

Rozdílová tabulka

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

Odůvodnění	Návrh MO	Náš návrh
<p>Monitoring kybernetického prostoru</p> <p>§ 16b odst. 2) a odst. 3)</p> <p>Monitorování kybernetického prostoru bylo dle původního návrhu změny zákona definováno jako nepřetržité vyhodnocování neadresných dat v kybernetickém prostoru, přičemž chyběla jasná definice termínu neadresná data. Gramatickým výkladem termínu neadresná data by bylo možné dojít k chybné interpretaci, že je tímto termínem myšlen samotný obsah zpráv oproštěn o “adresná data”, jako jsou identifikační údaje odesílatelů a příjemců zprávy. V takovém případě by zákon přiznával Vojenskému zpravodajství pravomoc monitorovat a vyhodnocovat samotný obsah zpráv.</p> <p>Monitorování a vyhodnocování samotného obsahu zpráv osob považujeme za nepřipustný zásah do soukromí, pokud má být prováděn plošně a necíleně na veškeré zachycené datové komunikaci. Dle vyjádření pracovníků samotného Vojenského zpravodajství není pro dosažení cíle ustanovení této části zákona - zajištění kybernetické bezpečnosti a obrany České republiky - nezbytné znát obsah zpráv přenášených dat, a že termínem neadresná data byla myšlena pouze metadata informačních paketů.</p> <p>Z tohoto důvodu navrhujeme zaměnit termín “neadresná data” v odstavci 2 za termín, který přesněji definuje okruh monitorovaných a vyhodnocovaných dat. Navrhujeme použití termínu “řídící data paketů”, který v oboru informačních a komunikačních technologiích označuje metadata datových zpráv. Současně navrhujeme nový odstavec 3, kde bude tento termín vymezen negativní i pozitivní definicí. Negativní vymezení pojmu “řídící data paketů” je formulováno tím, že “neobsahují datový obsah paketů”, čímž je v informačních a komunikačních technologiích myšleno datové pole neboli <i>payload</i>, což je samotný obsah zpráv přenášený při přenosu dat. Pozitivní vymezení “řídících dat paketů” je následně vymezeno jako “údaje o zprávě, které jsou nezbytné pro její přenos”.</p>	<p>(2) Monitorováním kybernetického prostoru se rozumí nepřetržité vyhodnocování neadresných dat v kybernetickém prostoru zaručující včasné zjištění bezpečnostních hrozeb pro důležité zájmy státu, posouzení míry jejich intenzity, závažnosti jejich důsledků a způsobu jejich zastavení nebo odvrácení v kybernetickém prostoru. Součástí monitorování kybernetického prostoru není zpracovávání osobních údajů nebo provádění odposlechů a záznamů podle zákona o elektronických komunikacích²¹⁾; monitorováním kybernetického prostoru nesmí být narušena důvěrnost obsahu zprávy a může být prováděno výlučně způsobem vylučujícím zásahy do soukromého života.</p>	<p>(2) Monitorováním kybernetického prostoru se rozumí nepřetržité vyhodnocování metadat zpráv v kybernetickém prostoru za účelem včasného zjištění bezpečnostních hrozeb pro důležité zájmy státu, posouzení míry jejich intenzity, závažnosti jejich důsledků a možností jejich zastavení nebo odvrácení. Součástí monitorování kybernetického prostoru není zpracovávání osobních údajů nebo provádění odposlechů a záznamů podle zákona o elektronických komunikacích²¹⁾.</p> <p>(3) Metadaty zprávy se rozumí takové údaje o zprávě, které jsou nezbytné pro její přenos. Součástí metadat není samotný obsah zprávy.</p>

<p>Úpravu odstavce 2 a doplnění § 16b o odstavec 3 považujeme za nezbytné z důvodu jasného vymezení monitorovaných a vyhodnocovaných dat, aby nemohlo dojít k chybné interpretaci ustanovení zákona a následně k jeho zneužití zpracováváním jiných než vymezených dat. Je nezbytné v zákoně jasně vymezit rozsah monitorovaných a vyhodnocovaných dat, protože představuje zásah do základních lidských práv, který vyžaduje jasné zákonné omezení.</p>		
<p>§ 16b odst. 4)</p> <p>Původní návrh změny zákona uvádí v odstavci 2 § 16b, že “monitorováním kybernetického prostoru nesmí být narušena důvěrnost obsahu zprávy a může být prováděno výlučně způsobem vylučujícím zásahy do soukromého života.” Taková formulace jde proti samotnému významu pravomocí udělených Vojenskému zpravodajství tímto paragrafem, proto vyžaduje přeformulovat tak, aby odpovídala záměru navrhovaného zákona. Důvěrnost obsahu zprávy a zásahy do soukromého života jsou dotčeny ze samotné podstaty monitoringu a vyhodnocování řídicích dat paketů v kybernetickém prostoru.</p> <p>Se zásahem do soukromé sféry občanů v důsledku monitoringu kybernetického prostoru navíc počítá v tomto smyslu také samotná důvodová zpráva k návrhu změny zákona, kde se zvažuje proporcionalita mezi ochranou národní bezpečnosti a základními lidskými právy a svobodami, chráněnými 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. Dle navrhované právní úpravy je vystaven zásahu do svých práv prakticky každý uživatel telekomunikačních sítí.</p> <p>Skutečnost, že se v případě nakládání s metadaty v elektronické komunikaci jedná o zásah do soukromí dle článku 10 (práva na ochranu před neoprávněným zasahováním do soukromého a rodinného života a před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě) a článku 13 Listiny základních práv a svobod (právo na zachování tajemství zpráv podávaných telefonem či jiným podobným zařízením), předpokládá také Ústavní soud České republiky v nedávném nálezu Pl. ÚS 45/17 ze dne 22. května 2019. V tomto řízení Ústavní soud zkoumal střet zmíněných práv mimo jiné také z důvodu ochrany národní bezpečnosti. Soud zkoumal omezení těchto základních lidských práv z důvodu preventivního uchovávání provozních a lokalizačních údajů o elektronické komunikaci u poskytovatelů telekomunikačních služeb, což jsou data svým charakterem podobná těm, která mají být předmětem monitoringu a vyhodnocování Vojenským zpravodajstvím.</p> <p>Navrhujeme, aby znění zákona tento zásah do práv a svobod na deklaratorní úrovni připustilo do nového odstavce 4 § 16b, ale současně aby deklarovalo, že jiným než uvedeným způsobem nebudou základní práva a svobody narušeny, a že k tomu bude docházet jen v</p>	<p>(2) Monitorováním kybernetického prostoru se rozumí nepřetržité vyhodnocování neadresných dat v kybernetickém prostoru zaručující včasné zjištění bezpečnostních hrozeb pro důležité zájmy státu, posouzení míry jejich intenzity, závažnosti jejich důsledků a způsobu jejich zastavení nebo odvrácení v kybernetickém prostoru. Součástí monitorování kybernetického prostoru není zpracovávání osobních údajů nebo provádění odposlechů a záznamů podle zákona o elektronických komunikacích²¹); monitorováním kybernetického prostoru nesmí být narušena důvěrnost obsahu zprávy a může být prováděno výlučně způsobem vylučujícím zásahy do soukromého života.</p>	<p>(4) Zásahy do soukromí osoby při monitorování kybernetického prostoru jsou přípustné pouze tehdy, pokud jsou nezbytné k dosažení cíle uvedeného v odstavci 2, tohoto cíle nelze efektivně dosáhnout jinak a zásah do soukromí je přiměřený bezpečnostní hrozbě, který má být odvrácena.</p>

