21. 5. 2020

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Kybernetický útok „za odstranění sochy“ – aneb „utajovaná“ role zpravodajské služby

V roce 2007 došlo k paralyzujícímu útoku na počítačovou infrastrukturu Estonska, přičemž následně byl tento útok Estonskem označen jako „pomsta“ jedné ze světových velmocí za přenesení válečného památníku této velmoci (bronzové sochy zobrazující vojáka) pryč z centra hlavního města Tallinnu na válečný hřbitov. Předmětný útok byl tak masivní, že vyřadil z provozu na několik týdnů vládní webové stránky, weby politických stran, médií nebo estonských bank. V roce 2013 došlo v České republice k rozsáhlému několikadennímu DDoS útoku zacíleného na české zpravodajské servery, vyhledávač Seznam.cz, české banky a weby českých mobilních operátorů, přičemž stopy útočníků vedly opět do jedné z velmocí světa.

Pro úvodní zajímavost autorka textu dále zmíní, že v současné době se za velkého mediálního zájmu v České republice vede diskuze laické i odborné veřejnosti jak k odstranění bronzové sochy maršála armády jedné ze světových velmocí, tak i k připravované novele zákona o Vojenském zpravodajství (zák. č. 289/2005 Sb.), kterou dne 16.3.2020 vláda schválila a předložila ji k dalšímu opatření parlamentu. Diskuze týkající se připravované novely probíhají převážně na téma ochrana soukromí jednotlivce, přiměřenosti použití hromadných sledovacích prostředků, důrazně je vyzdvihováno, že připravovaná novela generuje vysoká bezpečnostní rizika v případě selhání konkrétního jednotlivce a současně je vládě vytýkáno, že novelu předmětného zákona schválila a předložila ji parlamentu v době nouzového stavu. Oponenty novely je dále kritizována vágnost některých novelizovaných zákonných pasáží a nespecifičnost postupu ze strany Vojenského zpravodajství při případném „aktivním zásahu“ vůči kybernetickému útoku.

Autorka textu konstatuje, že nekonkrétnost některých zákonných pasáží obsahuje i velké množství jiných právních předpisů a z logiky věci tak v některých případech i odůvodněně být musí, neboť se jedná o specifické zákonné normy, které se zabývají např. ochrannou utajovaných informací nebo činností bezpečnostních sborů či zpravodajských služeb. Co se týká zpravodajských služeb, tak celková činnost jakékoli zpravodajské služby z důvodu naplnění účelu jejího zřízení a adekvátního plnění přidělených úkolů není a nesmí být pro širokou veřejnost konkrétní a plnohodnotně transparentní. Na rozdíl např. od Policie České republiky, kdy policejní činnost od určité fáze a do určité míry transparentní a konkrétní naopak být musí – např. vedení správního, přestupkového nebo trestního řízení. Z logiky věci nelze proto požadovat, aby zpravodajská služba přesně specifikovala své „know-how“ a to ať již se týká jakékoli oblasti její činnosti. Zákon o utajovaných informacích a o bezpečnostní způsobilosti (zák. č. 412/2005 Sb.) v části první a části druhé vymezuje základní pojmy a definice týkající se utajované problematiky, přičemž konkretizace zákonného znění zájmu České republiky a definice újmy či nevýhody pro tento zájem je vydefinována tak, jak je a nikdo z řad laické veřejnosti dle názoru autorky textu nebude schopen původci utajované informace vyvrátit jeho argumentaci ohledně vzniku utajované informace a to právě díky nekonkrétnosti zákonných definic, která je ovšem do určité míry ve zpravodajské oblasti pro praxi přínosná a žádoucí.

V daném případě novely zákona o Vojenském zpravodajství je si dle názoru autorky textu nutno uvědomit, že celý kyberprostor (včetně jeho ochrany a obrany) je postaven na informačním toku. Informace velmi rychle stárnou a jejich relevance se mění možná s každou uběhlou minutou. Ve státu rozsáhlou a různorodou kapacitou informací důležitých pro zájem České republiky primárně a

převážně disponují právě zpravodajské služby. Vojenské zpravodajství má v sobě zahrnuto jak toto zpravodajské informační „know-how“ (na rozdíl od ostatních zpravodajských služeb zahrnující vlastní rozvědnou i kontrarozvědnou činnost), tak i specifikaci vojenskou, kdy jeho příslušníci složili vojenskou přísahu, ve které kromě jiného i přísahali, že budou věrni České republice a pro obranu vlasti jsou připraveni nasadit i svůj život. A v tomto spatřuje autorka textu jeden ze zásadních rozdílů mezi příslušníky Vojenského zpravodajství a v oblasti kybernetické působícími civilními zaměstnanci např. Národního úřadu pro kybernetickou a informační bezpečnost nebo pracovníky týmu CERT nebo CSIRT.

