh zákona předpokládá kontinuální detekci uvedených jevů z nástrojů detekce umístěných na vybraných veřejných sítích elektronických komunikací; přitom se nejedná o preventivní vyhodnocování těchto jevů, ale o vyhodnocování v aktuálním čase s cílem včas a v potřebném rozsahu reagovat na vyhodnocený útok nebo hrozbu. Vzhledem k tomu, že jevy ohrožující důležité zájmy státu v kybernetickém prostoru nelze detekovat jiným způsobem, návrh zákona pouze kodifikuje tento způsob v rámci stanovení „podmínek pro provádění činností, jimiž se má Vojenské zpravodajství podílet na zajišťování obrany České republiky v kybernetickém prostoru" (viz čl. 3 odst. 2 ústavního zákona č. 110/1998 Sb.). Zákonnost detekce je tedy zřejmá s tím, že po omezenou dobu lze připustit pouze uchovávání dat a informací, které jsou určeny k vyhodnocení a stanovení opatření k odvrácení kybernetického útoku nebo hrozby.

K právu na soukromí v podobě práva na informační sebeurčení podle čl. 10 odst. 3 Listiny základních práv a svobod našel návrh zákona *inspiraci v rozhodnutí Spolkového ústavního soudu SRN ze dne 15. 12. 1983, BVerfGE 65, 1 (Volkszählungsurteil) nebo ze dne 4. 4. 2006, BVerfGE 115, 320 (Rasterfahndungurteil II)],* ve kterém se uvádí, že v moderní společnosti, charakterizované i obrovským nárůstem informací a dat, musí být ochrana jednotlivce před neomezeným sběrem, uchováváním, užitím a zveřejňováním dat o její/jeho osobě a soukromí poskytována v rámci obecnějšího, ústavně garantovaného práva jednotlivce na soukromí. Pokud jednotlivci nebude garantována možnost hlídat a kontrolovat obsah i rozsah osobních dat a informací jím poskytnutých, jež mají být zveřejněny, uchovány nebo použity k jiným než původním účelům, nebude-li mít možnost rozpoznat a zhodnotit důvěryhodnost svého potenciálního komunikačního partnera a případně tomu uzpůsobit i své jednání, pak nutně dochází k omezení až potlačování jeho práv a svobod, a nelze tak již nadále hovořit o svobodné a demokratické společnosti. Právo na informační sebeurčení je tak nezbytnou podmínkou nejen pro svobodný rozvoj a seberealizaci jednotlivce ve společnosti, nýbrž i pro ustavení svobodného a demokratického komunikačního řádu. **Zjednodušeně řečeno, v podmínkách vševědoucího a všudypřítomného státu a veřejné moci se svoboda projevu, právo na soukromí a právo svobodné volby chování a konání stávají prakticky neexistujícími a iluzorními.**

Judikatura ESLP [zejména rozhodnutí ve věci *Malone proti Spojenému království* (č. 8691/79, rozsudek ze dne 2. 8. 1984)], z čl. 8 Úmluvy, garantujícího právo na respektování soukromého a rodinného života, jakož i obydlí a korespondence, dovozuje i právo na informační sebeurčení. Zdůrazňuje, že sběr a uchovávání údajů týkajících se soukromého života jednotlivce spadají pod rozsah čl. 8 Úmluvy, neboť výraz „soukromý život" je širokým pojmem, který nesnese vyčerpávající definici. Tato fazeta práva na soukromí tak konzumuje i právo na ochranu před sledováním, hlídáním a pronásledováním ze strany veřejné moci, a to i ve veřejném prostoru či na veřejně přístupných místech. Navíc žádný zásadní důvod neumožňuje vyloučit z pojmu soukromého života aktivity profesní, obchodní či sociální [srov. rozhodnutí ve věci Niemietz proti Německu (no. 13710/88) ze dne 16. 12. 1992]. Jak uvedl ESLP, tato extenzivní interpretace pojmu „soukromý život" je ve shodě s Úmluvou o ochraně osob se zřetelem na automatizované zpracování osobních dat (vypracovanou Radou Evropy k 28. 1. 1981, v České republice v platnosti od 1. 11. 2001, publ. pod č. 115/2001 Sb. m. s.), jejímž cílem je „zaručit na území každé smluvní strany každé fyzické osobě (...) respektování jejích práv a základních svobod, a zejména jejího práva na soukromý život, v souvislosti s automatizovaným zpracováním údajů osobního charakteru, které se jí týkají (čl. 1), přičemž ty jsou definovány jako jakékoliv informace týkající se identifikované nebo identifikovatelné fyzické osoby (čl. 2)." [rozhodnutí ve věci Amann proti Švýcarsku (č. 27798/95) ze dne 16. 2. 2000 a tam citovaná judikatura].

Jak je uvedeno v nálezu Ústavního soudu České republiky Pl. US 45/17 ze dne 22. května 2019 ESLP ve své judikatuře k právu na respekt k soukromému životu podle čl. 8 Úmluvy označil za zásahy do soukromí jednotlivců mimo jiné i zásahy v podobě kontroly dat, obsahu pošty a odposlechu telefonních hovorů [srov. rozsudek pléna ve věci Klass a další proti Německu (č. 5029/71) ze dne 6. 9. 1978, rozsudek ve věci Leander proti Švédsku (č. 9248/81) ze dne 26. 3. 1987, rozsudek ve věci Kruslin proti Francii (č.11801/85) ze dne 24. 4. 1990 či rozsudek ve věci Kopp proti Švýcarsku (č. 23224/94) ze dne 25. 3. 1998], zjišťování telefonních čísel telefonujících osob [srov. rozsudek ve věci P. G. a J. H. proti UK (č. 44787/98) ze dne 25. 9. 2001], zjišťování údajů o telefonním spojení (srov. citovaný rozsudek ve věci Amann proti Švýcarsku) nebo uchovávání údajů o DNA jednotlivců v databázích obviněných [srov. rozsudek ve věci S. a Marper proti UK (č. 30562/04 a 30566/04) ze dne 4. 12. 2008]. V rozsudku ve věci Rotaru proti Rumunsku (č. 28341/95) ze dne 4. 5. 2000 ESLP dovodil z práva na soukromý život projevujícího se v podobě práva na informační sebeurčení i pozitivní povinnost státu zlikvidovat data, která o osobě z její soukromé sféry stát shromáždil a zpracoval.

Z judikatury ESLP dále plynou i četné požadavky na kvalitu právní úpravy, jež orgánům výkonné moci přiznává pravomoc uchýlit se k prostředkům tajného sledování obyvatelstva, a to nejen v kontextu trestního řízení, nýbrž podobně i za zpravodajskými a obdobnými účely (viz zejména *Szabó a Vissy proti Maďarsku*, č. 37138/14, rozsudek ze dne 12. ledna 2016; *Roman Zakharov proti Rusku*, č. 47143/06, rozsudek velkého senátu ze dne 4. prosince 2015). **V tomto ohledu je proto podstatné, že navrhovaná právní úprava nezakládá oprávnění Vojenského zpravodajství zasahovat prostřednictvím nástrojů detekce do soukromého života dotčených osob ani obsahu jejich korespondence. Proto se na ni citovaná rozhodovací praxe ESLP bez dalšího nevztahuje**.

I přesto návrh zákona zřizuje funkci inspektora pro kybernetickou obranu, k němuž se může dovolat každá fyzická osoba, která se cítí být dotčena na svých základních právech činnostmi Vojenského zpravodajství, jimiž se podílí na zajišťování obrany České republiky v kybernetickém prostoru. Bližší podrobnosti k úpravě funkce inspektora pro kybernetickou obranu jsou uvedeny ve zvláštní části důvodové zprávy (jmenování inspektora

pro kybernetickou obranu, jeho pravomoci a oprávnění ve vztahu k Vojenskému zpravodajství a návaznost na ostatní kontrolní mechanizmy).

V rámci zkoumání slučitelnosti návrhu zákona s právem Evropské unie, judikaturou soudních orgánů Evropské unie nebo obecnými právními zásadami práva Evropské unie, byla dále posuzována „**vhodnost vymezení okruhu orgánů oprávněných k přístupu ke shromažďovaným údajům ve vazbě na stanovení legitimních cílů, jejichž naplnění mají detekované jevy sloužit, včetně stanovení zákonných podmínek a záruk ochrany pro minimalizaci zásahu do základních práv jednotlivců“**. Vzhledem k tomu, že návrh zákona řeší podmínky zajišťování obrany České republiky v kybernetickém prostoru, je zřejmé, že je na tuto úpravu nutné pohlížet v celkovém rámci dalších právních předpisů upravujících postavení ozbrojených sil České republiky, ale především zajišťování obrany České republiky a další. Vymezení okruhu orgánů, které jsou návrhem zákona určeny ke spolupráci nebo součinnosti při zajišťování kybernetické obrany, je proto především nastaveno těmito „jinými právními předpisy“.

Návrh zákona v úpravě jednotlivých práv a povinností vždy důsledně sleduje silný veřejný zájem (plnění základní povinnosti České republiky při zajišťování její obrany, ochrana důležitých zájmů státu ve smyslu § 2 odst. 1 zákona č. 222/1999 Sb.) a jako takové je lze označit za legitimní. Data a informace, jimiž jsou prezentovány vyhodnocované detekované a identifikované jevy v kybernetickém prostoru, nelze získat jiným způsobem, než v kybernetickém prostoru, přičemž návrh zákona nevyužívá jejich plošný monitoring, ale výlučně výběrovou, jednoznačně definovanou detekci. Tato data a informace jako jedině možné mají potřebnou vypovídací hodnotu pro vyhodnocování kybernetických útoků a hrozeb, a tedy umožňují realizaci návrhem zákona stanoveného cíle.

Z hlediska nezbytnosti omezování práva na soukromí ve vztahu ke sledovanému cíli je možné se odkázat na skutečnosti uvedené shora s tím, že pro návrh zákona bylo zvažováno užití prostředků, které pro splnění daného cíle představují nejmenší invazivní zásah, a to právě pro užití nástroje detekce s funkčně omezenými parametry podle zadaných ukazatelů útoků a hrozeb. Z tohoto hlediska je třeba si uvědomit, že v právním řádu České republiky doposud neexistuje úprava, se kterou by bylo možné návrh porovnávat co do využití prostředků detekce a odvracení kybernetických útoků a hrozeb. Důležitou skutečností pak je, že Vojenské zpravodajství jako státní orgán, který se podílí na zajišťování obrany České republiky v kybernetickém prostoru, vyhodnocuje data a informace aktuálně detekované, nikoliv „minulé“ (z povahy věci je zřejmé, že pro zajišťování kybernetické obrany takové data a informace nemají velkou hodnotu).

Předkladatelé návrhu zákona se nemohli vyhnout provedení poměřování dopadů omezení základního práva na soukromí a informační sebeurčení a sledovaných cílů, naplňujících veřejný zájem, v užším slova smyslu. Test proporcionality pro tyto účely klade otázku, zda je dotčený veřejný zájem natolik důležitý, aby ospravedlnil rozsah omezení práva na soukromí a informační sebeurčení potenciální možností rozšíření funkce nástroje detekce, zda nemohla právní úprava omezit zásah do práva na soukromí a informačního sebeurčení více, tedy zda je zákonné nastavení podmínek dostačující, a zda poskytuje dostatek záruk proti zneužití tohoto významného nástroje, aby omezení vyvážila. Oproti standardním právním úpravám je třeba zdůraznit, že vyhodnocována je potenciální možnost takového zásahu, nikoliv běžná činnost Vojenského zpravodajství při zajišťování obrany České republiky v kybernetickém prostoru. Vyvolání této možnosti by bylo nutné spojit s přímým kybernetickým útokem nebo hrozbou a potřebou odvrátit jejich důsledky vysoké intenzity.

Převažující veřejný zájem je tedy zcela zřejmý, když fyzická osoba je současně chráněna nastavenými mechanismy zpětné kontroly; fyzická osoba je tak vůči případné svévoli orgánu veřejné moci nadána účinným prostředkem své obrany.