nezbytné míře v demokratické společnosti, což vyplývá již ze samotného výkladu Listiny a Úmluvy.		
Zásah v kybernetickém prostoru		
<p>§ 16c odst. 2)</p> <p>Návrh ministerstva je neurčitý a nejasný. Především chybí upřesnit, jak je definován “aktivní zásah”. Stejně tak v celém právním řádě dosud chybí definice pojmu “kybernetický útok”. Přitom se jedná o dosti zásadní pojmy, na jejichž základě bude možné použít mimořádně silné mocenské nástroje státu, de facto nasazení armády v kyberprostoru. Oprávnění “aktivně zasáhnout” nemůže zůstat s takto nedostatečnou zákonnou definicí. Požadujeme podrobného přepracování daného ustanovení, aby aktivní zásah měl jasné mantinely a pravidla.</p> <p>Navrhujeme znění v podobě, že na základě provedení vyhodnocení rozhodne Vojenské zpravodajství, zda zasáhne v kyberprostoru na území České republiky za účelem zastavení nebo odvrácení kybernetického útoku, případně za účelem odstranění bezpečnostní hrozby. Prostorové vymezení zásahu na kyberprostor na území České republiky zajistí, že se nebude v případě zásahu moci jednat o válečnou operaci v kyberprostoru na území cizího státu. Pojem “aktivně zasáhne” lze gramaticky zredukovat na pouhé “zasáhne”, přičemž pravomoc orgánu provést operaci zůstane nezměněná a sníží to možnosti interpretace rozsáhlejších pravomocí.</p>	<p>(2) Na základě provedení vyhodnocení podle odstavce 1 rozhodne Vojenské zpravodajství, zda</p> <p>a) aktivně zasáhne za účelem zastavení nebo odvrácení kybernetického útoku, případně za účelem odstranění bezpečnostní hrozby, nebo</p> <p>b) předá zjištěné informace k provedení dalších opatření k zajištění bezpečnosti České republiky podle jejich povahy:</p> <p>1. Generálnímu štábu Armády České republiky k provedení opatření k zajištění obrany České republiky ozbrojenými silami České republiky, nebo</p> <p>2. Národnímu úřadu pro kybernetickou a informační bezpečnost k provedení opatření směřujících k zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru, nebo</p> <p>3. Ministerstvu vnitra k provedení opatření k zajištění bezpečnosti České republiky ozbrojenými bezpečnostními sbory, a to s přihlédnutím k působnosti uvedených státních orgánů.</p>	<p>(2) Na základě provedení vyhodnocení podle odstavce 1 rozhodne Vojenské zpravodajství, zda</p> <p>a) zasáhne v kybernetickém prostoru na území České republiky za účelem zastavení nebo odvrácení kybernetického útoku, případně za účelem odstranění bezpečnostní hrozby, nebo</p> <p>b) předá zjištěné informace k provedení dalších opatření k zajištění bezpečnosti České republiky podle jejich povahy:</p> <p>1. Generálnímu štábu Armády České republiky k provedení opatření k zajištění obrany České republiky ozbrojenými silami České republiky, nebo</p> <p>2. Národnímu úřadu pro kybernetickou a informační bezpečnost k provedení opatření směřujících k zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru, nebo</p> <p>3. Ministerstvu vnitra k provedení opatření k zajištění bezpečnosti České republiky ozbrojenými bezpečnostními sbory, a to s přihlédnutím k působnosti uvedených státních orgánů.</p>