Příslušníci Vojenského zpravodajství jsou úplně stejně vojáky z povolání (dle zákona č. 221/1999 Sb., o vojácích z povolání) – a to jak s totožnou přísahou, tak i se základními totožnými povinnostmi – jako příslušníci Armády České republiky, resp. příslušníci ozbrojených sil České republiky. Mimořádně vážné kybernetické útoky na zájem suverénního státu jsou často vedeny nikoli „samostatnými civilními“ osobami, ale osobami podporovanými či přímo patřícími do nějaké státní soustavy „útočníka“. Útočníka, který disponuje informacemi takového rozsahu a charakteru, že je může využít a někdy využije pro závažný útok na svého „protivníka“, přičemž i útok v kyberprostoru může splňovat kritéria válečného aktu. Proti takovému způsobu a rozsahu je možno se účinně bránit pouze tím, že napadený bude mít minimálně stejné či ještě rozsáhlejší informace než jeho protivník. Jak již autorka textu uvedla, informace stárnou s každou uplynulou minutou, proto je důležité mít zásadní informace co nejvíce „čerstvé“ a moci a umět je v konkrétně probíhajícím čase a prostoru průběžně získávat, aktualizovat a využívat je. Proto z pohledu autorky textu se zdá naprosto přiléhavé, že primární pravomoc ke kybernetické obraně byla přiřazena přímo Vojenskému zpravodajství. V prostředí virtuálního prostoru, kdy je nutné reagovat okamžitě a pro své rozhodnutí získávat a vyhodnocovat průběžně aktuální informace, není přiléhavě žádoucí jakékoli informační předávání mezi různými státními subjekty v situaci vyžadující okamžitou reakci, neboť každá – i minimální prodleva – může v důsledku zmařit účinnou kybernetickou „odpověď“. Z těchto důvodů proto není dle názoru autorky na místě návrh tzv. MODELU 4 sil, který v rámci odborných připomínek navrhuje odborná organizace CZ.NIC ohledně přímého zapojení vojáků Armády České republiky jako vykonavatelů kybernetické obrany.

NATO i Evropská unie na kybernetickou ochranu a obranu kladou velký důraz a v dnešní moderní době, kdy kromě jiného existuje (před lety ještě nepředstavitelně) „internet věcí“, kdy dobrovolně využíváme různá kyberzařízení, a to i v rámci předmětů denní potřeby (telefony, osvětlení, topení, televize, kamery apod.), tak je dle názoru autorky textu částečně irelevantní argumentovat ve vztahu k připravované novele s primární důrazností na ochranu soukromí jednotlivce ve virtuálním prostředí. Dle osobního názoru autorky textu jednotlivec svoje naprosté a jednoznačné soukromí v záplavě nejrůznějších moderních technologií už dávno ztratil. Možná není od věci monitoring kyberprostoru „laicky“ přirovnat k monitorování nejrůznějšího veřejného prostoru kamerami či jinými obdobnými záznamovými zařízeními – instalované zařízení zaznamenává a archivuje konkrétní data všech osob, které se rozhodnou do daného veřejného prostoru vejít a pohybovat se v něm. A pokud někdo z takto plošně monitorovaných osob spáchá např. trestný čin či jiný protiprávní delikt, tak se zaznamenaná data mohou použít a v praxi používají k jeho odhalení či usvědčení. Tedy konkrétní plošně získaná data se v případě odůvodněné potřeby vyspecifikují a následně se využijí k ochraně zájmu České republiky. Autorka textu s touto relevancí má jako přísedící u soudu konkrétní zkušenosti a dovolí si tvrdit, že někdy jsou takto získaná data velmi přínosná pro finální rozhodnutí soudu. Kyberprostor je možno analogicky přirovnat k takovému fyzickému veřejnému prostoru, a pokud se osoba rozhodne využívat jej a pohybovat se v něm, musí počítat s tím, že její činnost v takovém prostoru může být z důvodu vyššího zájmu společnosti zahrnuta do plošného monitoringu.

Co se týká argumentace možného zneužití při využívání novelizovaného oprávnění uvedeného