Součástí návrhu zákona je rovněž úprava ukládání povinnosti právnickým a podnikajícím fyzickým osobám provozujícím veřejné sítě elektronických komunikací nebo poskytujících veřejně dostupnou službu elektronických komunikací zřídit rozhraní pro umístění nástroje detekce v těchto sítích. I v daném případě je úprava provedena jednoznačně, předvídatelně a aplikačně v rozsahu šetřícím práva a právem chráněné zájmy těchto osob, neboť povinnost je ukládána formou rozhodnutí vydaného ve správním řízení, ve kterém je stanovena doba takového zásahu (6 měsíců s možností jejího prodloužení), stejně jako lhůta, ve které má být rozhraní zpřístupněno.

Návrh zákona na základě provedeného vyhodnocení naplňuje požadavky kladené na zajištění souladu s právem EU, judikaturou soudních orgánů Evropské unie nebo obecnými právními zásadami práva Evropské unie a lze ho aplikovat ústavně konformním způsobem, tedy tak, aby byla maximálně šetřena práva jednotlivců, garantovaná články 10 a 13 Listiny.

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

Poznámka ke kapitole VI.: Kapitola VI. obecné části důvodové zprávy je zpracována jako obsahový dodatek ke kapitole V., ve které je zapracována judikatura ESLP, byť by jinak náležela pod tuto kapitolu věnovanou slučitelnosti s mezinárodními závazky České republiky.

Navrhovaná úprava není v rozporu s mezinárodními smlouvami, jimiž je Česká republika vázána. Zároveň je ovšem třeba poznamenat, že tyto mezinárodní smlouvy se vzhledem k datu svého vzniku eo ipso ani problematikou kybernetické obrany (ani kybernetické bezpečnosti) zabývat nemohou. Toto ovšem neznamená, že není možné dohledat ustanovení, která mohou být potencionálně aplikována i na tuto oblast.

Soulad s Úmluvou o ochraně lidských práv a základních svobod a Mezinárodním paktem o občanských a politických právech byl posouzen výše v části I. a II. obecné části důvodové zprávy.

Do otázek týkajících se práva na sebeobranu státu, tedy rovněž na sebeobranu v kybernetickém prostoru, zasahuje zejména Charta Spojených národů, která státům výslovně přiznává v čl. 51 právo na sebeobranu. Dále se bude jednat o prameny mezinárodního humanitárního práva. Jelikož však návrh zákona nijak nespecifikuje způsob provádění této (kybernetické) sebeobrany, sám o sobě není a nemůže být s Chartou ani dalšími prameny mezinárodního práva v rozporu. Konkrétní akce a opatření, jež budou při výkonu kybernetické obrany konány, budou schvalovány ad hoc, a to vždy po důkladném posouzení, že jsou jak v souladu s pravidly stanovenými Chartou, tak v souladu s ostatním mezinárodním právem, přičemž posuzován bude též soulad jak s ius ad bellum tak i ius in bello. Jako jeden z inspiračních zdrojů jak pro zpracování návrhu zákona, tak následně pro vytváření vlastních podmínek výkonu kybernetické obrany - alespoň do doby, než dojde k dalšímu vývoji v této oblasti mezinárodního práva – bude využit tzv. Tallinský manuál, který vyjadřuje expertní názory na aplikaci mezinárodního humanitárního práva ve sféře kybernetického prostoru.

VII. 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

Nově stanovené povinnosti Vojenskému zpravodajství, resp. zejména nezbytnost zajistit nové komplexní věcné, organizační a personální podmínky jejich výkonu, nepochybně vyvolají nároky na státní rozpočet, **avšak s předpokladem jejich zajištění v rámci existující rozpočtové kapitoly Ministerstva obrany.**

Návrh zákona nepředstavuje vzhledem k předmětu úpravy a nositeli působnosti pro výkon kybernetické obrany žádné nároky na rozpočty krajů a obcí.

Dopad na podnikatelské prostředí bude spočívat pouze v tom, že vybraným podnikatelům v oblasti sítí a služeb elektronických komunikací vznikne povinnost součinnosti při vytvoření rozhraní na jimi provozovaných sítích pro umístění nástrojů detekce.

Sociální dopady, dopad na rodiny ani na specifické skupiny obyvatel návrh zákona vzhledem k předmětu jeho úpravy nemá.

Návrh zákona rovněž není způsobilý vzhledem k povaze jím prováděné úpravy vyvolat dopady do životního prostředí.

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

Zhodnocení této oblasti je již součástí části I. a V. obecné části důvodové zprávy k návrhu zákona.

Nezbývá tedy, než shrnout, že na ochranu osobních údajů se v plném rozsahu použije hlava IV zákona č. 110/2019 Sb., o zpracování osobních údajů.

Nařízení 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), se nevztahuje na národní bezpečnost, jak stanoví bod 16. preambule a čl. 2 odst. 2 písm. a) nařízení.

Rovněž oblast dopadů návrhu zákona do soukromí jedince je již zpracována v předcházejících částech obecné části důvodové zprávy k návrhu zákona s tím, že návrh zákona plně respektuje právo k soukromému životu a vytváří potřebný prostor pro rozvoj a seberealizaci individuální osobnosti. Právo na soukromí garantuje rovněž právo jednotlivce rozhodnout podle vlastního uvážení, zda, popř. v jakém rozsahu, jakým způsobem a za jakých okolností mají být skutečnosti a informace z jeho osobního soukromí zpřístupněny jiným subjektům, avšak zakotvení tohoto práva připouští jeho omezení sledující veřejný zájem tak, jako je tomu u návrhu zákona. V případě, že by byl žádoucí rovnovážný stav narušen, je vždy nutné pro každý individuální případ takového narušení provést test proporcionality a určit, který z daných principů je v daném okamžiku hoden větší ochrany, resp. kdy zabránění důsledkům

narušení jednoho principu je tak důležité pro zachování funkcí státu, že je možné po omezený čas v omezené míře zasáhnout do principu druhého (v rámci vyhodnocování detekovaných jevů a stanovování účinných opatření proti zjištěným kybernetickým útokům a hrozbám). Proporcionalita mezi zájmem na zajišťování obrany České republiky a zájmem na zajišťování práva na soukromí je návrhem zákona zohledněna, a tedy obava, že by útok v kybernetickém prostoru mohl být automaticky vždy obecně kvalifikován jako „menší (nebo naopak větší) hrozba, než obava z neomezeného a nekontrolovaného průniku výkonné moci do soukromé sféry lidí“ není na místě díky jednoznačné, předvídatelné právní úpravě (k *tomu viz také rozsudek ESD ze dne 12. ledna 2016 ve věci 37138/14 – Szabó a Vissy proti Maďarsku, který uvádí:* „Mohou-li být dotčena základní práva a svobody, je však v demokratickém právním státě nepřípustné, aby byla diskrece svěřena orgánům moci výkonné v oblasti národní bezpečnosti bezbřehá. Právo tedy musí stanovit jasné meze pro její výkon tak, aby byli jednotlivci chráněni před svévolnými zásahy do svých práv.“).

IX. Zhodnocení korupčních rizik

Navržená zákonná úprava je pojata tak, aby zásahy do pokojného stavu byly co nejmenší a aby rozhodování o těchto zásazích bylo vždy víceúrovňové a nekoncentrovalo se v jedné osobě. Tyto kroky jsou pak základní pojistkou vedoucí k minimalizaci korupčních rizik.

Návrh zákona kompetence Vojenského zpravodajství rozšiřuje jen v nezbytné míře, která mu umožní plnit úkoly nově právně zakotvených činností v rámci kybernetické obrany, přičemž jeho korupční potenciál je velice nízký. Teoreticky je možné si představit snahy některých provozovatelů zajišťujících sítě elektronických komunikací nebo poskytujících službu elektronických komunikací ovlivnit – ať už pozitivně nebo negativně – své zařazení mezi subjekty, jimž bude ukládána povinnost pro zřízení rozhraní, na které bude připojován nástroj detekce. Vzhledem k tomu, že taková povinnost bude ukládána formou rozhodnutí vydávaného ve správním řízení a že jeho vydání bude nezbytně nutně předcházet vyhodnocení účinnosti umístění nástroje detekce, lze toto riziko označit za velmi nízké.

Ryze jako teoretickou úvahu lze posoudit riziko možnosti ovlivnit výši náhrady nákladů spojených se zřízením rozhraní pro připojení nástroje detekce. Pojistka vyloučení vzniku tohoto rizika je totiž obsažena v samotném návrhu zákona, a to ve zmocnění pro stanovení výše a podmínek poskytování náhrad vyhláškou Ministerstva obrany, jež by měla garantovat dostatečnou ochranu před možným korupčním rizikem.

X. Zhodnocení dopadů na bezpečnost a obranu státu

Návrh zákona má přímý dopad na obranu a bezpečnost státu, neboť určuje nový subjekt, jemuž se stanovují povinnosti při zajišťování obrany České republiky, a to obrany v kybernetickém prostoru. Obrana České republiky je tak posilována v oblasti zcela specifických hrozeb, a to nejenom z pohledu technologického, ale také z pohledu prostorového umístění hrozeb, jejich vzniku, možností likvidace i případných účinků. Současně je tato specifická část obrany České republiky důsledně začleňována do celkové koncepce obrany České republiky, jejího plánování, přípravy a zajišťování.

Návrh zákona nemá dopady na aktiva zpravodajských služeb ani bezpečnostních sborů ani na jejich příslušníky. Podrobnosti obsahuje závěrečná zpráva RIA.

ZVLÁŠTNÍ ČÁST

K části první – novela zákona o Vojenském zpravodajství

K čl. I

Obecně:

Bodem 1 je do zákona č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, začleňována nová část čtvrtá, která má pro účely identifikace Vojenského zpravodajství jako jednoho z nositelů povinnosti podílet se na zajišťování obrany České republiky v informačních systémech a službách a sítích elektronických komunikacích (kybernetickém prostoru) povahu provedení čl. 3 odst. 2 věty druhé ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky, tedy stanovení nezbytného rozsahu povinností a dalších podrobností pro výkon činností, jimiž se státní orgán – Vojenské zpravodajství – má podílet na zajišťování obrany České republiky („*Státní orgány, orgány územních samosprávných celků a právnické a fyzické osoby jsou povinny se podílet na zajišťování bezpečnosti České republiky. Rozsah povinností a další podrobnosti stanoví zákon*.“).

Koncepce návrhu zákona s přihlédnutím k zadání pro předložení návrhu zákona stanovenému usnesením vlády České republiky ze dne 25. května 2015 č. 382 zužuje užití prvků terminologické množiny pojmu „bezpečnost České republiky“ na prvek bezpečnosti vnější, tedy obranu České republiky. V tomto smyslu byl návrh zákona upřesněn s tím, že současně zůstává zachována obecná úprava (systém) zajišťování obrany České republiky a její definice (navrhovaná úprava se svým způsobem realizačně vztahuje k zákonu č. 222/1999 Sb., o zajišťování obrany České republiky, ve znění pozdějších předpisů, a zákonu č. 219/1999 Sb., o ozbrojených silách, ve znění pozdějších předpisů). Pojem „obrana České republiky v kybernetickém prostoru“ proto není nutné v návrhu zákona zvláště definovat, protože z povahy věci je součástí obrany České republiky tak, jak je definována v § 2 odst. 1 zákona č. 222/1999 Sb. (*Obrana* České republiky *je souhrn opatření k zajištění svrchovanosti, územní celistvosti, principů demokracie a právního státu* České republiky*, ochrany života obyvatel a jejich majetku před vnějším napadením. Obrana* České republiky *zahrnuje výstavbu účinného systému obrany státu, přípravu a použití odpovídajících sil a prostředků a účast v kolektivním obranném systému*.).