<p>§ 16c odst. 4)</p> <p>Navrhovaná úprava dává dle § 16a odst. 1) Vojenskému zpravodajství povinnost odvrátit nebo snížit účinky při ochraně důležitých zájmů státu identifikované v kybernetickém prostoru při dvou alternativních okolnostech. Za prvé má Vojenské zpravodajství tuto povinnost, pokud je odvrácení nebo snížení účinku vzhledem k intenzitě ohrožení nezbytné provést okamžitě po jeho zjištění. Druhou alternativní možností, kdy tato povinnost Vojenskému zpravodajství vzniká je, pokud k zastavení nebo odvrácení ohrožení nedisponují ozbrojené síly nebo ozbrojené bezpečnostní sbory potřebnými silami nebo prostředky.</p> <p>Obě tyto vzájemně se vylučující možnosti (spojka “anebo”) jsou novou pravomocí výkonné moci provádět vojenské operace v kyberprostoru. Prakticky se jedná o situaci analogickou té, o které dnes běžně rozhoduje vláda (§ 4 a § 5 zákona č. 222/1999 Sb., o zajišťování obrany České republiky a čl. 43 odst. 4 Ústavy ČR) a nikoliv pouze ministr obrany. Není žádný důvod, proč by o opatřeních jinak prováděných ozbrojenými silami státu měl rozhodovat sám ministr obrany, pokud se jedná o ohrožení, které není natolik intenzivní, aby bylo nezbytné provést opatření okamžitě po jeho zjištění.</p> <p>Teoreticky by mohla být druhá alternativní povinnost Vojenského zpravodajství dle návrhového § 16a odst. 1) naplňována na základě povinnosti poskytnout součinnost nebo podporu vykonávaných opatření ozbrojeným silám České republiky nebo ozbrojeným bezpečnostním sborům, pokud o to v individuálních případech výlučně pro účely jimi zajišťování bezpečnosti nebo obrany České republiky v kybernetickém prostoru požádají (dle § 16f odst 4). Tím spíše by byla nutná vyšší míra kontrola těchto opatření.</p> <p>Navrhujeme znění odstavce 4 tak, aby rozlišoval nutný souhlas k provedení opatření podle odstavce 2 písm. a) tak, že bude zohledněna nutnost časové nezbytnosti. V první variantě, kdy je zásah nutné provést okamžitě po jeho zjištění, by stačil pouhý souhlas ministra obrany, který by tím získal novou pravomoc. V druhé variantě, kdy ozbrojené síly nebo bezpečnostní složky disponují potřebnými silami nebo prostředky by byl potřeba souhlas vlády analogicky situacím, kdy o opatřeních při obraně České republiky rozhoduje vláda dle článku 43 odst. 4 Ústavy a § 5 zákona č. 222/1999 Sb., o zajišťování obrany České republiky.</p>	<p>(4) K provedení opatření podle odstavce 2 písm. a) je nutný souhlas ministra obrany.</p>	<p>(4) K provedení opatření podle odstavce 2 písm. a) je nutný souhlas a) ministra obrany v případě, že je jeho provedení vzhledem k intenzitě kybernetického útoku nebo bezpečnostní hrozby nezbytné okamžitě po jeho zjištění, anebo b) vlády v případě, že k zastavení nebo odvrácení kybernetického útoku nebo bezpečnostní hrozby nedisponují ozbrojené síly nebo ozbrojené bezpečnostní sbory potřebnými silami nebo prostředky.</p>
<p>Soudní ochrana provozovatelů sítě</p>		
<p>§ 16g odst. 3)</p> <p>Navrhované ustanovení obsahuje nesprávné označení opravného prostředku proti rozhodnutí ministerstva jako “odvolání”, které je potřeba zaměnit za “rozklad”. Dle § 152 Správního řádu (zákon č. 500/2004 Sb.) lze proti rozhodnutí, které vydal ústřední správní úřad, ministr nebo</p>	<p>(3) K zajištění účelu podle odstavce 1 vydá Ministerstvo obrany rozhodnutí, jímž právnické nebo podnikající fyzické osobě zajišťující síť elektronických</p>	<p>(3) K zajištění účelu podle odstavce 1 vydá Ministerstvo obrany rozhodnutí, jímž právnické nebo podnikající fyzické osobě zajišťující síť elektronických komunikací nebo</p>

<p>vedoucí jiného ústředního správního úřadu v prvním stupni, podat jako opravný prostředek rozklad.</p> <p>Navrhujeme do návrhu doplnit, aby Ministerstvo obrany při ukládání povinnosti rozhodlo také o časovém období, po které má být sonda připojena. Časově neomezené rozhodnutí by vytvořilo trvalou povinnost provozovatelů sítí strpět umístění sondy a to bez ohledu na aktuální potřebnost. Časové omezení může zajistit opětovnou kontrolu potřebnosti ze strany ministerstva.</p>	<p>komunikací nebo poskytující službu elektronických komunikací uloží povinnost zabezpečit rozhraní pro připojení sond určených k monitorování kybernetického prostoru a povinnost strpět umístění a provozování tohoto zařízení. Rozhodnutí podle věty první obsahuje výrokovou část a poučení účastníků; odvolání proti rozhodnutí nemá odkladný účinek.</p>	<p>poskytující službu elektronických komunikací uloží povinnost zabezpečit rozhraní pro připojení sond určených k monitorování kybernetického prostoru a povinnost strpět umístění a provozování tohoto zařízení, včetně časového období, po kterou má být toto zařízení umístěno. Rozhodnutí podle věty první obsahuje výrokovou část a poučení účastníků; rozklad proti rozhodnutí nemá odkladný účinek.</p>
<p>Spolupráce Vojenského zpravodajství s tuzemskými a zahraničními orgány</p>		
<p>§ 16f odst. 4)</p> <p>Navrhujeme z navrhovaného ustanovení vyjmout možnost, aby mohly ozbrojené bezpečnostní sbory (Policie ČR a případně další) po Vojenském zpravodajství požadovat povinnost poskytnout součinnost nebo podporu jimi vykonávaných opatření. Z důvodové zprávy není zřejmé, k jakému účelu by mohla policie a případně další bezpečnostní sbory požadovat od Vojenské rozvědky povinnost součinnosti při jimi vykonávaných úkolech. Možnost spolupráce mezi bezpečnostními sbory a Vojenskou rozvědkou přitom umožňuje již odstavec 1 stejného paragrafu.</p> <p>Formulace v původním návrhu § 16f odst. 4 neobsahuje záruky, že informace získané v rámci monitoringu provozu (§ 16b) nebudou moci být díky tomuto ustanovení použity pro účely trestního řízení jako operativní poznatky. Původní návrh bez vysvětlení případů, při kterých může policie nebo jiné bezpečnostní sbory úkolovat Vojenskou rozvědku, považujeme z uvedených důvodů za problematický. Případně požadujeme doplnění možných případů, při kterých by bezpečnostní sbory požadovali povinnost součinnosti při plnění jejich úkolů.</p>	<p>(4) Vojenské zpravodajství je při plnění úkolů podle § 16a odst. 1 povinno poskytnout součinnost nebo podporu vykonávaných opatření ozbrojeným silám České republiky nebo ozbrojeným bezpečnostním sborům, pokud o to v individuálních případech výlučně pro účely jimi zajišťování bezpečnosti nebo obrany České republiky v kybernetickém prostoru požádají; tím není dotčena povinnost Vojenského zpravodajství podle odstavce 1.</p>	<p>(4) Vojenské zpravodajství je při plnění úkolů podle § 16a odst. 1 povinno poskytnout součinnost nebo podporu vykonávaných opatření ozbrojeným silám České republiky, pokud o to v individuálních případech výlučně pro účely jimi zajišťování bezpečnosti nebo obrany České republiky v kybernetickém prostoru požádají; tím není dotčena povinnost Vojenského zpravodajství podle odstavce 1.</p>
<p>§ 16f odst. 5)</p> <p>Ministerstvem navrhovaný § 16f odst. 1 připouští, že Vojenské zpravodajství při plnění úkolů na kybernetické obraně České republiky spolupracuje s orgány jiných států, přičemž neobsahuje bližší spolupráci, na základě jakých principů by měla tato spolupráce probíhat. Účelem zahraniční spolupráce nesmí být plošné předávání dat nebo zpřístupnění sond</p>	<p>nebyl</p>	<p>(5) Vojenské zpravodajství není oprávněno zpřístupnit sondy nebo plošný obsah dat získaných při monitoringu kybernetického prostoru prováděný dle § 16b spolupracujícím orgánům jiných</p>

