1. vydanie

Miroslav Chlipala
Ivan Makatura
Štefan Pilár

Zákon o kybernetickej bezpečnosti
Komentár

prvé vydanie, Bratislava: EUROKÓDEX, s. r. o., máj 2019. 408 s.

ISBN 978-80-8155-086-7

www.eurokodex.sk

Predslov

V dnešnej dobe už niet pochýb, že zaručenie bezpečnosti informácií prenášaných sieťami a spracúvaných informačnými systémami je absolútne nevyhnutné pre trvalo udržateľný hospodársky rast spoločnosti. Vzhľadom na neustále sa rozvíjajúce hrozby v oblasti kybernetickej bezpečnosti je ošetrenie rizík spojených s kybernetickou bezpečnosťou jednou z hlavných výziev pre zabezpečenie jednotného digitálneho trhu Európskej únie.

Smernica Európskeho parlamentu a Rady 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (ďalej len „Smernica NIS") je prvým právnym aktom Európskej únie, ktorý sa dotýka odborných disciplín zaoberajúcich sa problematikou zaručenia bezpečnosti informácií. Cieľom Smernice NIS je dosiahnuť vysoký spoločný štandard bezpečnosti sietí a informačných systémov vo všetkých členských štátoch EÚ. Keďže Slovenská republika do doby jej prijatia nemala samostatný právny predpis, ktorý by implementoval požiadavky bezpečnosti informácií (najmä informácií spracúvaných v kybernetickom priestore), pre slovenskú legislatívu bolo prijatie Smernice NIS podnetom a zároveň záväzkom pre prijatie národného zákona, ktorým by táto oblasť bola pokrytá. Transpozičným zákonom Smernice NIS je práve zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v platnom znení (ďalej len „Zákon").

Ako pri každej novej regulácii, aj pri Smernici NIS a Zákone existuje množstvo názorov na spôsob implementácie požiadaviek vyplývajúcich z právnej úpravy. Ak pre tento prípad nebudeme považovať bezpečnosť za hypotetický cieľový stav, ale za cyklický proces, je kybernetická bezpečnosť špecializovanou odbornou disciplínou. Je to najmä systém manažérstva, ktorý je založený na široko akceptovaných teoretických základoch a na dlhodobej dobrej praxi. Tento systém manažérstva sa opiera o paralelnú potrebu znalostí z oblasti práva, riadenia organizácií, riadenia rizík a informatiky. Preto popri právnom výklade ustanovení samotného Zákona má táto publikácia za cieľ aj vysvetlenie špecifík odbornej disciplíny „kybernetická bezpečnosť" v kontexte požiadaviek tejto novej právnej úpravy.

Ambíciou komentára je poskytnúť nezávislý pohľad na výkladové a aplikačné problémy, praktickú stránku požiadaviek Zákona vrátane vysvetlenia všeobecného významu bezpečnostných opatrení a procesných povinností, ktoré vyplývajú povinným osobám v zmysle Zákona, predovšetkým však prevádzkovateľom základných služieb a poskytovateľom digitálnych služieb. Komentár má snahu prijateľným spôsobom vysvetliť ciele ustanovení Zákona, ktoré môžu mnohým subjektom prinášať nové, úplne neznáme či neuchopiteľné povinnosti a pre mnohé organizácie s už zavedeným systémom riadenia bezpečnosti spôsobovať starosti pri zosúladení s ich doterajšími opatreniami. Cieľom komentára nie je kritika legislatívy v podobe súčasného znenia Zákona, no nájde sa v ňom aj niekoľko návrhov na vylepšenie pri jeho budúcich novelizáciách.

Všetci autori tohto komentára sú pracovne vyťažení a časovo veľmi zaneprázdnení profesionáli vo svojej oblasti, preto táto publikácia nevznikala hladko. Nebola tvorená počas hemingwayovských pokojných rán, ale naopak – po častiach, prerušovane, počas nocí, keď bolo možné nájsť si chvíľu na sústredenie. Nakoniec je však nespornou výhodou, že sa do jej obsahu dostali práve rozsiahle a praktické skúsenosti autorov. Publikácia tak nie je iba teóriou, ktorá by nikdy nebola overená v praxi, ale je pohľadom ľudí z reálnej praxe v informačnej bezpečnosti a IT práve.