Částí čtvrtou jsou nově upravovány povinnosti Vojenského zpravodajství, jimiž se podílí na zajišťování obrany v kybernetickém prostoru; vzhledem k specifické povaze tohoto prostoru i aktivitám, které v něm probíhají, včetně nemožnosti určit jeho hranice a předpokládané možné lokalizaci zdrojů jednotlivých kybernetických útoků a hrozeb také mimo území České republiky, je Vojenskému zpravodajství přiznána možnost využívat výsledků analýzy jeho vlastní zpravodajské činnosti nikoliv pouze pro určení hrozby, ale také k přímému výkonu jejího odvrácení nebo omezení jejích účinků tam, kde by jinak byly příslušné ozbrojené síly České republiky.

K plnění úkolů Vojenského zpravodajství při zajišťování obrany České republiky v kybernetickém prostoru jsou návrhem zákona vytvářeny specifické podmínky, ale vždy s přihlédnutím k tomu, že k obraně České republiky jsou určeny ozbrojené síly a obrana České republiky je zajišťována jako celek, tedy bez ohledu na místo jejího provádění, typu využívaných sil a prostředků apod. Kybernetická obrana je tedy pojata jako nedílná součást obrany České republiky, tedy včetně využívání všech jejich aspektů přípravy, organizace a strukturálních vazeb a současně při zachování odpovědnosti vlády České republiky za její výkon v rámci komplexu opatření směřujících k zabezpečení obrany České republiky.

Stejně je důraz kladen na to, že obrana České republiky v kybernetickém prostoru má velmi proměnlivé hranice ve vztahu k zajišťování vnitřní bezpečnosti státu v kybernetickém prostoru a že by bylo mimořádně kontraproduktivní obě tyto úrovně zajišťování bezpečnosti státu jako celku vnímat jako dvě důsledně oddělované aktivity.

Terminologická poznámka:

Pokud se týká užívání pojmů „data, informace nebo údaje“, jsou v návrhu zákona užívána ve smyslu jejich významové aplikace v zákoně č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

K § 16a:

K odstavcům 1 a 2:

V navrhovaném znění § 16a odst. 1 je tak, jak je uvedeno výše, stanovena Vojenskému zpravodajství povinnost podílet se na zajišťování obrany České republiky v kybernetickém prostoru. Tento podíl je obsahově naplněn vyhledáváním (detekcí) jevů v kybernetickém prostoru, které nesou znaky kybernetického útoku nebo hrozby mající původ v zahraničí (zde se úprava harmonizuje s působností Vojenského zpravodajství podle zákona o zpravodajských službách České republiky) a významně ohrožující skutečnosti, které jsou v § 2 odst. 1 zákona č. 222/1999 Sb. definovány jako důležité zájmy státu chráněné jako základní povinnost České republiky před vnějším napadením. Tyto zájmy, tedy svrchovanost, územní celistvost, principy demokracie a právního státu, ochrana života obyvatel a jejich majetku, jsou v § 16a odst. 1 označeny jako „důležité zájmy státu“.

Činnosti Vojenského zpravodajství, jimiž se bude podílet na zajišťování obrany státu, nejsou jedinečně prováděnou činností, ale plněním úkolů imanentně náležejících do komplexu činností, jimiž je zajišťována obrana České republiky, a tedy plně podřízené vazbám, organizaci a plánování zajišťování obrany České republiky tak, jako jsou nastaveny zákonem č. 222/1999 Sb. Vojenské zpravodajství se proto při plnění úkolů (činností), jimiž se bude podílet na zajišťování obrany státu, bude řídit a v koordinačních vazbách jeho činnost bude koordinována především ústředním plánem obrany státu, seznamem opatření národního systému reakce na krize pro potřeby řízení obrany státu, katalogem opatření národního systému reakce na krize pro potřeby řízení obrany státu a dílčím plánem obrany Ministerstva obrany.

Základním úkolem Vojenského zpravodajství v rámci jeho postavení státního orgánu, který se podílí na zajišťování obrany České republiky v kybernetickém prostoru, je na základě jím určených kritérií provádět detekci kybernetických útoků a hrozeb, tj. vyhledávat jevy vykazující tato kritéria a následně je identifikovat co do způsobilosti stát se hrozbou nebo být kybernetickým útokem proti důležitým zájmům státu. Takto identifikovaná data a informace jsou pak vyhodnocována z hlediska síly jejich bezprostředního potenciálu ohrozit důležité zájmy státu, důsledků ukončení jejich vnějšího zamýšleného projevu, ale také způsobilosti dopadnout svými účinky i do jiných oblastí, než je zajišťování obrany České republiky. Jak vyplývá z dalších ustanovení návrhu zákona, toto vyhodnocování představuje náročný, strukturovaný proces, do kterého jsou v různých úrovních zapojovány další státní orgány, a to s přihlédnutím k působnosti v oblasti zajišťování vnitřní bezpečnosti státu, a to včetně bezpečnosti kybernetické, ale také ostatní zpravodajské služby. V praxi to do budoucna může znamenat například zřízení pracovních skupin, konzultačních týmů nebo nastavení účelných komunikačních cest, které v daném čase umožní získat potřebnou podporu a součinnost toho kterého státního orgánu.

K odstavci 3:

V § 16a odst. 3 je pro účely návrhu zákona stanoven postup, jakým Vojenské zpravodajství stanovuje ukazatele útoků a hrozeb, tedy ona kritéria, kterými jsou objektivizovány znaky útoků a hrozeb v kybernetickém prostoru tak, aby bylo možné provádět jejich rámcové vyhledávání. Tyto ukazatele nebudou stanovovány ani nahodile, ale ani trvale. K jejich nastavení a další aktualizaci využije Vojenské zpravodajství výsledky své vlastní zpravodajské činnosti, zpravodajské činnosti ostatních zpravodajských služeb, poznatků Národního úřadu pro kybernetickou a informační bezpečnost a dalších státních orgánů. Pro nastavení ukazatelů útoků a hrozeb - což vyplývá z účelu jejich stanovování - však Vojenské zpravodajství využije také veškeré další zdroje vypovídající o skutečnostech způsobilých ohrozit plnění funkce státu v oblasti zajišťování jeho obrany.

K § 16b:

Vojenskému zpravodajství je ustanovením § 16b ukládána povinnost spolupracovat s ostatními zpravodajskými službami a s dalšími státními orgány, ozbrojenými silami České republiky, bezpečnostními sbory a právnickými a fyzickými osobami, pokud působí v oblasti zajišťování kybernetické bezpečnosti nebo obrany státu. Touto povinností je zajišťována potřebná míra koordinace činností tam, kde specifická povaha kybernetického prostoru vyžaduje například identifikaci detekovaných jevů vůči dalším informacím, prověření obdobných situací nebo využití účinných postupů, které ve srovnatelných situacích použily jiné státní orgány. Toto ustanovení navíc vytváří předpoklad pro to, aby pro vyhodnocování a správné (účinné) řešení určitých situací mohlo být využito různých forem spolupráce, tedy například vytváření pracovních skupin, zřízení konferenční komunikační cesty, individuální využití specialistů jiného státního orgánu apod.

Zakotvením povinnosti spolupracovat má zásadní význam, neboť se tím navazuje na strukturu opatření určených k zabezpečování obrany České republiky obecně, resp. k zajištění plánování a zabezpečení operační přípravy státního území, doplňování ozbrojených sil a mobilizaci ozbrojených sil, pro jejichž realizaci je Ministerstvo obrany oprávněno „vyžadovat od příslušných ministerstev, jiných správních úřadů a územních samosprávných celků součinnost; ministerstva, jiné správní úřady a územní samosprávné celky jsou povinny požadavkům vyhovět“ [viz § 6 odst. 1 písm. c) zákona o zajišťování obrany České republiky]. Obdobně pak Vojenské zpravodajství při provádění všech činností, jimiž se podílí na zajišťování obrany České republiky, spolupracuje, s ozbrojenými silami České republiky, ozbrojenými bezpečnostními sbory a dalšími státními orgány i právnickými a fyzickými osobami, pokud působí v oblasti zajišťování kybernetické bezpečnosti nebo obrany České republiky. Uvedená zásada se stává garantem komplexního vyhodnocování detekovaných jevů, správnosti a účelnosti jejich vyhodnocení a zejména včasné využitelnosti příslušných dat a informací tam, kde jejich povaha svědčí nejenom o ohrožení důležitých zájmů státu jako předmětu obrany České republiky, ale i o ohrožení zájmů hodných ochrany v rámci systému vnitřní bezpečnosti.

K § 16c:

Ustanovení § 16c stanoví nástroje detekce kybernetických útoků a hrozeb a podmínky jejich provozování, které Vojenské zpravodajství využívá při výkonu činností, jimiž se podílí na zajišťování obrany České republiky, tedy zcela mimo výkon zpravodajské činnosti.

Nástroje pro odhalování kybernetických útoků budou předem nadefinovány, aby upozornily na fakt, že hrozí nebo již probíhá kybernetický útok či hrozba. Z toho důvodu bude Vojenské zpravodajství disponovat pouze metadaty o probíhajícím, případně bezprostředně

hrozícím kybernetickém útoku a žádná další data o komunikaci nebudou ukládána nebo archivována. Návrh nepřipouští použití nástrojů k jiným účelům než pouze k odhalení útoků, resp. ke kontrole, zda tato činnost je dodržována. Rozhodně se tedy nemůže jednat o plošný monitoring metadat, a už vůbec ne o sledování obsahu komunikace. Zjednodušeně to lze přirovnat k systému včasného varování, jak ho známe i z jiných oblastí naší bezpečnosti. Jde o upozornění na blížící se nebezpečí. Zaznamená-li systém v síti nějakou formu anomálie, anebo ohrožení, zaktivuje se a vyšle signál, který bude impulzem pro další kroky.

Cílem návrhu není a ani nemůže být sledování či jakékoli seznamování se s obsahem komunikace. Pro tyto účely stát již disponuje zákonnými oprávněními se striktně danými podmínkami soudní kontroly apod. Návrh ustanovení § 16c umožní disponovat velmi omezeným rozsahem dat – pouze o záchytu předem definovaných ukazatelů (nejčastěji se bude jednat o tzv. indikátory kompromitace, případně jevy nasvědčující, že se chystá masivní kybernetický útok) – pro účely přijetí potřebných opatření.

Cílená detekce je totiž koncipována tak, že se nebude jednat o sledování či zaznamenávaní nejen samotného obsahu, ale ani metadat o komunikaci (typicky provozních a lokalizačních údajů). Nástroje detekce budou zaznamenávat data pouze v rozsahu předem definovaných ukazatelů. Tzn. v nástroji detekce bude nadefinován např. škodlivý kód odpovídající již v minulosti zaznamenanému útoku na nemocnici v zahraničí – když pak tento kód nástroj v provozu detekuje, tak zaznamená výhradně tuto skutečnost a uchová související metadata. Informaci o záchytu dané škodlivosti nástroj automaticky pošle stálému operačnímu centru Vojenského zpravodajství.

Nástroj dále bude zaznamenávat už jen metadata o svém vlastním provozu a případné manipulaci – pro potřebu jak kontroly, tak i bezpečnosti samotného nástroje, resp. informací ohledně toho, jaké ukazatele jsou vyhledávány.

K odstavci 1:

Základním technologickým prostředkem výkonu činností, jimiž se Vojenské zpravodajství podílí na zajišťování obrany státu, je nástroj detekce umísťovaný v určených bodech veřejných komunikačních sítí a umožňující provádět cílenou detekci jevů nasvědčujících existenci kybernetického útoku nebo hrozby a jejich identifikaci podle zákona o Vojenském zpravodajství. Tyto nástroje detekce jsou funkčně limitovány (předurčeny) ukazateli útoků (viz shora), což umožňuje včasnou detekci jevů, vypovídajících o možném výskytu kybernetického útoku nebo hrozby. Na základě identifikace těchto jevů pak dojde k jejich konkrétnímu přiřazení tak, aby byly přesně identifikovány typy kybernetického útoku nebo hrozby, síla ohrožení důležitých zájmů státu, zdroje hrozby apod., tedy skutečnosti umožňující reagovat ve smyslu „přijetí opatření k zabezpečení obrany České republiky“.