<p>samotných. Navrhujeme proto v novém odstavci 5 zakotvení ochrany osobních údajů obyvatel s ohledem na předávání informací od zahraničí. Podle námi navrhovaného ustanovení by Vojenské zpravodajství nemělo oprávněno zpřístupnit sondy nebo plošný obsah dat získaných při monitoringu kybernetického prostoru spolupracujícím orgánům jiných států, přičemž by mohlo na dožádání orgánů jiných států předávat informace získané při monitoringu pouze v individuálních odůvodněných případech.</p> <p>V této souvislosti je potřeba doplnit, že obecným problémem zpravodajských služeb v České republice je nedostatečné zákonné ošetření zásad zahraniční zpravodajské spolupráce. Agentura Evropské unie pro základní práva (<i>European Union Agency for Fundamental Rights</i>) vydala v roce 2017 srovnávací analýzu právních předpisů Sledování zpravodajskými službami: záruky ochrany základních práv a prostředky nápravy v Evropské unii – díl II. Podle agentury mají téměř všechny členské státy zákony o mezinárodní zpravodajské spolupráci. Třetina z nich ukládá zpravodajským službám, aby stanovily vnitřní předpisy pro postupy a metody mezinárodní spolupráce, včetně ochranných opatření při sdílení údajů. Několik členských států pak umožňuje vnější posouzení dohod o mezinárodní zpravodajské spolupráci. Dle stanoviska agentury: <i>“Členské státy EU by měly stanovit pravidla pro způsob mezinárodní výměny zpravodajských informací.”</i></p> <p>V České republice samostatný zákon o mezinárodní zpravodajské spolupráci neexistuje a není tato spolupráce dostatečně ošetřena ani v zákoně o zpravodajských službách či v zákoně o Vojenském zpravodajství. Nedostatek zákonného ošetření mezinárodní spolupráce zpravodajských služeb je proto zásadním deficitem současné právní úpravy v České republice.</p>		<p>států. V individuálních odůvodněných případech může na žádost orgánů jiných států předávat informace získané při monitoringu.</p>
<p>Náhrada škody</p>		
<p>§ 16k</p> <p>Navrhované ustanovení o náhradě škody považujeme za nedostatečné. Z toho důvodu navrhujeme rozšířit dané ustanovení tak, aby byly zohledněny všechny formy škody, které mohou v důsledku nových pravomocí a povinností Vojenského zpravodajství občanům vzniknout, a aby mohly být řádně nahrazeny.</p> <p>Obecná právní úprava o náhradách škody (zákona č. 82/1998 Sb., o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem) poskytuje náhrady v případě, že škoda vznikla v důsledku nezákonného rozhodnutí či nesprávného úředního postupu. V obecné rovině musí být dle uvedeného zákona pro vznik odpovědnosti státu splněny tři kumulativní podmínky (nesprávný úřední postup, vznik škody a existence příčinné souvislosti mezi nimi). V případě, že je státní orgán zmocněn k novým</p>	<p>§ 16k Náhrada škody</p> <p>V případě, že při odvracení nebo zastavení kybernetického útoku nebo odstranění kybernetického rizika vznikne škoda, postupuje Ministerstvo obrany podle obecných právních předpisů upravujících náhradu škody.</p>	<p>§ 16k Náhrada škody</p> <p>(1) Ministerstvo obrany je povinno nahradit škodu způsobenou právnícké nebo podnikající fyzické osobě zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací a) v souvislosti s monitoringem kybernetického prostoru, pokud dojde k ovlivnění plnění povinností této osoby vůči uživatelům sítě;</p>

