



Stanovisko Svazu průmyslu a dopravy České republiky k návrhu zákona, kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství (dále jen „návrh zákona“)

Kontext:

Ministerstvo obrany dne 17.6.2019 představilo od roku 2012 již třetí přepracovaný návrh novely zákona č. 289/2005 Sb., o Vojenském zpravodajství (č.j. OVA 15/20). Tento konkrétní návrh má představovat realizaci úkolů z usnesení vlády ČR z 25.5.2016 č. 382, kterým byl schválen Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020, konkrétně bodu C 9.01 Akčního plánu. Ministerstvo obrany se rozhodlo nevyslyšet zásadní připomínky civilního sektoru a nabídky možných alternativ k realizaci zamýšlených nástrojů. Po delších průtazích byl návrh zákona náhle zařazen na jednání Vlády ČR, a to překvapivě 16.3.2020, v době vyhlášeného nouzového stavu kvůli pandemii nemoci COVID-19. Vláda předlohu schválila, a to i přes výzvu Svazu průmyslu ČR a navzdory dopisu předsedovi vlády Andreji Babišovi, vyzývající v této době kontroverzní návrh neprojednat.

Stanovisko Svazu průmyslu a dopravy České republiky (dále jen SP ČR):

SP ČR považuje za důležité bránit bezpečnost České republiky i v oblasti kyberprostoru, který se, vzhledem k rostoucímu využití digitálních technologií, stává stále významnějším. Bezpečnosti klíčových infrastrukturních prvků a systémů České republiky je nutné věnovat adekvátní pozornost, aby bylo možné včas zasáhnout proti kybernetickým nebo teroristickým útokům. Zajišťování bezpečnosti ČR však musí probíhat v co nejvíce možném souladu se zabezpečením dat a soukromí občanů ČR.

Nerozporujeme význam kybernetické obrany ČR. Nejsme však přesvědčeni, že došlo k adekvátnímu vypořádání připomínek, které byly k návrhům zákona uplatňovány ze strany našich členských firem, a to ani na základě semináře, který se uskutečnil dne 13. května 2019, kde byly připomínky soukromého sektoru prezentovány. Jsme proto nuceni konstatovat, že ani aktuální text novely zákona o Vojenském zpravodajství nevypořádává nejzásadnější připomínky, které byly k návrhu zákona uplatněny:

- Návrh zákona stále nereflektuje výhrady ke koncepčnímu pojetí, které ve stávající podobě představuje plošné a nepřetržité sledování veškeré komunikace na uzlech veřejných komunikačních sítí a u provozovatelů služeb veřejných elektronických komunikací (dále jen jako „provozovatel SEK“), aniž by k tomu byl předem dán souhlas soudem nebo státním zástupcem. Návrh zákona dle našeho názoru celou věc zjednodušuje přejmenováním dříve v textu používaného termínu „sonda“ na „nástroj detekce“ a pro sbíraná data o provozu pak používá neurčitý termín „metadata“. Metadata jsou však v tomto kontextu data popisující, kdo s kým a kdy komunikoval, což bez pochyby představuje informace, které narušují oprávněné soukromí všech uživatelů veřejných komunikačních sítí a veřejných služeb elektronických komunikací. V důsledku to tedy znamená narušení

oprávněného soukromí uživatelů služeb informační společnosti. Vojenské zpravodajství by tato metadata sbíralo v režimu 24/7, bez potřeby souhlasu soudu nebo státního zástupce a uchovávalo po prakticky neomezenou dobu.

V uvedeném považujeme návrh zákona za zcela nekonceptní, v rozporu s existující právní úpravou v oblasti trestní a v této části by měl být zákon vrácen k přepracování, neboť navrhované řešení negarantuje, že nemůže docházet k nekontrolovatelnému sběru přenášených dat na sítích Vojenským zpravodajstvím.

- Návrh zákona popírá dosavadní zákonné postupy např. policejních orgánů dle zákona č. 141/1961 Sb., o trestním řízení soudním (dále jen „trestní řád“), ve znění pozdějších předpisů, a dalších příslušných právních předpisů, kdy takový policejní orgán má k metadatům či provozně lokalizačním údajům přístup pouze na základě zákonné a odůvodněné písemné žádosti, a v případech, kdy je zasahováno do základních lidských práv a svobod, lze takový zásah ve smyslu § 158d odst. 3 trestního řádu uskutečnit pouze s předchozím povolením soudce. Novela zákona o Vojenském zpravodajství tak opravňuje Vojenské zpravodajství k tomu, aby si údaje prostřednictvím nástroje detekce opatřilo bez jakýchkoli překážek, neomezeně, kdykoli, a bez předchozího povolení soudu sledovalo průběh komunikace ve veřejných sítích elektronických komunikací.

V uvedeném považujeme návrh zákona za zcela nekonceptní, v rozporu s existující právní úpravou v oblasti trestní a v této části by měl být zákon vrácen k přepracování, neboť navrhované řešení negarantuje, že nemůže docházet k nekontrolovatelnému sběru přenášených dat na sítích Vojenským zpravodajstvím.

- § 16f odst. 6 v navrhovaném znění stanovuje, že Vojenské zpravodajství poskytne v souvislosti s jím prováděnými činnostmi součinnost vůči NÚKIB a Policii České republiky, pokud o to v individuálních případech pro účely zajišťované bezpečnosti v kybernetickém prostoru požádají. Toto ustanovení povinnosti na poskytnutí součinnosti nemá žádné upřesnění co do rozsahu, ve kterém by mělo být vůči Policii ČR nebo NÚKIBu vykonáváno, což zejména ve vztahu k již dnes projednávané novele zákona č. 273/2008 Sb., o Policii České republiky a některých dalších zákonů (sněmovní tisk 642), přináší velké otázky, když tato projednávaná novela zavádí možnost užití informace zpravodajských složek v trestních řízeních.