Rovněž tato činnost je ovládána zásadou spolupráce s dalšími subjekty, a tím tedy v podstatě také zásadou vysoké efektivity prováděných činností (přijímaných opatření) v zájmu zajištění obrany České republiky.

V odstavci 1 je také zdůrazněna skutečnost, že nástroj detekce může být umisťován pouze pro účely obrany České republiky v kybernetickém prostoru.

K odstavci 2:

Tímto ustanovením je provedeno výlučné určení nástrojem detekce zaznamenávaných metadat. Nástroje detekce v rámci svého provozu zaznamenávají metadata o provozu veřejných

komunikačních sítí a veřejně dostupných služeb elektronických komunikací, ale pouze v rozsahu souvisejícím s detekovaným kybernetickým útokem nebo hrozbou na základě stanovených ukazatelů.

Dále je stanoveno, že nástroj detekce zaznamenává metadata o provozu nástroje detekce. Tato funkce by pro činnosti, jimiž se Vojenské zpravodajství podílí na zajišťování obrany České republiky, mohla zdánlivě mít jenom podružnou roli, což však nabyde naprosto odlišného vyhodnocení pro případy, kdy se začneme zabývat otázkou, do jaké míry a v jakém rozsahu lze provést zásah do základních práv a svobod jedince v případech, kdy tato práva musí být dočasně potlačena zájmem na zajišťování obrany České republiky (k tomu viz kapitola V. obecné části důvodové zprávy). Pokud dojde k ukončení takového zásahu, je třeba plně restituovat zasažené základní práva a svobody, a to včetně umožnění přezkumu provedeného zásahu a vyloučení jeho svévolného provedení. K tomu bude sloužit záznam o vlastním životním cyklu nástroje detekce.

Obdobné poslání mají metadata o manipulaci s konfigurací nástroje detekce pro potřeby auditu Vojenským zpravodajstvím vykonávaných činností, kterými je zajištěno sledování a uchovávání dat o jakékoliv aktivitě vůči nástroji detekce, ať již oprávněné nebo neoprávněné. Uchování těchto metadat se váže k navrhovanému znění § 98a odst. 3 podle části třetí návrhu zákona (novela zákona o elektronických komunikacích), podle kterého právnická nebo podnikající fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací není bez souhlasu Vojenského zpravodajství oprávněna jakýmkoliv způsobem zasáhnout do jím připojeného nástroje detekce nebo jakkoliv omezit jeho funkčnost; o porušení této povinnosti pak budou vypovídat právě tato metadata.

K odstavci 3:

Ustanovení odstavce 3 vylučuje, aby nástroje detekce sloužily jako nástroj zpravodajské techniky, tedy je pojistkou jejich využití výlučně ve smyslu funkcí vymezených účelem a obsahem stanovených ukazatelů útoků podle § 16a odst. 2. Zákon pro tyto účely stanoví, že nástroje detekce nesmí být využito pro provádění odposlechů nebo pro záznam zpráv podle zákona o elektronických komunikacích, tedy pro výkon zpravodajské činnosti.

K odstavci 4:

Ustanovení § 16c odst. 4 poskytuje záruky fyzickým osobám ve vztahu k ochraně jejich základních práv na informační sebeurčení, ale také právnickým nebo podnikajícím fyzickým osobám zajišťujícím veřejnou komunikační síť nebo poskytujícím veřejně dostupnou službu elektronických komunikací co do zajištění řádného výkonu jimi prováděných činností. Činnosti, jimiž se Vojenské zpravodajství podílí na zajišťování obrany České republiky, a to zejména cílená detekce kybernetických útoků a hrozeb, musí být prováděna způsobem (tedy technicky zajištěna tak), aby bylo vyloučeno zasahování do důvěrnosti komunikací fyzických a právnických osob při poskytování veřejně dostupné služby elektronických komunikací, integrity veřejných komunikačních sítí a dostupnosti veřejných komunikačních sítí a služeb elektronických komunikací, byť lze u nástroje detekce předpokládat, že v sobě nese potenciál možnosti takového zásahu. Zákon však využití takového latentního potenciálu zakazuje.

Stejně tak činností Vojenského zpravodajství nesmí být zasahováno nebo ovlivňováno plnění povinností právnické nebo podnikající fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací vůči uživatelům sítě jinak, než v rozsahu odpovídajícím veřejnému zájmu na zajišťování obrany státu; v daném případě se opět zákonem stanoví garance nerušeného výkonu práv a povinností právnickým

nebo podnikajícím fyzickým osobám zajišťujícím veřejnou komunikační síť nebo poskytujícím veřejně dostupnou službu elektronických komunikací, které jsou omezeny výlučně veřejným zájmem na zajišťování obrany státu, a to vždy na základě provedení testu proporcionality pro nalezení maximálně možné míry takového zásahu.

Ustanovení § 16c odst. 4 je klíčovým ustanovením návrhu zákona pro zajištění ochrany soukromí fyzických osob a ochrany jejich osobních údajů tak, jak je podrobněji popsáno v kapitole V. obecné části důvodové zprávy, a to s přihlédnutím k nezbytnosti poměřování síly ochrany zájmu (práva) vzhledem k aktuální situaci, ze které vyplývá převažující hodnota pro ochranu „vyššího" zájmu státu. Jak je již uvedeno výše, účelem získávání a shromažďování osobních údajů zpravodajskými službami je ochrana ústavního zřízení, významných ekonomických zájmů, bezpečnosti a obrany České republiky. Vedle sebe tak stojí dva obdobně silné zájmy státu a jeho obyvatel, pro něž za standardních (tedy předvídatelného a legálního chování všech účastníků) podmínek není problémem, aby nerušeně působily vedle sebe, aniž by se vzájemně ovlivňovaly. V případě, že je tento rovnovážný stav narušen, je však vždy nutné pro každý individuální případ takového narušení provést test proporcionality a určit, který z daných principů je v daném okamžiku hoden větší ochrany, resp. kdy zabránění důsledkům narušení jednoho principu je tak důležité pro zachování funkcí státu, že je možné po omezený čas v omezené míře zasáhnout do principu druhého. V zájmu zabránění svévole při uplatňování veřejného zájmu je proto návrhem zákona stanoveno, že při plnění úkolů při zajišťování kybernetické obrany zasahuje Vojenské zpravodajství do základních práv a svobod jen v rozsahu přiměřeném nezbytnosti zajištění důležitých zájmů státu a po dobu nezbytně nutnou, a to jen v případě, kdy k zajištění bezpečnosti České republiky v kybernetickém prostoru nepostačují prostředky ozbrojených sil České republiky nebo ozbrojených bezpečnostních sborů, popřípadě kdy intenzita kybernetického útoku nesnese pro jeho zastavení nebo odvrácení časového odkladu.

K § 16d:

K odstavcům 1 až 3 a 7:

Navrhovaným ustanovením § 16d je upraveno právo Ministerstva obrany, jehož součástí je Vojenské zpravodajství, které ministerstvo řídí [viz § 16 odst. 2 písm. e) kompetenčního zákona a § 3 psím. c) zákona o zpravodajských službách České republiky] požadovat od právnických nebo podnikajících fyzických osob zajišťujících veřejnou komunikační síť nebo poskytujících veřejně dostupnou službu elektronických komunikací zřízení a zabezpečení rozhraní pro připojení nástrojů detekce a podmínky jeho výkonu. Jde o obdobu v současnosti platného ustanovení § 9 odst. 5 písm. a) zákona o Vojenském zpravodajství, podle něhož Vojenské zpravodajství je oprávněno v rozsahu potřebném pro plnění konkrétního úkolu požadovat od právnických nebo podnikajících fyzických osob zajišťujících veřejnou komunikační síť nebo poskytujících veřejně dostupnou službu elektronických komunikací zřízení, popřípadě zabezpečení rozhraní pro připojení koncového telekomunikačního zařízení pro odposlech nebo záznam zpráv v určených bodech jejich sítě. Navrhované znění § 16d upravuje obdobné oprávnění k součinnosti pro účely kybernetické obrany.

Uvedené povinnosti budou právnickým nebo podnikajícím fyzickým osobám zajišťujícím veřejnou komunikační síť nebo poskytujícím veřejně dostupnou službu elektronických komunikací ukládány rozhodnutím vydávaným Ministerstvem obrany; forma rozhodnutí, jimž je pro ten který konkrétní případ rozhodováno o nezbytnosti umístit nástroj detekce, je nejvhodnějším řešením, neboť umožňuje zohlednit individuální podmínky jak na straně provozovatele veřejné komunikační sítě, tak potřeb Vojenského zpravodajství na umístění a užívání nástroje detekce pro cílenou detekci kybernetického prostoru. Před

vydáním rozhodnutí proto bude Vojenské zpravodajství povinno posoudit, zda připojení nástroje detekce samo o sobě není bezpečnostním rizikem, popřípadě zda je možné důsledky takového bezpečnostního rizika přijmout jako akceptovatelné vzhledem k účelu připojení konkrétního nástroje detekce, bude jednat s povinnými osobami a společně budou hledat nejvhodnější řešení určení místa veřejné komunikační sítě. Ze závěrů této činnosti Vojenské zpravodajství zpracuje stanovisko, a to jako dokument uchovávaný odděleně mimo spis z důvodu ochrany utajovaných informací (§ 17 odst. 3 správního řádu).

Související finanční nároky právnických nebo podnikajících fyzických osob zajišťujících veřejnou komunikační síť nebo poskytujících veřejně dostupnou službu elektronických komunikací pak budou řešeny na základě jednotné úpravy provedené vyhláškou Ministerstva obrany.

Návrhem zákona je stanoveno, že základní charakteristiky veřejných komunikačních sítí využitelných pro umístění nástrojů detekce z hlediska zajištění důležitých zájmů státu stanoví vláda v ústředním plánu obrany státu; tato úprava vychází z koncepce jedinečné a jednotné struktury stanovované v zájmu zajištění obrany České republiky, a tedy i podrobnosti výkonu činností, jimiž se Vojenské zpravodajství podílí na zajišťování obrany České republiky, musí být předvídatelně stanovovány v plánech obrany, konkrétně v ústředním plánu obrany. Tedy i navrhovaným ustanovením § 16d je plnění úkolů Vojenského zpravodajství při zajišťování obrany České republiky v kybernetickém prostoru začleňováno do obrany státu jako celku; vnímání kybernetické obrany jako součásti souhrnu opatření k zajištění svrchovanosti, územní celistvosti, principů demokracie a právního státu, ochrany života obyvatel a jejich majetku před vnějším napadením. Proto také kybernetická obrana musí být plánována v rámci celého souboru opatření, který je označován jako plánování obrany státu (§ 2 odst. 8 zákona č. 222/1999 Sb.) a Vojenské zpravodajství se při jejím zajišťování musí důsledně podřizovat příslušnými plány nastaveným parametrům, zásadám a vazbám s ozbrojenými silami.

K odstavcům 4 a 5:

Vzhledem k předvídatelnosti podmínek umístění nástroje detekce je přímo zákonem stanoveno, že rozhodnutí vedle náležitostí stanovených správním řádem musí obsahovat také určení doby, po kterou má být nástroj detekce v určeném bodě provozován, a lhůtu, ve které je právnická nebo podnikající fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinna v určených bodech jí zajišťované veřejné komunikační sítě zřídit rozhraní pro připojení nástroje detekce.

Doba umístění nástroje detekce nesmí být delší než 6 měsíců, Ministerstvo obrany ji však může na návrh Vojenského zpravodajství prodloužit.

Zákon tak reaguje na požadavky Evropského soudu pro lidská práva, kterými směřuje k zajištění jednoznačné, předvídatelné a vymahatelné právní úpravy, přičemž považuje za nepostačující, aby uvedené skutečnosti byly ponechány na vůli orgánu vydávajícího správní rozhodnutí.