<p>oprávněním či povinností, při kterých by občanům nebo provozovatelům sítě mohla vzniknout škoda, může být pro vymahatele škody problematické prokázat nesprávný úřední postup. Z toho důvodu navrhuje vyjmenovat možné situace, při kterých mohou vzniknout škody při výkonu oprávnění a povinností Vojenského zpravodajství a určit povinnost státu vzniklou škodu nahradit.</p> <p>Navrhujeme, aby měl stát vůči provozovatelům sítě povinnost nahradit škody vzniklé v souvislosti s monitoringem kybernetického prostoru, pokud dojde k ovlivnění plnění povinností této osoby vůči uživatelům sítě. Tuto možnost škody provozovatelů sítí připouští také ustanovení § 16f odst. 3 písm. c), které tvrdí, že monitorování kybernetického prostoru může ovlivňovat plnění povinností právnické nebo podnikající fyzické osoby zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací vůči uživatelům sítě. Na takto vzniklé škody by se totiž ve všech případech nemusel vztahovat navrhovaný § 98a odstavec 3) zákona o elektronických komunikacích, který stanoví úhrada nákladů za zřízení a zabezpečení sondy umožňující monitorování kybernetického prostoru.</p> <p>Dále navrhuje, aby měl stát vůči provozovatelům sítě povinnost nahradit škody vzniklé v důsledku cíleného kybernetického útoku na infrastrukturu této osoby v souvislosti s umístěním sondy zřízené za účelem monitoringu kybernetického prostoru. Povinnost státu by v tomto případě nevznikla, pokud by provozovatel sítě vyvolala kybernetický útok proti sobě v souvislosti porušením povinnosti zachovávat mlčenlivost o umístění sondy.</p> <p>V dalších dvou odstavcích daného paragrafu navrhuje uvést, že stát je povinen nahradit škodu způsobenou Vojenským zpravodajstvím v souvislosti s aktivním zásahem v kybernetickém prostoru, a že ve zbytku se postupuje podle obecných právních předpisů upravujících náhradu škody.</p>		<p>b) pokud dojde k cílenému kybernetickému útoku na infrastrukturu této osoby v souvislosti s umístěním sondy zřízené za účelem monitoringu kybernetického prostoru.</p> <p>(2) Povinnost státu podle odstavce 1) písmene b) nevznikne, pokud se jedná o škodu způsobenou osobě, která vyvolala kybernetický útok proti sobě v souvislosti porušením povinnosti zachovávat mlčenlivost dle § 98a odst. 4 zákona o elektronických komunikacích.</p> <p>(3) Ministerstvo obrany je povinno nahradit škodu způsobenou Vojenským zpravodajstvím v souvislosti s aktivním zásahem dle § 16c odstavce 2 písm. a).</p> <p>(4) V případě, že při vykonávání oprávnění a povinností Vojenského zpravodajství při zajišťování bezpečnosti České republiky v kybernetickém prostoru vznikne jiná škoda než uvedená v odst. 1 až 3, postupuje Ministerstvo obrany podle obecných právních předpisů upravujících náhradu škody.</p>
<p>Kontrola Vojenského zpravodajství</p>		
<p>§ 22 odst. 3)</p>	<p>(3) Ředitel Vojenského zpravodajství předkládá kontrolnímu orgánu na jeho požádání</p>	<p>(3) Ředitel Vojenského zpravodajství předkládá kontrolnímu orgánu na jeho požádání zejména</p>

<p>Vytvoření silného mechanismu dohledu je zásadní součástí systému odpovědnosti zpravodajských služeb obecně. Rámec dohledu kontrolních orgánů by proto měl odpovídat pravomocem, které jsou Vojenskému zpravodajství svěřeny. Vyplývá to z výsledků výzkumu, který Agentura Evropské unie pro základní práva (<i>European Union Agency for Fundamental Rights</i>) vydala v roce 2017 v publikaci Sledování zpravodajskými službami: záruky ochrany základních práv a prostředky nápravy v Evropské unii – díl II. Zmíněná zpráva porovnává činnost a zákonné ukotvení zpravodajských služeb ve všech státech EU. Část stanoviska 3 z tohoto reportu uvádí: <i>“Členské státy EU by měly zřídit spolehlivý rámec dohledu odpovídající pravomocem a kapacitám zpravodajských služeb. Členské státy by orgánům dohledu měly rovněž poskytnout pravomoc zahajovat vlastní vyšetřování jakož i trvalý, úplný a přímý přístup k informacím a dokumentům nezbytným k plnění jejich role.”</i></p> <p>Z důvodu naplnění lepší funkce parlamentní kontroly Vojenského zpravodajství navrhneme doplnit seznam informací, které by ředitel Vojenského zpravodajství poskytoval na požádání orgánu parlamentní kontroly. Konkrétně se jedná o tři typy informací: 1) roční a pololetní zprávu o plnění úkolů na zajišťování kybernetické obrany a bezpečnosti České republiky a vyhodnocení jejich účinnosti (vypracovává Vojenské zpravodajství dle § 16i), 2) záznamy o řešení kybernetických útoků (vypracovává Vojenské zpravodajství dle § 16e), a 3) rozhodnutí Ministerstva obrany vydaná k umístění sondy u provozovatelů sítě (vypracovává Ministerstvo obrany základě § 16g odst. 3. a zmocňuje Vojenské zpravodajství k umístění sond).</p> <p>Považujeme za nezbytné oprávnění k předání uvedených informací kontrolnímu orgánu od Vojenského zpravodajství uvést výslovně v zákoně. Praxe při kontrolách zpravodajských služeb výslovné uvedení konkrétních dokumentů vyžadují. Bez jejich uvedení by ředitel Vojenského zpravodajství mohl argumentovat, že nemá pravomoc tyto informace předávat. Pokud by nebylo výslovné zmocnění ředitele Vojenského zpravodajství uvedené informace parlamentnímu kontrolnímu orgánu předat, byla by kontrola uvedených dokumentů ze strany orgánů nezávislých na vládě zásadně ztížena. Toto ustanovení tak napomáhá správnému nastavení principu brzd a protiváh v demokratickém systému. Zákonodárná moc tím lépe kontroluje moc výkonou.</p> <p>Taxativní výčet dokumentů, které ředitel Vojenského zpravodajství předkládá kontrolnímu orgánu na jeho požádání, navrhneme změnit na demonstrativní výčet přidáním slova “zejména”. Taxativní výčet dokumentů předkládaných ředitelem Vojenského zpravodajství, omezuje výkon parlamentní kontroly pouze na dokumenty uvedené v tomto seznamu. Považujeme za žádoucí, aby kontrolní orgán měl potenciální možnost přístupu také k dalším dokumentům Vojenského zpravodajství.</p>	<p>a) zprávu o činnosti Vojenského zpravodajství¹¹⁾, b) zprávu o použití zpravodajských prostředků, vyjma zpravodajských prostředků použitých při zabezpečování informací majících původ v zahraničí¹²⁾, a to pouze ve věcech a v případech, ve kterých Vojenské zpravodajství svou činnost již ukončilo, c) souhrnnou informaci obsahující zaměření a počet případů a věcí, v nichž je Vojenské zpravodajství činné, vyjma případů a věcí při zabezpečování informací majících původ v zahraničí¹²⁾; v informaci odliší případy a věci podle zvláštního právního předpisu¹³⁾, d) počet případů, ve kterých byla podána žádost o poskytnutí zprávy bankou nebo pobočkou zahraniční banky o záležitostech týkajících se klienta, které jsou předmětem bankovního tajemství¹⁸⁾, e) zprávu o využívání žádostí o poskytnutí zprávy bankou nebo pobočkou zahraniční banky o záležitostech týkajících se klienta, které jsou předmětem bankovního tajemství¹⁸⁾, a to pouze ve věcech a případech, ve kterých Vojenské zpravodajství svou činnost již ukončilo.</p>	<p>a) zprávu o činnosti Vojenského zpravodajství¹¹⁾, b) zprávu o použití zpravodajských prostředků, vyjma zpravodajských prostředků použitých při zabezpečování informací majících původ v zahraničí¹²⁾, a to pouze ve věcech a v případech, ve kterých Vojenské zpravodajství svou činnost již ukončilo, c) souhrnnou informaci obsahující zaměření a počet případů a věcí, v nichž je Vojenské zpravodajství činné, vyjma případů a věcí při zabezpečování informací majících původ v zahraničí¹²⁾; v informaci odliší případy a věci podle zvláštního právního předpisu¹³⁾, d) počet případů, ve kterých byla podána žádost o poskytnutí zprávy bankou nebo pobočkou zahraniční banky o záležitostech týkajících se klienta, které jsou předmětem bankovního tajemství¹⁸⁾, e) zprávu o využívání žádostí o poskytnutí zprávy bankou nebo pobočkou zahraniční banky o záležitostech týkajících se klienta, které jsou předmětem bankovního tajemství¹⁸⁾, a to pouze ve věcech a případech, ve kterých Vojenské zpravodajství svou činnost již ukončilo, f) roční a pololetní zprávu o plnění úkolů podle § 16a odst. 1 a vyhodnocení jejich účinnosti, zpracovávané Vojenským zpravodajstvím dle § 16i,</p>
---	--	--