Touto cestou sa chceme poďakovať našim rodinám za trpezlivosť a priestor, ktorý nám poskytli.

Autori

Autori komentára

JUDr. Ing. Miroslav Chlipala, PhD.
partner a advokát v advokátskej kancelárii Bukovinský & Chlipala

Advokát s 15-ročnou praxou so zameraním na IT právo, právne aspekty kybernetickej bezpečnosti, GDPR a ochranu osobných údajov, právny rámec eIDAS a e-Governmentu, cloudové služby a duševné vlastníctvo. Vybudoval a vedie tím právnikov, ktorý predstavuje na Slovensku jedinečnú kombináciu pre oblasti duševného vlastníctva a IT práva a telekomunikácií. Pod jeho vedením je advokátska kancelária BCH opakovane zaraďovaná medzi odporúčané kancelárie v súťaži Právnická firma roka na Slovensku.

Mimo výkonu advokácie sa venuje teoreticko-odborným aspektom práva informačných technológií a ich dopadom na podnikateľskú sféru. Aktívne sa zúčastňuje odborných konferencií a vedie workshopy a semináre, kde prednáša aktuálne témy z oblasti IT práva s dôrazom na logické prepojenie práva a technológií. Opakovane prednáša na prestížnych podujatiach, ako sú Slovenské dni práva Slovenskej advokátskej komory alebo na najvýznamnejšej slovenskej odbornej konferencii z oblasti IT práva, na ktorej sa podieľa aj ako predseda programového výboru.

Dlhodobo pôsobil ako pedagóg na Právnickej fakulte UK v Bratislave. Je spoluzakladateľom predmetu právo informačných a komunikačných technológií na FIIT STU v Bratislave. Je aktívnym autorom mnohých odborných článkov a niekoľkých publikácií z oblasti IT práva. Absolvoval viacero zahraničných pobytov a stáží (Hague Academy of International Law, University of Oslo, University of Zaragoza, University of Ljubljana, Jagiellonian University in Kraków).

Ing. Ivan Makatura
Executive Consultant, IBM Security Services

Senior konzultant IBM Security Services so zameraním na oblasť informačnej a kybernetickej bezpečnosti, ochranu osobných údajov, manažment rizík. Skúsený bezpečnostný manažér s dlhoročnou praxou riaditeľa odboru bezpečnosti v bankách, v IT odvetví od roku 1993. Pracovne pôsobí aj ako súdny znalec v odvetví Bezpečnosť a ochrana informačných systémov a tiež ako certifikovaný audítor informačnej bezpečnosti. V role člena technickej komisie Úradu pre normalizáciu a metrológiu SR sa spolupodieľa na implementácii noriem ISO do sústavy Slovenských technických noriem. Vyštudoval odbor aplikovaná informatika na Fakulte elektrotechniky a informatiky Technickej univerzity v Košiciach. Neskôr absolvoval postgraduálne štúdium na Znaleckom ústave elektrotechniky a informatiky Slovenskej technickej univerzity v Bratislave. Je držiteľom mnohých profesijných certifikácií v oblasti informačnej bezpečnosti a riadenia rizika. Je známym prednášajúcim na slovenských i medzinárodných konferenciách a vzdelávacích aktivitách, ako aj autorom mnohých článkov s témou informačnej bezpečnosti a ochrany osobných údajov.

JUDr. Štefan Pilár
advokátsky koncipient v advokátskej kancelárii Bukovinský & Chlipala

V súčasnosti pôsobí ako právnik so zameraním na kybernetickú bezpečnosť, ochranu osobných údajov a IT právo. Súčasťou jeho odborného zamerania sú aj školenia a semináre venované implementácii a praktickým skúsenostiam s GDPR či problematike

kybernetickej bezpečnosti. Podieľa sa na implementačných projektoch zavádzajúcich opatrenia pre spracúvanie a ochranu osobných údajov pre významné spoločnosti z oblasti cloud computingu, telekomunikačných služieb alebo finančného sektora.