K odstavci 6:

Rozklad proti rozhodnutí nebude mít odkladný účinek.

K § 16e:

Ustanovením § 16e je specifikováno, jakými konkrétními opatřeními je Vojenské zpravodajství oprávněno odvracet detekované kybernetické útoky a hrozby. Reakce na odhalený kybernetický útok bude vždy záležet na intenzitě, možných dopadech a okolnostech konkrétního odhaleného útoku. Přednostně se bude sdělovat informace o útoku jiným oprávněným institucím, aby byla přijatá potřebná opatření z jejich strany. Ve velkém počtu případů totiž postačí, aby např. NÚKIB varoval prvky kritické informační infrastruktury a doporučil přijetí potřebných opatření. Aktivně působit proti útoku bude moci Vojenské zpravodajství jen v krajním případě a za přísně stanovených zákonných podmínek.

V zájmu vytvoření potřebných vazeb pro komplexní zajišťování vnitřní bezpečnosti a obrany České republiky v kybernetickém prostoru a současně s přihlédnutím k nezbytnosti zajistit potřebný, tedy účelný a pro výkon stanovených povinností efektivní „rozsah povinností a podrobnosti“ pro jejich provádění, je v návrhu zákona Vojenskému zpravodajství stanoveno, že v případech, kdy Vojenské zpravodajství identifikuje konkrétní kybernetický útok nebo hrozbu, pro jejichž odvrácení nejsou naplněny podmínky pro provedení aktivního zásahu podle § 16f, předá neprodleně zjištěné informace k provedení dalších opatření příslušným státním orgánům.

K tomuto kroku by nemohlo být přistoupeno bez podrobného vyhodnocování detekovaných útoků a hrozeb. Tím je určena v podstatě hlavní role Vojenského zpravodajství při zajišťování kybernetické obrany poté, kdy identifikují hrozbu pro důležité zájmy státu v kybernetickém prostoru; touto rolí je posoudit intenzitu ohrožení důležitých zájmů státu, časovou naléhavost provedení zastavení nebo odvrácení kybernetického útoku anebo odstranění nebo omezení důsledků vyhodnocených hrozeb pro důležité zájmy státu v kybernetickém prostoru a aktuální schopnosti a technické možnosti ozbrojených sil České republiky nebo ozbrojených bezpečnostních sborů zastavit nebo odvrátit kybernetický útok anebo odstranit nebo omezit důsledky vyhodnocených bezpečnostních rizik pro důležité zájmy státu v kybernetickém prostoru v potřebném čase; poslední z uvedených kritérií bude vyhodnocováno na základě informací sdílených mezi Ministerstvem obrany a Ministerstvem vnitra na základě § 27 kompetenčního zákona („Ministerstva si navzájem vyměňují potřebné informace a podklady.“), resp. konkrétněji na základě § 6 odst. 1 písm. a) a b) zákona č. 222/1999 Sb., o zajišťování obrany České republiky (Ministerstvo obrany k zajišťování obrany státu „navrhuje vládě základní opatření k přípravě a organizování obrany státu; k tomu zejména zpracovává obranné koncepce a požadavky na zabezpečení obrany státu“ a „odpovídá za proces plánování obrany státu a koordinuje jeho přípravu; k tomu může vyžadovat od příslušných ministerstev, jiných správních úřadů a územních samosprávných celků podkladové materiály“).

Dalším kritériem, jehož vyhodnocení musí být identifikovaný kybernetický útok nebo hrozba podrobeny, je stanovení účelného a účinného řešení identifikované bezpečnostní hrozby a zastavení nebo odvrácení kybernetického útoku; toto kritérium je mimořádně důležité, neboť identifikovanou hrozbu podrobuje testu jejího nejúčelnějšího řešení z hlediska veškerých souvislostí, tedy času, intenzity, důsledků, možností provedených aktivit, doby působení a její povahy z hlediska ohrožení zájmů vnitřní bezpečnosti státu nebo jeho obrany. Tento kontext prolíná zajišťováním obrany státu v kybernetickém prostoru, neboť každá hrozba musí být vyhodnocována z hlediska zajišťování vnitřní bezpečnosti a obrany České republiky jako celku za aktivní podpory všech státních subjektů, jimž byly svěřeny úkoly v této oblasti.

Posledním stanoveným kritériem, jímž je identifikovaná hrozba posuzována, je stanovení míry tolerance vůči rizikům (důsledkům dokonaného útoku nebo hrozby) vyvolaným kybernetickým útokem nebo hrozbou vzhledem k jeho předpokládaným důsledkům vůči důležitým zájmům státu a nezbytnosti zajistit podmínky pro plnění jiných povinností České republiky. Toto kritérium vychází z praktických zásad řízení rizik, když v některých případech je pro dosažení sledovaného účelu vhodné ponechat působení hrozby až do míry akceptovatelného rizika (tedy akceptovatelných důsledků pro důležité zájmy státu), což například umožní shromáždit kvalitnější soubor informací o zdroji hrozby nebo soustředit síly proti hrozbě působící tak, že odvrátí hrozbu společně s likvidací jejího zdroje.

Vyhodnocení identifikované hrozby podle stanovených kritérií je pro Vojenské zpravodajství spojeno s jemu stanovenou povinností (a odpovědností) rozhodnout, který ze subjektů zřízených za účelem zajišťování vnitřní bezpečnosti a obrany České republiky bude „nejlepší“ k provedení potřebných opatření proti identifikované hrozbě; na základě svého rozhodnutí pak Vojenské zpravodajství samo aktivně proti hrozbě zasáhne, nebo řešení situace předá určenému subjektu, a to s přihlédnutím k jeho působnosti.

Odstavec 2 de facto představuje reálné využití zásady spolupráce. V případech, kdy Vojenské zpravodajství vyhodnotí detekované jevy v kybernetickém prostoru jako nenáležející do jeho pravomoci aktivně proti nim zasáhnout, předá zjištěné data a informace o nich k provedení dalších opatření v případě obrany České republiky primárně Generálnímu štábu Armády České republiky, nebo v případě vnitřní bezpečnosti České republiky jiným státním orgánům, a to zejména Národnímu úřadu pro kybernetickou a informační bezpečnost nebo Policii České republiky. Takto sdílená data se tak stanou předpokladem pro naplnění základní povinnosti České republiky, tedy zabezpečení její bezpečnosti v širším slova smyslu, a to na základě jejich zpravidla společného vyhodnocení. Efektivita takového postupu je tedy vysoce účinná a garantuje správnost a vysokou efektivitu zvolených postupů.

Návrh zákona předpokládá, že mohou nastat situace, kdy na základě detekovaných jevů lze vyhodnotit také jevy (skutečnosti), pro jejichž skutečně účelné řešení nebude vhodné postupovat cestou technologií nebo jinou formou aktivního (vojenského) zásahu. Již v současné době existují v praxi případy, kdy se jako vysoce účelné prokazuje využití diplomatických jednání. V takových případech bude vhodné předat informace např. Ministerstvu zahraničních věcí, které buď svými aktivitami tyto kybernetické útoky a hrozby zcela eliminuje nebo významně podpoří jejich odstranění, popřípadě posílí účinnost přijímaných opatření.

Postup Vojenského zpravodajství při identifikování, vyhodnocování a zvládání hrozeb v kybernetickém prostoru je pak zarámován informačními povinnostmi Vojenského zpravodajství, které jsou zárukou jednak zpětného hodnocení všech skutečností souvisejících s identifikovanou hrozbou a jejím odstraněním, popřípadě zmírněním jejích důsledků, jednak posilováním vnitřní bezpečnosti a obrany České republiky sdílením informací o identifikovaných kybernetických útocích nebo hrozbách tak, aby bylo možné reagovat i na s nimi související jevy nebo nastavovat společné postupy, popřípadě rozvíjet využívané technologie.

K odstavci 3:

Ustanovením § 16e odst. 3 je Vojenskému zpravodajství stanovováno do jisté míry výlučné oprávnění provést aktivní zásah proti zjištěnému útoku nebo hrozbě směřující proti důležitým zájmům státu; toto oprávnění jednak vychází z výlučné povahy kybernetického prostředí, které – na rozdíl od jiných obranných prostředí – vyžaduje v přesně stanovených

situacích provedení příslušných činností bez jakéhokoliv odkladu, jednak je ale limitováno kritérii, kdy může, resp. v zájmu zajištění obrany České republiky v kybernetickém prostoru musí být využito. Prvním z těchto kritérií je hrozba nebezpečí z prodlení, další jsou stanovena zákonem a patří k nim zejména vysoká míra závažnosti dopadů detekovaného kybernetického útoku nebo hrozby.

K § 16f:

Ustanovení obsahuje výčet podmínek, za kterých je Vojenské zpravodajství oprávněno aktivně zasáhnout za účelem odvrácení detekovaného kybernetického útoku či hrozby.

K odstavci 1:

V odstavci 1 jsou uvedeny podmínky, které musí být současně splněny, aby bylo Vojenské zpravodajství oprávněno provést aktivní zásah proti zjištěnému kybernetickému útoku nebo hrozbě. Výkon tohoto oprávnění je podmíněn objektivně vyhodnocenou existencí ohrožení důležitých zájmů státu ve značném rozsahu, jednoznačně identifikovaným kybernetickým útokem nebo hrozbou směřující proti důležitým zájmům státu, které nejsou nahodilé, ale trvají nebo bezprostředně hrozí, a současně směřují proti důležitým zájmům státu a nelze je odvrátit v součinnosti s ozbrojenými silami České republiky (např. z hlediska disponování vhodnou technologií nebo odbornými kapacitami) a aktivní zásah byl vyhodnocen jako jediný možný účinný způsob jejich odvrácení. V žádném jiném případě Vojenské zpravodajství aktivní zásah provést nemůže a vyhodnocenou situaci, byť ohrožuje důležité zájmy státu, musí řešit v součinnosti především s ozbrojenými silami České republiky a dalšími státními orgány.

K odstavci 2:

Další limitace tohoto výlučného oprávnění spočívá v získání nezbytného souhlasu ministra obrany, jako člena vlády České republiky, která odpovídá za přípravu a zajišťování obrany České republiky (viz § 4 zákona č. 222/1999 Sb.).

K odstavcům 3 až 5:

O zahájení aktivního zásahu je Vojenské zpravodajství bezodkladně povinno informovat vládu České republiky, Národní úřad pro kybernetickou a informační bezpečnost a ostatní zpravodajské služby. Tato informační povinnost souvisí jednak s odpovědností vlády České republiky za zajišťování obrany České republiky, ale rovněž s působností uvedených státních orgánů, pro něž by provedení aktivního zásahu nemělo být neznámou skutečností identifikovanou v rámci jím prováděných činností jako negativní zásah proti zájmům státu.

Vojenskému zpravodajství je pak informační povinnost uložena ještě také po provedení aktivního zásahu, a to bezodkladně po jeho ukončení; ta je primárně plněna vůči ministrovi obrany (k tomu viz jeho postavení člena vlády stojícího v čele ministerstva, jenž Vojenské zpravodajství řídí) a dále pak jeho prostřednictvím vůči vládě České republiky, náčelníku Generálního štábu Armády České republiky, řediteli Národního úřadu pro kybernetickou a informační bezpečnost a ostatním zpravodajským službám. V zájmu jejího jednotného obsahu a potřebné vypovídací hodnotě je také určen závazný obsah předávané informace, a to s odkazem na využití struktury záznamu o provedeném aktivním zásahu podle § 16g odst. 2 návrhu zákona.