v rámci předmětného zákona o Vojenském zpravodajství, tak je možno konstatovat, že každá přítomnost „lidského faktoru“ nese i riziko zneužití, a to kdekoli. Zneužití svých pravomocí a povinností páchají jak příslušníci různých bezpečnostních sborů, tak i zaměstnanci různých státních institucí, státní zástupce a soudce nevyjímaje. Nicméně dle názoru autorky textu není od věci, aby odpůrci předkládané novely vzali na mysl jednu důležitou skutečnost – na rozdíl od ostatních občanů státu (např. i od vládních představitelů nebo představitelů parlamentu) příslušníci zpravodajských služeb kromě jiného podléhají velmi důkladnému bezpečnostnímu prověření pro nejvyšší stupeň utajení, který zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti umožňuje. A jistě pro laickou veřejnost není bez zajímavosti, že takovýmto hloubkovým několikaměsíčním bezpečnostním řízením nemusí procházet žádný člen vlády, parlamentu ba dokonce ani soudce. Např. soudci, jež povolují různé konkrétní odposlechy či sledování a dostanou se tak často k velmi citlivým soukromým informacím, nemusí projít žádnou bezpečnostní prověrkou a autorce textu je známo, že takové zjištění někdy bývá pro laickou veřejnost zarážející. Přičemž bezpečnostním řízením s prověřením pro nejvyšší stupně utajení neprochází ani velká většina vojáků Armády České republiky či příslušníků Policie České republiky. A ano, samozřejmě – „lidský faktor“ i u takto velmi prověřené osoby může selhat a minulost dokládá, že v ojedinělých případech i selhává – nicméně zde mějme na paměti, že pokud k takovému selhání dojde, může k němu dojít u kohokoli, ať již se jedná o člena vlády, parlamentu, zpravodajce, vojáka, policistu, soudce nebo zaměstnance Národního bezpečnostního úřadu, Národního úřadu pro kybernetickou a informační bezpečnost či jiného úřadu. K selhávání jednotlivců dochází, to je prostě skutečnost, která se nedá ze společnosti nikdy zcela eliminovat. U zpravodajců obecně ovšem existuje dle názoru autorky textu „důležitá záruka“, vyplývající ze zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti, neboť kdokoli se stane v souladu s tímto zákonem držitelem osvědčení, tak ukončením bezpečnostního řízení a vydáním osvědčení „prověřování“ takovéto osoby nekončí. Držitel osvědčení musí splňovat podmínky nutné pro jeho vydání po celou dobu jeho platnosti, kdy toto je samozřejmě průběžně ověřováno a držitel osvědčení, jež ho opravňuje k přístupu k utajovaným informacím, je nadále podrobován neustálému průběžnému prověřování, jež je adekvátní výši stupně utajení jím drženého osvědčení. Tedy čím vyšší stupeň utajení, tím složitější a hlubší bezpečnostní prověřování.

Dle názoru autorky textu tedy pokud znění novely zákona o Vojenském zpravodajství není v některých pasážích konkrétní, tak je to pravděpodobně z toho důvodu, že by mohlo dojít „ke konfliktu“ se zákonem na ochranu utajovaných informací a potažmo k následnému možnému ohrožení činnosti zpravodajské služby a zájmu České republiky. Činnost zpravodajských služeb souznící taktéž se zákonem na ochranu utajovaných informací nemusí být, a někdy dokonce i nesmí být, pro veřejnost tak transparentní, jak by oproti tomu naopak měla být činnost orgánů činných v trestním řízení, jež utajované informace taktéž zpracovávají. Orgány činné v trestním řízení mohou velmi různorodé účastníky trestního procesu ohledně utajovaných informací ad hoc poučovat a tím jim de facto utajované informace zákonně „vyzrazovat“, přičemž s částí utajovaných informací po jejich řádném odtajnění mohou veřejně např. v rámci soudního projednání případu nakládat a tím takové informace sdělovat veřejnosti. Zpravodajské služby oproti tomu z podstaty své působnosti a činnosti „svoje“ utajované informace nikdy neodtajňují. Zpravodajské služby jsou taktéž z rámce státních institucí jediné, jež mají v nařízení vlády č. 522/2005 Sb. – přílohou č. 18 – stanoveno v největším počtu pořadových čísel přílohy pro svoji působnost rozsah stupňů utajení až po nejvyšší stupeň PŘÍSNĚ TAJNÉ (PT), kdy pod tento nejvyšší rozsah samozřejmě spadají i formy a metody zpravodajské činnosti a prostředky při nich používané. A je proto reálné, že s nějakou takovou „utajovanou“ metodou zpravodajské činnosti a s konkrétními prostředky při ní v praxi používanými, pravděpodobně „zákulisně“ počítá i připravovaná novela zákona o Vojenském zpravodajství, ale s ohledem na stupeň utajení nemůže předkladatel zákonné novely tyto informace blíže specifikovat a konkretizovat.

Závěrem textu autorka na základě výše argumentovaného vznáší dotaz – kdy jindy tuto potřebnou

novelu zákona o Vojenském zpravodajství schválit, když ne teď? Kdy jindy, když ne v době, kdy kybernetické útoky začínají čím dál více sílit a zasahovat i do takových sfér jako jsou nemocnice nebo letiště?

Mgr. Zdeňka Kovaříková, DiS.

Další články:

- Nový zákon o veřejných dražbách, aukce a obálkové metody
- Pohled přes hranice – natáčení pornografických klipů jako důvod výpovědi z nájmu bytu
- Nařízení EU o umělé inteligenci a jeho dopady na využití jazykových modelů v advokátní praxi
- Revize zájezdové směrnice: co přináší, co hrozilo a co to znamená pro praxi
- Kupní smlouva o převodu nemovitosti bez uvedení výše kupní ceny
- Druhá „tlačítková novela": povinné tlačítko pro odstoupení od smlouvy
- Souhlas s veřejným užíváním pozemku jako překážka nároku na bezdůvodné obohacení – nález Ústavního soudu sp. zn. I. ÚS 2541/25
- Kupní smlouva bez přesného určení kupní ceny
- Byznys a paragrafy, díl 36.: Doložka o mlčenlivosti
- Detekce podezřelého obchodu v kontextu hazardních her
- AI omnibus