		g) záznamy provedených opatření vedených podle § 16e, nebo h) rozhodnutí Ministerstva obrany vydaná na základě § 16g odst. 3.
<p>§ 23a</p> <p>Navrhujeme do zákona doplnit ustanovení, že kontrolní orgán dle § 21 a dále Orgán nezávislé kontroly zpravodajských služeb České republiky (dle zákona č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů) je oprávněn od poskytovatele sítě požadovat informace o monitorování kybernetického prostoru. Toto poskytování informací kontrolním orgánům od poskytovatelů sítě navrhujeme současně vyjmout z povinnosti mlčenlivosti (v zákoně o elektronických komunikacích).</p> <p>Navrhované ustanovení je nezbytné pro řádný výkon činnosti kontrolních orgánů. V situaci, kdyby bylo monitoringu zneužito, neměl by bez tohoto ustanovení poskytovatel sítě možnost na tuto skutečnost upozornit kontrolní orgány, které jsou nezávislé na výkonné moci.</p>	nebyl	<p>§ 23a</p> <p>Kontrolní orgán dle § 21 a Orgán nezávislé kontroly zpravodajských služeb České republiky je oprávněn požadovat od právnické nebo podnikající fyzické osoby zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací informace o monitorování kybernetického prostoru Vojenským zpravodajstvím prostřednictvím sítí a služeb elektronických komunikací.</p>

Změna zákona o elektronických komunikacích

Připojení sondy u provozovatele sítě		
<p>§ 98a odst. 1)</p> <p>Navrhované ustanovení o připojení sondy do sítě je z hlediska zajištění dobré praxe nedostatečně formulované. Především chybí bližší specifikace sondy - např. zda se jedná o software či hardware. Navrhujeme do návrhu doplnit, že sonda je pasivním hardwarovým zařízením, které je do zřízeného rozhraní připojeno odbočně.</p> <p>Nezbytnost použití pasivních typů sond je především v možnosti zneužití sond aktivních. Pasivní sondu je možné plně využít k mapování komunikačních toků. Taková sonda plně dostačuje k monitoringu kybernetického prostoru a současně zajišťuje ochranu dat občanů před možným zneužitím. Aktivní sonda je zapojena tzv. in-line, přímo v cestě, zatímco pasivní</p>	<p>§ 98a</p> <p>(1) Právnická nebo podnikající fyzická osoba zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací je povinna na základě rozhodnutí vydaného Ministerstvem obrany podle zákona o Vojenském zpravodajství⁽⁷⁰⁾ zřídit a zabezpečit ve vhodných bodech jí provozované sítě rozhraní pro připojení sondy</p>	<p>§ 98a</p> <p>(1) Právnická nebo podnikající fyzická osoba zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací je povinna na základě rozhodnutí vydaného Ministerstvem obrany podle zákona o Vojenském zpravodajství⁽⁷⁰⁾ zřídit a zabezpečit ve vhodných bodech</p>