K odstavci 6:

Navrhovaným ustanovením § 16e odst. 6 je Vojenskému zpravodajství v souvislosti

s plněním povinností při zajišťování obrany v kybernetickém prostoru ukládána součinnostní povinnost, a to v zájmu naplnění obecné povinnosti státu zajistit obranu státu ve všech jejích úrovních jako celek; pokud si stát k obraně státu zřizuje ozbrojené síly, ale současně je mu umožněno využít povinnosti státních orgánů, orgánů územních samosprávných celků a právnických nebo fyzických osob podílet se na zajišťování vnitřní bezpečnosti a obrany České republiky, je zřejmé, že všechny povinné osoby musí postupovat koordinovaně, s jednotně řízeným cílem a pravidly. Proto tam, kde jsou Vojenskému zpravodajství nad rámec jeho obvyklé působnosti svěřovány zvláštní úkoly při obraně České republiky, musí být zajištěna jejich koordinace (součinnost) s dalšími subjekty podílejícími se na zajišťování obrany České republiky, tedy s dalšími státními orgány, ozbrojenými silami České republiky, ozbrojenými bezpečnostními sbory, právnickými a fyzickými osobami a s orgány jiných států, a to zejména pokud působí v oblasti zajišťování kybernetické bezpečnosti nebo obrany České republiky.

Podmínky součinnosti tak, jak jsou upraveny pro účely části čtvrté zákona o Vojenském zpravodajství, je však nutné vnímat skutečně v rámci plnění úkolů svěřených Vojenskému zpravodajství v oblasti jeho podílu na zajišťování obrany státu v rámci kybernetické obrany. V žádném případě pak v rámci této součinnosti není možné poskytovat nebo vyžadovat spolupráci v oblasti trestního řízení apod.

Návrhem zákona jsou součinností vazby upřesňovány, a to pro případy využití výstupů z činností Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu České republiky v kybernetickém prostoru. Poskytnutí součinností je povinností Vojenského zpravodajství, nicméně bude prováděno v takovém rozsahu, aby neohrozilo plnění svých dalších úkolů. Rovněž okruh adresátů této součinnosti je limitován; poskytnout součinnost lze pro výkon úkolů plněných Národním úřadem pro kybernetickou a informační bezpečnost nebo Policie ČR, pouze pokud o to v individuálních případech výlučně pro účely jimi zajišťované bezpečnosti České republiky v kybernetickém prostoru požádají.

K § 16g:

Návrhem zákona je v souvislosti s plněním úkolů při zajišťování obrany v kybernetickém prostoru ukládána Vojenskému zpravodajství povinnost vést o každém provedeném zásahu nebo jiném opatření vážícím se k řešení identifikované hrozby v kybernetickém prostoru záznam, a to v přesně stanovené struktuře, tedy opět se stejnou informační hodnotou každého záznamu. Vedení těchto záznamů má velký význam pro vyhodnocování správnosti a účinnosti zvolených postupů, účelné plánování obrany v této oblasti, ale také pro zajišťování potřebného technického a personálního vybavení Vojenského zpravodajství pro plnění jemu svěřených úkolů.

Návrhem zákona je stanovována jednak struktura záznamu o součinnostním předání dat a informací, které jsou výstupem jím prováděné cílené detekce a identifikace a vyhodnocování jevů nasvědčujících existenci útoku nebo hrozby ohrožujících důležité zájmy státu v kybernetickém prostoru (odstavec 1), jednak struktura záznamu o provedení aktivního zásahu (odstavec 2).

Zpracované záznamy je Vojenské zpravodajství povinno vést 10 let od data jejich zpracování, a to v zájmu možnosti zpětného vyhodnocování prováděných činností nebo jejich porovnání s obdobnými aktivními zásahy v kybernetickém prostoru, ale také v zájmu prováděné kontrolní činnosti.

K § 16h:

K odstavci 1:

Podle § 4 zákona č. 222/1999 Sb. „za přípravu a zajišťování obrany státu odpovídá vláda“, která také vyhodnocuje rizika ohrožení státu, která mohou být příčinou ozbrojeného konfliktu, a činí nezbytná opatření ke snížení, popřípadě vyloučení těchto rizik, a vyhodnocuje úroveň připravenosti státu k zajišťování jeho obrany a v souvislosti s tím předkládá prezidentu republiky a komorám Parlamentu zprávu o zjištěných skutečnostech a navržených opatřeních k posílení obranyschopnosti státu. Je tedy zřejmé, že pokud jsou státnímu orgánu svěřovány úkoly při zajišťování obrany České republiky mimo obecnou koncepci jejich zajišťování ozbrojenými silami, je nezbytné, aby vláda České republiky měla možnost plnit své úkoly a nést odpovědnost za přípravu a zajišťování obrany státu také v oblasti výkonu svěřených úkolů. Návrhem zákona je proto Vojenskému zpravodajství ukládána povinnost informovat vládu České republiky prostřednictvím ministra obrany o plnění svěřených úkolů, a to včetně provedení analýzy účinnosti aktivních zásahů, předání zjištěných skutečností dalším subjektům nebo spolupráce při odstraňování zjištěných hrozeb v kybernetickém prostoru.

K odstavci 2:

V zájmu řádného výkonu činností, jimiž se Vojenské zpravodajství podílí na zajišťování obrany státu, a v zájmu zajištění vysoké kvality přijímaných opatření, nastavování architektury technického řešení a vysoké účinnosti vykonávaných činností je současně návrhem zákona stanovováno, že pokud Orgán nezávislé kontroly zpravodajských služeb České republiky, jemuž jsou v tomto smyslu zákonem o zpravodajských službách České republiky nově stanovovány další působnosti ve vztahu k Vojenskému zpravodajství, vykoná kontrolu Vojenského zpravodajství v rozsahu činností vykonávaných podle návrhu zákona, je povinen předložit vládě České republiky, Poslanecké sněmovně a ministru obrany podrobnou zprávu o této kontrole, a to vždy neprodleně po jejím provedení. Jedná se o zajištění zpětné vazby a možnosti reagovat opatřeními, která povedou k nápravě zjištěných pochybení.

K odstavci 3:

Stejně jako první z uvedených povinností, také povinnost nově ukládaná Vojenskému zpravodajství v § 16h odst. 3 předkládat ministru obrany neprodleně po ukončení kalendářního pololetí písemnou zprávu o stavu jím plněných úkolů, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru, za toto období, navazuje na ustanovení jiného zákona, konkrétně na § 16 odst. 2 písm. e) kompetenčního zákona, jímž je stanoveno, že Ministerstvo obrany řídí Vojenské zpravodajství. Proto je Vojenskému zpravodajství ukládána informační povinnost rovněž vůči ministru obrany, a to jednak v rámci jeho řídící pravomoci vůči Vojenskému zpravodajství jako celku, jednak v rámci zajištění podmínek pro plnění úkolů Ministerstva obrany stanovených v § 6 odst. 1 zákona č. 222/1999 Sb., z nichž lze v souvislosti s plněním povinností Vojenského zpravodajství při zajišťování kybernetické obrany zdůraznit především odpovědnost Ministerstva obrany za proces plánování obrany státu a koordinaci jeho přípravy [§ 6 odst. 1 písm. b) zákona č. 222/1999 Sb.] (k tomu viz § 16d odst. 1 návrhu zákona). Ministr obrany je oprávněn vyžádat kdykoliv jakékoliv informace o zajišťování kybernetické obrany Vojenským zpravodajstvím, pokud jsou nezbytné pro plnění povinností Ministerstva obrany podle § 6 odst. 1 zákona č. 222/1999 Sb., a tedy provázaně k již uvedenému také k nastavení koordinačních vazeb mezi činnostmi Vojenského zpravodajství při zajišťování kybernetické obrany k zajišťování obrany jako celku (a to i pro další činnosti ozbrojených sil České republiky v kybernetickém prostoru).

K § 16i:

Ustanovení § 16i by mohlo být označeno jako ustanovení „záruky“ využívat data

a informace získané Vojenským zpravodajstvím při provádění cílené detekce a identifikace výlučně pro účely zabezpečování činností, jimiž se Vojenské zpravodajství podílí na zajišťování obrany České republiky.

Zákon tak vylučuje případné sdružování takto získaných dat a informací Vojenským zpravodajstvím pro zpravodajskou činnost, a to i přesto, že využití informací získaných zpravodajskou činností se například pro stanovení ukazatelů útoků předpokládá.

Navrhovaným ustanovením § 16i je rovněž zohledněno znění § 16e odst. 2, tedy výjimka z obecné zásady podle § 16i neslučovat data a informace k jiným účelům, než pro plnění úkolů, jimiž se Vojenské zpravodajství podílí na zajišťování obrany České republiky; návrh zákona totiž v § 16e odst. 2 předpokládá předání zjištěných dat a informací k provedení dalších opatření tam, kde je zřejmé, že na jejich základě je nutné zajistit úkony v zájmu zajišťování vnitřní bezpečnosti České republiky, tedy pro stejně významný veřejný zájem, resp. plnění shodné povinnosti státu.

K § 16j a 16k:

K § 16j:

K odstavci 1 a 2:

Návrhem zákona je zřizována funkce inspektora pro kybernetickou obranu, a to jako nezávislé erudované osoby, jejímž posláním je plnění úkolů v oblasti ochrany dat při zajišťování ochrany dat a informací zpracovávaných Vojenským zpravodajstvím při výkonu činností, jimiž se podílí na zajišťování obrany státu v kybernetickém prostoru, ověřování správnosti postupů v této oblasti a dodržování souvisejících povinností Vojenským zpravodajstvím.

Jako nezávislá osoba je inspektor pro kybernetickou obranu pověřen prověřováním správnosti postupů Vojenského zpravodajství při činnostech, jimiž se podílí na zajišťování obrany České republiky v kybernetickém prostoru, **pokud se týkají zabezpečení ochrany dat a informací**, ověřováním účinnosti opatření přijatých Vojenským zpravodajstvím za účelem zajišťování ochrany dat a informací zpracovávaných při činnostech, jimiž se Vojenské zpravodajství podílí na zajišťování obrany státu v kybernetickém prostoru, poskytování vyžádané poradenské podpory příslušníkům Vojenského zpravodajství v oblasti ochrany dat a informací a na **zajišťování účinnosti opatření k dodržování zákona spolupracuje se státními orgány a dalšími právnickými osobami**.

Inspektor pro kybernetickou obranu je funkce zřizovaná za účelem zajišťování nezávislých postupů při prověřování činnosti Vojenského zpravodajství podle návrhu zákona, a to s důrazem na nezávislost prověřování podnětů osob, pokud by se takovou činností cítily dotčeny ve svých právech.

Inspektora pro kybernetickou obranu bude jmenovat vláda České republiky, přičemž návrh na jeho jmenování podává ministr obrany poté, kdy je nominace příslušné osoby projednána v příslušném výboru Poslanecké sněmovny Parlamentu České republiky.

Inspektor pro kybernetickou obranu je jmenován na dobu 5 let.

K odstavcům 3, 4 a 8:

Inspektor pro kybernetickou obranu je vybírán z příslušníků Vojenského zpravodajství. Účelem této úpravy je zejména zajištění přístupu inspektora pro kybernetickou obranu k potřebným informacím, a to včetně zajištění vstupu do prostor Vojenského zpravodajství a přístupu k záznamům vedených o činnostech, jimiž se Vojenské zpravodajství podílí na zajišťování obrany České republiky. Stejně tak inspektor pro kybernetickou obranu v rámci stanovování opatření a poskytování poradenské podpory nemůže mít postavení „vnějšího subjektu" stojícího mimo Vojenské zpravodajství, neboť by to vedlo k vysoké míře neúčinnosti jeho aktivit a nemožnosti zamýšlené komunikace, aniž by nemusely být odstraňovány administrativní bariéry přístupu k utajovaným informacím apod..

Pokud se týká služebního poměru inspektora pro kybernetickou obranu, návrh zákona stanoví, že ve „věcech služebního poměru inspektora pro kybernetickou obranu činí právní úkony jménem České republiky ministr obrany, a to včetně provádění služebního hodnocení inspektora pro kybernetickou obranu". Inspektor pro kybernetickou obranu je tak vyčleněn ze sféry závislosti na řediteli Vojenského zpravodajství při služebním hodnocení a dalších skutečnostech, které by mohly ovlivňovat výkon jeho nezávislé funkce. S tím pak také souvisí úprava, jíž se zakotvuje odpovědnost inspektora pro kybernetickou obranu při plnění úkolů souvisejících s výkonem jeho funkce výlučně vůči ministru obrany.