V uvedeném považujeme návrh zákona za zcela nekonceptní, v rozporu s existující právní úpravou v oblasti trestní a v této části by měl být zákon vrácen k přepracování nebo by měla být odpovídajícím způsobem upravena novela zákona o Policii ČR (sněmovní tisk 642), v části první, novelizující § 39 „Rušení provozu elektronických komunikací“ zákona o Policii ČR a v části druhé, novelizující § 89 odst. 3 a 4 trestního řádu.

- Návrh zákona je vnitřně rozporným v textu nového § 98a a textu stávajícího § 98 zákona č. 127/2005 Sb., o elektronických komunikacích, a to z důvodu, že jakékoliv cizí a neznámé zařízení v podobě nástroje detekce je při umístění k provozovateli SEK z principu kybernetickou hrozbou. **Požadujeme, aby provozovatelé sítí měli možnost volby vlastního řešení, kterým by metadata předávali na základě zákona Vojenskému zpravodajství.**
- Návrh zákona explicitně nevylučuje, že nástroj detekce umístěný k provozovateli SEK nemůže být využit k aktivnímu zásahu Vojenským zpravodajstvím podle § 16e návrhu zákona. Takový aktivní zásah přitom představuje naprosto bezprecedentní využívání privátní civilní infrastruktury k vojenským účelům, namísto toho, aby návrh zákona výslovně stanovil, že k aktivnímu útoku může být využita výhradně infrastruktura státu, tedy Vojenského zpravodajství nebo jiných zpravodajských složek nebo složek Armády ČR.

Požadujeme, aby byl aktivní zásah u nástrojů detekce explicitně vyloučen.

- Zavedení institutu inspektora pro kybernetickou obranu v § 16j návrhu zákona, které by mělo představovat vyšší úroveň kontroly činnosti Vojenského zpravodajství v oblasti kybernetické obrany, považujeme za zcela nešťastné. Dle návrhu zákona je tento Inspektor pro kybernetickou obranu zároveň příslušníkem Vojenského zpravodajství. Takové nastavení negarantuje dostatečnou neustrannost. Inspektor pro kybernetickou obranu rovněž nemá v zákoně uvedenou žádnou možnost ověřit skutkové okolnosti uvedené v podnětu fyzické nebo právnické osoby a jednak budou fyzické a právnické osoby obracející se na Inspektora vždy ve značné důkazní nouzi, neboť o chování umístěných „detekčních zařízení“ nebudou mít žádné informace, aby se mohli svých práv řádně domáhat.

Požadujeme, aby dohledem na činnosti Vojenského zpravodajství v oblasti kybernetické obrany byl určen skutečně nezávislý orgán, kterým by mohl být např. Úřad na ochranu osobních údajů nebo k tomu účelu zřízená parlamentní komise.

- Návrh znění § 16m odst. 4 návrhu zákona dává rozhodovací pravomoc v otázce přiznání náhrady škody nebo nemajetkové újmy v souvislosti s činností Vojenského zpravodajství výlučně do rukou Ministerstva obrany, kterému je Vojenské zpravodajství podřízeno – nikoliv do rukou nezávislého soudu, který by o její oprávněnosti a výši nestranně rozhodoval.

Požadujeme, aby o rozhodnutích týkajících se náhrad škod a nemajetkové újmy v souvislosti s činností Vojenského zpravodajství rozhodovaly obecné soudy, byť v adekvátním režimu utajení.

- V návrhu zákona v novém § 98a odst. 2 zákona č. 127/2005, o elektronických komunikacích, se uvádí, že rozhraní pro připojení nástroje detekce nesmí umožnit předávat obsah detekovaných jevů provozu v SEK v opačném směru. Ani při čtení důvodové zprávy k této části návrhu zákona není zřejmé, co je zamýšleno touto formulací.

Stávající návrh zákona považuje SP ČR za velmi problematický a vyzývá Vojenské zpravodajství a Ministerstvo obrany, aby s privátním sektorem a odbornou veřejností zahájili skutečnou a seriózní diskusi o potřebách při kybernetické ochraně státu, ve které dnes naprosto zásadní a neoddiskutovatelnou roli hrají právě především zástupci privátního sektoru v České republice. Jsme přesvědčeni, že pokud by k tomu dalo Ministerstvo obrany a Vojenské zpravodajství prostor, tak privátní sektor je schopen v horizontu několika týdnů, resp. měsíců, navrhnout funkční model splňující potřeby státu v oblasti kybernetické ochrany při zachování zabezpečení dat a soukromí občanů ČR. Jsme přesvědčeni, že jen skutečná spolupráce veřejného a soukromého sektoru v oblasti kybernetické ochrany státu může přinést kvalitativní posun v oblasti kybernetické bezpečnosti a obrany České republiky. Zároveň jsme přesvědčeni, že je nutné najít širokou politickou a odbornou shodu na zásadách ochrany soukromí a svobody jednotlivce v oblasti kybernetické bezpečnosti a obrany. Pro tyto účely je potřeba využít všech dostupných kontrolních a na vlastním výkonu kybernetické bezpečnosti a obrany nezávislých mechanismů mezi něž nepochybně patří i rozdělení jednotlivých rolí a kompetencí mezi více subjektů, které budou v dané oblasti působit.