V minulosti pôsobil na viacerých pozíciách s prepojením práva a IT technológií, a to ako právny poradca CSIRT-u alebo ako spolutvorca zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti. Na medzinárodnej úrovni pôsobil v pozícii národného experta pre oblasť kybernetickej bezpečnosti, a to v rámci pracovných platforiem Európskej komisie (NIS Expert Group, Komitologický výbor NIS, Politika kybernetickej bezpečnosti – Galileo).

V pozícii národného právneho poradcu zastupoval Slovenskú republiku na medzinárodných cvičeniach kybernetickej obrany (Locked Shields, Cyber Coalition). V rámci svojho odborného zamerania absolvoval stáž v Centre výnimočnosti NATO pre oblasť spoločnej kybernetickej obrany, Tallinn, Estónsko.

Obsah

Literatúra a zdroje

Súvisiace predpisy

Národné

- Zákon č. 387/2002 Z. z. o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu
- Zákon č. 110/2004 Z. z. o fungovaní Bezpečnostnej rady Slovenskej republiky v čase mieru
- Zákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy
- Zákon č. 319/2002 Z. z. o obrane Slovenskej republiky
- Zákon č. 42/1994 Z. z. o civilnej ochrane obyvateľstva
- Zákon č. 45/2011 Z. z. o kritickej infraštruktúre
- Zákon č. 251/2012 Z. z. o energetike a o zmene a doplnení niektorých zákonov
- Zákon č. 261/2002 Z. z. o prevencii závažných priemyselných havárií a o zmene a doplnení niektorých zákonov
- Zákon č. 351/2011 Z. z. o elektronických komunikáciách
- Zákon č. 308/2000 Z. z. o vysielaní a retransmisii a o zmene zákona č. 195/2000 Z. z. o telekomunikáciách
- Zákon č. 143/1998 Z. z. o civilnom letectve (letecký zákon) a o zmene a doplnení niektorých zákonov
- Zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov
- Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov
- Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
- Zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov
- Zákon č. 250/2007 Z. z. o ochrane spotrebiteľa
- Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov
- Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov
- Zákon č. 300/2005 Z. z. Trestný zákon
- Uznesenie vlády SR č. 136/2010 Legislatívny zámer zákona o informačnej bezpečnosti
- Uznesenie vlády SR č. 391/2009 Systém vzdelávania v oblasti informačnej bezpečnosti v Slovenskej republike
- Výnos Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy

Medzinárodné – EÚ

- Nariadenie Európskeho parlamentu a Rady (EÚ) č. 460/2004/ES z 10. marca 2004 o zriadení Európskej agentúry pre bezpečnosť sietí a informácií
- Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1077/2011/ES, ktorým sa zriaďuje Európska agentúra na prevádzkové riadenie rozsiahlych informačných systémov v priestore slobody, bezpečnosti a spravodlivosti
- Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES
- Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
- Smernica Európskeho parlamentu a Rady (EÚ) č. 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii
- Smernica Európskeho parlamentu a Rady (EÚ) č. 2002/58/ES z 12. júla 2002 týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií, transponovaná do zákona č. 351/2011 Z. z. o elektronických komunikáciách
- Smernica Európskeho parlamentu a Rady (EÚ) č. 2008/114/ES z 8. decembra 2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu
- Rozhodnutie Rady (EÚ) č. 92/242/EHS z 31. marca 1992 o bezpečnosti informačných systémov
- Rozhodnutie Rady (EÚ) č. 2011/292/EÚ z 31. marca 2011 o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ
- Rozhodnutie Rady (EÚ) č. 2005/222/SVV z 24. februára 2005 o útokoch na informačné systémy
- Stratégia kybernetickej bezpečnosti Európskej únie (Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace), 2013
- Oznámenie Komisie z 28. marca 2012 o zriadení Európskeho centra boja proti kybernetickej kriminalite (EC3), COM(2012)140

Medzinárodné – NATO

- Politika kybernetickej obrany NATO (NATO Policy on Cyber Defence)
- Akčný plán kybernetickej obrany NATO (NATO Cyber Defence Action Plan)
- Posilnená politika kybernetickej obrany NATO (Enhanced NATO Policy on Cyber Defence)