K odstavci 5:

Nezávislost postavení inspektora pro kybernetickou obranu je výslovně zakotvena v odstavci 5, a to jednak jako deklarace nezávislosti výkonu jeho funkce, resp. její vázanosti pouze právním řádem, jednak jako povinnost inspektora pro kybernetickou obranu vykonávat jemu svěřenou funkci nestranně a výlučně v mezích svého oprávnění; součástí této povinnosti je pak také závazek zdržet se při jejím výkonu všeho, co by mohlo ohrozit důvěru v jeho nestrannost a profesionalitu.

K odstavci 6:

Činnost inspektora pro kybernetickou obranu je prováděna jako součást činností, jimiž se Vojenské zpravodajství podílí na zajišťování obrany České republiky, a to ve prospěch zajištění jejího řádného výkonu zejména v těch oblastech, kde se tato činnost dotýká nebo přímo zasahuje do základních práv a svobod, konkrétně do práva na ochranu soukromí, ochranu osobních údajů a práva na informační sebeurčení. Vzhledem k vysoké citlivosti této oblasti a zejména vzhledem k nezbytnosti neustálého posuzování podmínek výkonu předmětných činností v tom kterém konkrétním případě, je Vojenské zpravodajství povinno zajistit, aby byl inspektor pro kybernetickou obranu náležitě, včas a v potřebném rozsahu zapojen do veškerých záležitostí souvisejících s činnostmi Vojenského zpravodajství, jimiž se podílí na zajišťování obrany České republiky v kybernetickém prostoru, tedy aby měl jednoznačné a kompletní informace o jím posuzovaných činnostech. Toto ustanovení je z hlediska normativního uchopení celé problematiky pro výkon činností inspektora pro kybernetickou obranu klíčové, neboť charakterizuje funkční vztah mezi inspektorem pro kybernetickou obranu a Vojenským zpravodajstvím; Vojenské zpravodajství je totiž inspektorovi pro kybernetickou obranu povinno zpřístupnit veškeré potřebné informace, ty jsou pak dále inspektorem pro kybernetickou obranu posuzovány zcela nezávisle, a to v souladu s právními předpisy a vědomostmi a odbornou erudicí inspektora.

K odstavci 7:

Inspektor pro kybernetickou obranu v souladu se svými povinnostmi analyzovat závěry své činnosti a zasazovat se o zkvalitňování podmínek výkonu činností, jimiž se Vojenské

zpravodajství podílí na zajišťování obrany České republiky zejména z hlediska ochrany práva a právem chráněných zájmů třetích, touto činností dotčených osob, vypracovává vždy v půlročních intervalech hodnotící zprávu. Vzhledem k tomu, že je inspektor pro kybernetickou obranu při výkonu své funkce přímo odpovědný ministru obrany, tuto zprávu, včetně návrhu opatření k nápravě zjištěných nedostatků předává ministru obrany.

Výjimku z tohoto časového intervalu tvoří zprávy o zjištěných závažných nedostatcích, které se mohou týkat například šetření podnětů osob, které se cítí dotčeny na svých právech činností Vojenského zpravodajství, jimiž se podílí na zajišťování obrany České republiky; pokud by takové šetření prokázalo závažné nedostatky s dopady do těchto práv osob, vyhotovenou zprávu předává inspektor pro kybernetickou obranu ministru obrany bezodkladně po jejich zjištění, a to včetně návrhů na jejich odstranění a přijetí preventivních opatření.

K § 16k:

K odstavci 1:

V navrhovaném znění § 16k odst. 1 je proveden taxativní výčet úkolů inspektora pro kybernetickou obranu, jimiž jsou charakterizovány základní oblasti jeho působení. Inspektor pro kybernetickou obranu působí v oblasti prověřování správnosti postupů Vojenského zpravodajství při činnostech, jimiž se podílí na zajišťování obrany České republiky v kybernetickém prostoru, pokud se týkají zabezpečení ochrany dat a informací, ověřování účinnosti opatření přijatých Vojenským zpravodajstvím za účelem zajišťování ochrany dat a informací zpracovávaných při činnostech, jimiž se Vojenské zpravodajství podílí na zajišťování obrany státu v kybernetickém prostoru a poskytování vyžádané poradenské podpory příslušníkům Vojenského zpravodajství v oblasti ochrany dat a informací. Na zajišťování účinnosti opatření přijímaných k ochraně práv spolupracuje se subjekty, u nichž byly umístěny nástroje detekce podle § 16d.

K odstavcům 2 a 3:

Ustanovení odstavce 2 má velký význam pro zajištění práv a právem chráněných zájmů osob, které se mohou cítit nebo skutečně být dotčené na svých právech zásahy vyvolanými činnostmi Vojenského zpravodajství, jimiž se podílí na zajišťování obrany České republiky. Tyto osoby se mohou dovolat prošetření těchto zásahů, a to právě u inspektora pro kybernetickou obranu.

Inspektor pro kybernetickou obranu dodaný podnět prošetří a na základě zjištěných skutečností vypracuje zprávu se svými závěry. Zprávu zašle inspektor pro kybernetickou obranu dané osobě, ministru obrany, řediteli Vojenského zpravodajství a Orgánu nezávislé kontroly zpravodajských služeb České republiky k vyslovení závěru rozhodného pro další postup v dané věci.

Orgán nezávislé kontroly zpravodajských služeb České republiky si pro posouzení věci může vyžádat od Vojenského zpravodajství další doplňující informace, popřípadě stanoviska, tak, aby věc mohl nezávisle a s potřebnými informačními zdroji posoudit.

Závěr Orgánu nezávislé kontroly zpravodajských služeb České republiky o tom, zda byl porušen zákon, se zveřejní způsobem umožňujícím dálkový přístup.

Závěry Orgánu nezávislé kontroly zpravodajských služeb České republiky a inspektora pro kybernetickou obranu je nutné považovat nikoliv pouze jako informační stanovisko objasňující důvody zásahu do práv osob, které se cítí dotčeny na svých právech, ale jako

dokument, o který lze opřít postup dotčené osoby při dovolání se ochrany svých práv v soudním řízení, když samozřejmě není vyloučen ani postup osoby vůči Ministerstvu obrany podle zákona č. 82/1998 Sb., o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem a o změně zákona České národní rady č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád), ve znění pozdějších předpisů, a to v případech, kdy by činností Vojenského zpravodajství vykonávanou při jemu svěřeném podílu na zajišťování obrany České republiky vznikla škoda a odpovědnost za ni by nebyla řešena podle § 16m návrhu zákona.

K § 16l:

K odstavcům 1 a 2:

Pro činnosti Vojenského zpravodajství vykonávané podle nově vkládané části čtvrté zákona o Vojenském zpravodajství nelze využít nastavení kontrolních mechanismů pro zpravodajskou činnost prováděnou Vojenským zpravodajstvím. Proto je návrhem zákona stanovována kontrola Vojenského zpravodajství pro činnosti představující jeho účast na zajišťování obrany České republiky, a to s přihlédnutím k povaze prováděných činností a jejich významu pro zajišťování funkcí státu, v několika úrovních. Základní kontrola je svěřena vládě České republiky (která odpovídá za přípravu zajišťování obrany státu), v další úrovni pak Poslanecké sněmovně Parlamentu České republiky – konkrétně Stálé komisi pro kontrolu činnosti Vojenského zpravodajství a také Orgánu nezávislé kontroly zpravodajských služeb České republiky.

Návrhem zákona je stanoven rozsah dokumentů, které je Vojenské zpravodajství povinno v zájmu účelného provedení kontroly předložit, přičemž je současně umožněno, aby si kontrolující vyžádal zpracování a zpřístupnění dalších souvisejících, avšak účelem kontroly odůvodněných zpráv, nebo poskytnutí dalších informací (odstavce 2 a 3).

K odstavci 3:

Výkon kontroly není omezen například „neukončenými případy Vojenského zpravodajství“, což souvisí s tím, že kontrolu je třeba vnímat jako postup namířený nikoliv vůči zpravodajské činnosti Vojenského zpravodajství, ale výlučně vůči veškerým činnostem, jimiž se Vojenské zpravodajství podílí na zajišťování obrany České republiky.

Kontrolující je však povinen v průběhu kontroly postupovat tak, aby šetřil práva a oprávněné zájmy Vojenského zpravodajství, stejně jako třetích osob, kterým byly v souvislosti s prováděním činností Vojenského zpravodajství, jimiž se podílí na zajišťování obrany České republiky, uloženy povinnosti.

K odstavci 4:

Kontrola činností, jimiž se Vojenské zpravodajství podílí na zajišťování obrany České republiky ze strany Orgánu nezávislé kontroly, nemusí být zahajována pouze z podnětu Stálé komise pro kontrolu činností Vojenského zpravodajství, ale podnět k jejímu zahájení může podat také právnická nebo podnikající fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací, jíž byla uložena povinnost zřídit a zabezpečit rozhraní pro připojení nástroje detekce v určeném bodě veřejné komunikační sítě a povinnost strpět umístění a provozování tohoto nástroje, nebo Český telekomunikační úřad. Adresátem zpráv o výsledku kontroly vykonané na základě takového podnětu je v případě, došlo-li k protiprávnímu zásahu do základních práv a svobod, rovněž podnět podávající osoba, která tak opět získává dokument, který se v případě jejího neuspokojení může využít pro zahájení případného soudního řízení, ve kterém by se dovolávala zajištění ochrany

činnostmi Vojenského zpravodajství, jimiž se podílí na zajišťování obrany České republiky, zasažených práv.

K odstavci 5:

Navrhovaným ustanovením je pak z provádění kontroly Vojenského zpravodajství při provádění činností v zájmu zajišťování kybernetické obrany vyloučen kontrolní řád, neboť vzhledem k povaze prováděných činností, jejich struktuře a času, ve kterém jsou v jednotlivých segmentech vykonávány, je jeho užití nevhodné.

K odstavci 6:

Ministru obrany je pak vzhledem ke skutečnostem uvedeným v odůvodnění k § 16k svěřena pravomoc prověřovat stav přípravy a zajišťování obrany státu v kybernetickém prostoru, na němž se podílí Vojenské zpravodajství. Toto ustanovení navíc opět začleňuje činnosti, jimiž se Vojenské zpravodajství podílí na zajišťování obrany České republiky, do kontextu obrany České republiky jako celku, neboť využívá obecný institut prověřování efektivity stavu obrany České republiky stanoveného v § 41 zákona č. 422/1999 Sb.

K § 16m:

K odstavcům 1 a 2 a 4:

Z povahy činností naplňujících povinnosti při zajišťování kybernetické obrany, například pak také z kritérií pro vyhodnocování identifikovaných hrozeb a rizik v kybernetickém prostoru je zřejmé, že při odvracení nebo zastavení kybernetického útoku nebo odstranění kybernetického rizika nelze vyloučit případy, kdy je nutné přijmout v zájmu ochrany důležitých zájmů státu jako převažující hodnoty skutečnost, že v ojedinělých situacích může vzniknout fyzickým nebo právnickým osobám škoda nebo nemajetková újma; návrh zákona pro tyto případy stanoví specifické postupy, jimiž má být zefektivněno řízení o náhradě škody a její realizace oproti využití postupu obecné úpravy náhrady škody.

Vzhledem k tomu, že návrh zákona řeší také mimořádné situace, kdy by činnostmi Vojenského zpravodajství, jimiž se podílí na zajišťování obrany České republiky, mohlo dojít také k zásahu do základních práv a svobod, je návrhem zákona řešen zvláštní postup nejenom pro škodu, ale také pro nemajetkovou újmu.

Za škodu nebo nemajetkovou újmu způsobenou Vojenským zpravodajstvím odpovídá stát. Náhradu škody nebo nemajetkové újmy poskytuje v zastoupení státu Ministerstvo obrany.