<p>sonda je zapojena na odbočce, proto požadujeme také doplnit, že sonda je na zřízeném rozhraní připojena odbočně.</p> <p>Aktivní sonda by mohla do komunikace také přímo vstupovat. Mohla by selektivně blokovat některé komunikační toky (například blokovat vybrané weby) nebo se vydávat za některého z účastníků komunikace. Rizikem je u aktivních sond také podvržení kanálu s aktualizacemi operačního systému nebo mobilního telefonu, v důsledku kterého by došlo k úplnému ovládnutí koncového zařízení. Tyto funkce nejsou k účelu monitoringu kybernetického prostoru potřeba, ale je u nich riziko zneužití.</p> <p>Jako další pojistku před zneužitím do ustanovení navrhuje, aby rozhraní pro připojení sondy muselo být technicky uzpůsobeno tak, že do sondy předává pouze ta data, která jsou pro monitoring kybernetického prostoru nezbytná. Pokud bude provozovatel sítě předávat do sondy jen řídicí data paketů, jak jsou definována v zákoně o Vojenském zpravodajství, zamezí se tím, aby mělo Vojenské zpravodajství přímý přístup k obsahu komunikace mezi uživateli sítě. Tato data pak nebudou moci být zneužita a přitom Vojenské zpravodajství od provozovatelů sítí dostane data potřebná k monitoringu kybernetického prostoru.</p> <p>Dále v původním návrhu chybí určení, kde je stanovena specifikace toho, jaké rozhraní mají poskytovatelé sítí zajistit. Z toho důvodu navrhuje do návrhu zákona doplnit, že rozhraní pro připojení sondy a technické požadavky na provozovatele sítí stanoví prováděcí právní předpis. Odpovídajícím způsobem by měl být návrh vyhlášky doplněn. V souvislosti s nedávným varováním Národního úřadu pro kybernetickou a informační bezpečnost, doporučujeme v návrhu vyhlášky zohlednit bezpečnostní požadavky na sondy samotné.</p>	<p>umožňující za účelem zajišťování obrany a bezpečnosti České republiky v kybernetickém prostoru nepřetržité monitorování kybernetického prostoru podle zákona o Vojenském zpravodajství⁷¹⁾ (dále jen „sonda“).</p>	<p>jí provozované sítě rozhraní pro připojení zařízení umožňujícího za účelem zajišťování obrany a bezpečnosti České republiky v kybernetickém prostoru nepřetržité monitorování kybernetického prostoru podle zákona o Vojenském zpravodajství⁷¹⁾ (dále jen „sonda“). Zřízené rozhraní pro připojení sondy musí být technicky uzpůsobeno tak, že do sondy předává pouze metadata zpráv, definovaná v § 16b odst. 3 zákona o Vojenském zpravodajství, a zároveň neumožňuje sondě komunikovat v opačném směru. Bližší technické požadavky na připojení sondy k rozhraní stanoví prováděcí právní předpis.</p>
<p>§ 98a odst. 3)</p> <p>V návrhu vyhlášky se píše, že se "do výše nákladů se zahrnují pouze ty náklady, které byly zachyceny v účetnictví subjektem". V praxi se však může ukázat jako problematické určit přesný počet odpracovaných hodin zaměstnance subjektu, které strávil při řešení závad v síti, u kterých se například až zpětně zjistí, že vznikly v důsledku připojení zpravodajské sondy. Navíc není úplně jasné, proč je povinnost navázaná na účetnictví, když tento typ nákladů nebude zpravidla účtován jako samostatná položka. Z toho důvodu navrhuje upravit navrhované znění zákona tak, že provozovateli sítí náleží náhrada jakýchkoliv efektivně vynaložených nákladů bez ohledu na to zda jsou zaznamenány v účetnictví nebo jiným prokazatelným způsobem.</p>	<p>(3) 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 a způsob jejich úhrady stanoví prováděcí právní předpis.</p>	<p>(3) Za plnění povinností podle odstavce 1 náleží právnické nebo podnikající fyzické osobě od Vojenského zpravodajství úhrada efektivně vynaložených nákladů zaznamenaných v účetnictví nebo jinak. Způsob určení výše efektivně vynaložených nákladů a způsob jejich úhrady stanoví prováděcí právní předpis.</p>
<p>§ 98a odst. 4)</p>	<p>(4) Osoba uvedená v odstavci 1, jakož i jiné osoby podílející se na plnění povinnosti podle odstavce 1,</p>	<p>(4) Osoba uvedená v odstavci 1, jakož i jiné osoby podílející se na plnění povinnosti podle odstavce</p>

<p>Navrhujeme doplnit navrhovaný odstavec 4 o výjimku z povinnosti mlčenlivosti pro provozovatele sítí na komunikaci se členy kontrolních orgánů, které jsou nezávislé na výkonné moci. Jednalo by se o kontrolní orgán Poslanecké sněmovny (dle § 21 zákona č. 289/2005 Sb., o Vojenském zpravodajství) a dále Orgán nezávislé kontroly zpravodajských služeb České republiky (dle § 12e zákona č. 153/1994 Sb., o zpravodajských službách České republiky). Navrhované ustanovení je nezbytné pro řádný výkon činnosti kontrolních orgánů. V situaci, kdyby bylo monitoringu zneužito a provozovatel sítě by nebyl zproštěn mlčenlivosti vůči kontrolním orgánům, zbývala by provozovateli sítě pouze ochrana prostřednictvím správního soudnictví.</p>	<p>jsou povinny zachovávat mlčenlivost o všech skutečnostech souvisejících s připojením a užíváním sond. Tato povinnost trvá i poté, kdy tato osoba přestane být osobou podle odstavce 1 nebo osobou podílející se na plnění povinnosti podle věty první.</p>	<p>1, jsou povinny zachovávat mlčenlivost o všech skutečnostech souvisejících s připojením a užíváním sond. Tato povinnost trvá i poté, kdy tato osoba přestane být osobou podle odstavce 1 nebo osobou podílející se na plnění povinnosti podle věty první. Povinnost mlčenlivosti se nevztahuje na komunikaci s kontrolním orgánem Poslanecké sněmovny dle § 21 zákona o Vojenském zpravodajství a Orgánem nezávislé kontroly zpravodajských služeb České republiky dle § 12e zákona o zpravodajských službách České republiky.</p>
<p>Přestupky</p>		
<p>§ 118 odst. 23)</p> <p>Navrhujeme určit výjimku z přestupku neoprávněného zásahu do sondy nebo omezení její funkčnosti ze strany provozovatele sítě za situace, kdy osoba odpojí sondu za stavu kybernetického útoku na svou vlastní telekomunikační infrastrukturu z důvodu umístění sondy.</p>	<p>(23) Právnická nebo podnikající fyzická osoba se jako osoba zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací dopustí přestupku tím, že</p> <p>a) v rozporu s § 98a odst. 1 nezřídí nebo nezabezpečí v určených bodech své sítě rozhraní pro připojení sondy podle rozhodnutí vydaného Ministerstvem obrany,</p> <p>b) neumožní Vojenskému zpravodajství přístup k sondě,</p> <p>c) neoprávněně zasáhne do sondy nebo omezí její funkčnost, nebo</p> <p>d) poruší povinnost zachovávat mlčenlivost podle § 98a odst. 4.</p>	<p>(23) Právnická nebo podnikající fyzická osoba se jako osoba zajišťující síť elektronických komunikací nebo poskytující službu elektronických komunikací dopustí přestupku tím, že</p> <p>a) v rozporu s § 98a odst. 1 nezřídí nebo nezabezpečí v určených bodech své sítě rozhraní pro připojení sondy podle rozhodnutí vydaného Ministerstvem obrany;</p> <p>b) neumožní Vojenskému zpravodajství přístup k sondě;</p> <p>c) neoprávněně zasáhne do sondy nebo omezí její funkčnost,</p>