K odstavci 3:

Návrhem zákona je současně řešena situace, kdy povinnost státu k náhradě i prokazatelně vzniklé škody nebo nemajetkové újmy nevznikne. Tato liberace se týká případů škody nebo nemajetkové újmy, na jejímž vzniku se „poškozená“ osoba podílela, tedy způsobená osobou, která vyvolala útok nebo hrozbu. V těchto případech lze naopak předpokládat vůči takové osobě zcela odlišný, sankční postup.

K části druhé – změna zákona o zpravodajských službách

K čl. II

K bodu 1, k navrhované změně § 2:

Ustanovením § 2 zákona č. 153/1994 Sb. je v současné době stanovena působnost zpravodajských služeb České republiky, která je pak následně v § 5 odst. 1 až 3 pro jednotlivé zpravodajské služby upřesňována podle účelu jejich zřízení; v § 5 odst. 4 zákona č. 153/1994 Sb. je pak upravena možnost rozšířit spektrum úkolů plněných zpravodajskými službami nad rámec stanovený v citovaných odstavcích 1 až 3, a to za předpokladu, že tak stanoví „zvláštní zákon nebo mezinárodní smlouva, jíž je Česká republika vázána“. Toto ustanovení však umožňuje rozšířit spektrum úkolů zpravodajských služeb výlučně v mantinelech jejich působnosti tak, jak je stanovena v § 2 zákona č. 153/1994 Sb., tedy v mezích činností charakterizovaných účelem „získávání, shromažďování a vyhodnocování informací důležitých pro ochranu ústavního zřízení, významných ekonomických zájmů, bezpečnost a obranu České republiky“.

V zájmu vytvoření právních podmínek pro realizaci úkolů uložených usnesením vlády České republiky ze dne 25. května 2015 č. 382, kterým schválila Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 a současně uložila Ministerstvu obrany úkol předložit návrh normativního řešení vytvoření podmínek kybernetické obrany České republiky, je pak nutné uvedenou působnost zpravodajských služeb pro Vojenské zpravodajství doplnit o činnosti náležející obecně do působnosti ozbrojených sil České republiky, a to v rozsahu možnosti podílet se na zajišťování obrany České republiky, konkrétně pak se specifickým zaměřením na kybernetickou obranu. Díky navrhované úpravě pak bude možné využít čl. 3 odst. 2 ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky, a vytvořit právní základ pro využití Vojenského zpravodajství v oblasti jeho podílu na zajišťování obrany České republiky v kybernetickém prostoru. Citovaným ustanovením je totiž stanoveno, že „státní orgány, orgány územních samosprávných celků a právnické a fyzické osoby jsou povinny se podílet na zajišťování bezpečnosti České republiky. Rozsah povinností a další podrobnosti stanoví zákon.“, přičemž z této citace je zřejmé, že uvedená povinnost je opět vázána k působnosti příslušného státního orgánu (blíže viz I. kapitola obecné části odůvodnění k návrhu zákona).

Navrhovaná úprava tedy rozšiřuje účel zřízení Vojenského zpravodajství vedle výkonu zpravodajské činnosti také o provádění úkolů, jimiž je zajišťována obrana státu v kybernetickém prostoru.

K bodu 2, k navrhované změně § 12 odst. 1:

Navrhovaná změna ustanovení § 12 odst. 1 zákona č. 153/1994 Sb. se váže k navrhovanému znění § 16l v části první návrhu zákona, jímž se předpokládá, že kontrolu činností, jimiž se Vojenské zpravodajství podílí na zajišťování obrany státu, budou vykonávat také ty subjekty, které se již dnes podílejí na kontrole zpravodajských služeb České republiky.

Proto je také do ustanovení, které v současné době stanoví, že „činnost zpravodajských služeb podléhá kontrole vlády, Poslanecké sněmovny a Orgánu nezávislé kontroly zpravodajských služeb České republiky (dále jen "orgán nezávislé kontroly")“ doplňován text „; kontrole kontrolujícími podléhá rovněž činnost Vojenského zpravodajství, kterou se podílí na zajišťování obrany státu v kybernetickém prostoru podle zákona o Vojenském zpravodajství“. Současně pak platí věta druhá § 12 odst. 1, tedy že i pro doplňovaný specifický

účel „rozsah a způsob kontroly zpravodajských služeb stanoví tento nebo zvláštní zákon“ (viz § 16l).

K části třetí – změna zákona o elektronických komunikacích

K čl. III

K bodu 1

K § 98a:

K odstavci 1:

Nově vkládaný § 98a odst. 1 je provázán k rovněž nově navrhovanému znění § 16d zákona o Vojenském zpravodajství podle čl. I návrhu zákona, a tedy v podstatě lze odkázat také na odůvodnění tohoto ustanovení. Podle něj je právnická nebo podnikající fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinna vyhovět Ministerstvu obrany v jeho žádosti zřídit a zabezpečit v určených bodech jí zajišťované veřejné komunikační sítě rozhraní pro připojení nástroje detekce. Jde o obdobu ustanovení § 97 odst. 1, který je odpovídající k § 9 odst. 5 zákona o Vojenském zpravodajství, a ukládá určeným osobám povinnost součinnosti.

K odstavci 2:

Ustanovení § 98 odst. 2 stanoví povinný technický parametr nástroje detekce (tedy nikoliv obsahový, který je dán stanovenými identifikátory útoku), kterým je požadavek na znemožnění předávání obsahu detekovaných jevů provozu veřejné komunikační sítě a komunikace nástroje detekce s veřejnou komunikační sítí v opačném směru; tento požadavek garantuje minimalizaci zásahů (s výjimkou umístění nástrojů detekce a jejich provozování) do standardního provozu zajišťování veřejné komunikační sítě nebo poskytování veřejně dostupné služby elektronických komunikací.

K odstavci 3:

K ochraně nástroje detekce, a tedy k zajištění bezpečného a efektivního provádění cílené detekce kybernetického prostoru způsobem, který bude garantovat zajišťování obrany České republiky v kybernetickém prostoru, je právnické nebo podnikající fyzické osobě zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací ukládána povinnost do umístěného nástroje detekce zásadně nezasahovat. Je však zřejmé, že pro plnění povinností těchto osob se budou vyskytovat případy, kdy zásah do nástroje detekce bude nutný nebo také i nevyhnutelný. Pro tyto případy bude nutné získat souhlas Vojenského zpravodajství, který jednak umožní Vojenskému zpravodajství pracovat s informací, že nástroj detekce je nefunkční nebo jeho funkčnost je omezena z jemu známých důvodů, jednak dokáže identifikovat záznamy metadat o provozu nástroje detekce jako standardní, nikoliv avizující porušení zákona a ohrožení zajišťování obrany České republiky.

Souhlas Vojenského zpravodajství však není nutný v případech, pokud provedení zásahu do nástroje detekce nebo omezení jeho funkčnosti je nutné vzhledem k tomu, že v souvislosti s jeho připojením a provozováním je vyvolán stav ohrožující samotný provoz veřejné komunikační sítě, poskytování veřejně dostupné služby elektronických komunikací nebo ohrožující zdraví anebo životy fyzických osob, hrozí-li nebezpečí z prodlení. V tomto případě je sledována proporcionalita ochrany zájmu na poskytování konkrétních služeb elektronických

komunikací.

K odstavci 4:

Právnická nebo podnikající fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna umožnit Vojenskému zpravodajství na požádání přístup k nástroji detekce umístěnému na jí zajišťované veřejné komunikační síti, a to v zájmu kontroly správnosti jejího provozu a případné aktualizace indikátorů útoku, tedy aktualizace jeho obsahových funkcí. Vojenské zpravodajství je v těchto případech povinno postupovat tak, aby jeho činností nebyly porušovány podmínky výkonu povinností těmto osobám uložené zákonem o elektronických komunikacích.

K odstavci 5:

V navrhovaném znění § 98a odst. 5 je provedena úprava náhrady nákladů právnické nebo podnikající fyzické osobě zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací, spojených s povinností zřídit a zabezpečit v určených bodech jejich sítě rozhraní pro připojení nástrojů detekce, a to k tíži Vojenského zpravodajství (k tomu viz odůvodnění k § 16d části první návrhu zákona). Součástí tohoto ustanovení je zmocnění k vydání prováděcího předpisu – vyhlášky Ministerstva obrany, která následně stanoví výši, postup uplatnění a způsob určení úhrady za takto vynaložené náklady.

K odstavci 6:

Navrhovaná úprava § 98a odst. 6 stanoví povinnost mlčenlivosti právnické nebo podnikající fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací a osob s ní spolupracujících, a to v plném rozsahu skutečností souvisejících s připojením a užíváním nástroje detekce.

Tato mlčenlivost není časově omezená a trvá i potom, kdy tyto osoby přestanou být nositeli povinnosti zřídit a zabezpečit v určených bodech jimi zajišťovaných sítí rozhraní pro připojení nástrojů detekce.

Takto uložená povinnost mlčenlivosti nemá vliv na povinnost mlčenlivosti podle zákona č. 422/2005 Sb. ve vztahu k utajovaným informacím.

K odstavci 7:

V § 98a odstavci 7 je upraveno jediné prolomení povinnosti mlčenlivosti, a to pro případy podávání informací kontrolujícím, kteří provádějí kontrolu činností Vojenského zpravodajství podle části čtvrté zákona o Vojenském zpravodajství. Toto prolomení povinnosti mlčenlivosti je zcela nezbytné, neboť její zachování by znemožnilo získat pro provádění kontroly nutné a zásadní informace.

K bodu 2

Navrhovaná úprava doplňuje do zákona o elektronických komunikacích nové skutkové podstaty přestupku spočívající v nezřízení a nezabezpečení rozhraní pro umístění nástroje detekce, neumožnění přístupu k němu, neoprávněnému zasahování do nástroje detekce nebo omezení jeho funkčnosti a v porušení mlčenlivosti.

O sankcích za tyto přestupky bude rozhodovat Český telekomunikační úřad, který je garantem nezávislého posouzení naplnění uvedených skutkových podstat a posouzení míry nebezpečnosti naplněné jejich uskutečněním.

K bodům 3 až 5

Jedná se o legislativně technické změny provedené v návaznosti na novelizační body 1 a 2.

K bodu 6

Navrhované znění § 119 odst. 7 doplňuje novou skutkovou podstatu přestupku spočívající v porušení mlčenlivosti uložené podle navrhovaného znění § 98a odst. 6.

K bodu 7

Jedná se o legislativně technickou změnu provedenou v návaznosti na novelizační bod 6.

K bodu 8

Ministerstvo obrany se zmocňuje k vydání vyhlášky, kterou se stanoví způsob určení výše efektivně vynaložených nákladů za zřízení a zabezpečení rozhraní, postup jejich uplatnění a způsob jejich úhrady.

K části čtvrté – ÚČINNOST

K čl. IV

Navrhovanou úpravou se stanoví, že návrh zákona nabývá účinnosti patnáctým dnem po jeho vyhlášení ve Sbírce zákonů. Výjimka z obecného pravidla stanoveného zákonem o Sbírce zákonů a mezinárodních smluv, tj. jednotného nabytí účinnosti právních předpisů k 1. lednu nebo 1. červenci kalendářního roku, je v případě návrhu stanovena z důvodu nutnosti činit okamžitě kroky směrem k započetí faktického výkonu obrany státu v kybernetickém prostoru, aby mohlo být předcházeno kybernetickým útokům či hrozbám, které se v poslední době bohužel čím dál častěji reálně objevují. Navíc jelikož zákon samotný neukládá nestátním adresátům žádné povinnosti, které by bylo nutné plnit okamžitě po nabytí účinnosti zákona, není nutné pro nabytí účinnosti stanovit delší legisvakanční lhůtu ani z jiných důvodů.

V Praze dne 16. března 2020

Předseda vlády:

Ing. Andrej Babiš v. r.

Ministr obrany:

Mgr. Lubomír Metnar v. r.