		<p>s výjimkou situace, kdy osoba odpojí sondu za stavu kybernetického útoku na svou vlastní telekomunikační infrastrukturu z důvodu umístění sondy v jí provozované síti; nebo d) poruší povinnost zachovávat mlčenlivost podle § 98a odst. 4.</p>
<p>§ 118 odst. 24)</p> <p>Navržená podoba sankcí za uvedené přestupky je nepřiměřená. Navrhovaná výše pokuty 50 000 000 Kč se svou výší rovná například výši pokuty stanovené pro provozovatele jaderné elektrárny za porušení povinností týkajících se provozu jaderného reaktoru (§ 178 odst. 5 písm. b) atomového zákona). Z tohoto důvodu navrhuje zmírnění sankcí podle míry závažnosti jednání.</p> <p>Sankci za přestupky, kdy provozovatel sítě nezřídí a nezabezpečí připojení sondy podle rozhodnutí Ministerstva obrany (dle § 98a odst. 1), neumožní Vojenskému zpravodajství přístup k sondě, nebo neoprávněně zasáhne do sondy nebo omezí její funkčnost, navrhuje ve výši 15 000 000 Kč, protože již tato výše je dostatečně odrazující sankcí.</p> <p>Sankce za přestupek, kdy provozovatel sítě poruší povinnost zachovávat mlčenlivost (podle § 98a odst. 4.), je dostatečně odstrašující již ve výši 5 000 000 Kč. K podobné výši sankce lze dospět i srovnáním se zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, dle kterého je podnikatelům možné uložit sankci za přestupky, při kterých vyradí informace v různém stupni utajení v maximální výši 5 000 000 Kč. Přitom tato nejvyšší možná sankce je za dva přestupky: 1) když podnikatel poskytne utajovanou informaci stupně utajení Přísně tajné, Tajné nebo Důvěrné zahraničnímu partneru, anebo 2) když vyveze z území České republiky certifikovaný kryptografický prostředek bez povolení Národního bezpečnostního úřadu.</p>	<p>23 (24) Za přestupek podle § 118 lze uložit pokutu do</p> <p>a) 5 000 000 Kč, jde-li o přestupek podle odstavce 1 písm. n) až r), odstavce 2 písm. f), odstavce 3 písm. b), odstavce 5, odstavce 6 písm. g) nebo odstavce 14 písm. ae),</p> <p>b) 15 000 000 Kč nebo do výše 5 % z čistého obratu pachatele přestupku dosaženého za poslední ukončené účetní období, podle toho, která z těchto hodnot je vyšší, jde-li o přestupek podle odstavce 1 písm. m), odstavce 2 písm. c) až e), odstavce 3 písm. a), odstavce 8 písm. d) až m), odstavce 10 písm. j) až r), odstavce 12 písm. f) až p), odstavce 13 písm. i) až n), odstavce 14 písm. k) až ad) nebo odstavce 15,</p> <p>c) 50 000 000 Kč nebo do výše 10 % z čistého obratu pachatele přestupku dosaženého za poslední ukončené účetní období, podle toho, která z těchto hodnot je vyšší, jde-li o přestupek podle odstavce 1 písm. a) až l), odstavce 2 písm. a), b), odstavce 4, odstavce 6 písm. a) až f), odstavce 7, odstavce 8 písm. a) až c), odstavce 9, odstavce 10 písm. a) až i), odstavce 11, odstavce 12 písm. a) až e), odstavce 13 písm. a) až</p>	<p>(24) Za přestupek podle § 118 lze uložit pokutu do</p> <p>a) 5 000 000 Kč, jde-li o přestupek podle odstavce 1 písm. n) až r), odstavce 2 písm. f), odstavce 3 písm. b), odstavce 5, odstavce 6 písm. g), odstavce 14 písm. ae), nebo odstavce 23 písm. d),</p> <p>b) 15 000 000 Kč nebo do výše 5 % z čistého obratu pachatele přestupku dosaženého za poslední ukončené účetní období, podle toho, která z těchto hodnot je vyšší, jde-li o přestupek podle odstavce 1 písm. m), odstavce 2 písm. c) až e), odstavce 3 písm. a), odstavce 8 písm. d) až m), odstavce 10 písm. j) až r), odstavce 12 písm. f) až p), odstavce 13 písm. i) až n), odstavce 14 písm. k) až ad), odstavce 15, odstavce 23 písm. a) až c),</p> <p>c) 50 000 000 Kč nebo do výše 10 % z čistého obratu pachatele přestupku dosaženého za poslední ukončené účetní období, podle toho, která z těchto hodnot je vyšší, jde-li o přestupek podle odstavce 1 písm. a) až l), odstavce 2 písm. a), b), odstavce 4, odstavce 6 písm. a)</p>

	h), odstavce 14 písm. a) až j), odstavce 16, 17, 18, 19, 20, 21 nebo 22 , 22 nebo 23.	až f), odstavce 7, odstavce 8 písm. a) až c), odstavce 9, odstavce 10 písm. a) až i), odstavce 11, odstavce 12 písm. a) až e), odstavce 13 písm. a) až h), odstavce 14 písm. a) až j), odstavce 16, 17, 18, 19, 20, 21 nebo 22.
--	---	--