Strategické a koncepčné dokumenty na úseku kybernetickej bezpečnosti

- Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020 schválený uznesením vlády SR č. 93/2016
- Správa o plnení úloh vyplývajúcich z materiálu Príprava Slovenskej republiky na plnenie úloh v oblasti kybernetickej obrany vyplývajúcich z cieľov spôsobilostí Slovenskej republiky, schválená uznesením vlády SR č. 334/2015
- Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020, schválená uznesením vlády SR č. 328/2015

- Správa o plnení úloh vyplývajúcich z materiálu Príprava Slovenskej republiky na plnenie úloh v oblasti kybernetickej obrany vyplývajúcich z cieľov spôsobilostí Slovenskej republiky (2015)
- Príprava Slovenskej republiky na plnenie úloh v oblasti kybernetickej obrany vyplývajúcich z cieľov spôsobilostí Slovenskej republiky schválená uznesením vlády SR č. 497/2014
- Správy o plnení úloh z Národnej stratégie pre informačnú bezpečnosť v Slovenskej republike a akčného plánu z rokov 2009 až 2014, predložené na rokovanie vlády SR (2014)
- Legislatívny zámer zákona o informačnej bezpečnosti, schválený uznesením vlády SR č. 136/2010
- Akčný plán na roky 2009 až 2013 k dokumentu Národná stratégia pre informačnú bezpečnosť v Slovenskej republike schválený uznesením vlády SR č. 46/2010
- Národná politika pre elektronické komunikácie na roky 2009 – 2013 schválená uznesením vlády SR č. 360/2009
- Návrh organizačného, personálneho, materiálno-technického a finančného zabezpečenia na vytvorenie špecializovanej jednotky pre riešenie počítačových incidentov v Slovenskej republike – CSIRT.SK, schválený uznesením vlády SR č. 479/2009
- Návrh systému vzdelávania v oblasti informačnej bezpečnosti/kybernetickej bezpečnosti v Slovenskej republike, schválený uznesením vlády SR č. 391/2009
- Koncepcia šifrovej ochrany informácií, schválená uznesením vlády SR č. 771/2008
- Národná stratégia pre informačnú bezpečnosť Slovenskej republiky schválená uznesením vlády SR č. 570/2008
- Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany schválená uznesením vlády SR č. 120/2007
- Bezpečnostná stratégia Slovenskej republiky (2005)

Iné zdroje

- Odporúčania ENISA (nie sú právne záväzné, ale môžeme konfrontovať s našou právnou úpravou)
- ISO normy, najmä ISO27k

Zoznam použitých skratiek

Akčný plán	Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020 schválený uznesením vlády SR č. 93/2016 (2016)
CSIRT/CERT	Computer Security Incident Response Team/Computer Emergency Response Team
ENISA	Európska agentúra pre bezpečnosť sietí a informácií
EÚ alebo Únia	Európska únia
GDPR	Nariadenie Európskeho parlamentu a Rady (EÚ) č. 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119/89, 4. 5. 2016)
ITIL®	z angl. „Information Technology Infrastructure Library" je súbor publikácií, ktorý obsahuje zbierku najlepších skúseností z odboru riadenia IT služieb (skratka je registrovanou ochrannou známkou)
Jednotka CSIRT	Jednotka pre riešenie kybernetických bezpečnostných incidentov [§ 1 písm. d) Zákona]
Jednotný informačný systém kybernetickej bezpečnosti alebo JISKB	§ 8 Zákona
Kompetenčný zákon	Zákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v platnom znení
Koncepcia kybernetickej bezpečnosti SR	Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020, schválená uznesením vlády SR č. 328/2015 (2015)
Krízový zákon	Zákon č. 387/2002 Z. z. o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu v platnom znení
Nariadenie eIDAS	Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES
NATO	Organizácia Severoatlantickej zmluvy
Notársky poriadok	Zákon č. 323/1992 Zb. o notároch a notárskej činnosti (Notársky poriadok) v platnom znení
Občiansky zákonník	Zákon č. 40/1964 Zb. Občiansky zákonník v platnom znení
Obchodný zákonník alebo ObZ	Zákon č. 513/1991 Zb. Obchodný zákonník v platnom znení

Poskytovateľ digitálnej služby alebo PDS	§ 3 písm. n) Zákona
Prevádzkovateľ základnej služby alebo PZS	§ 3 písm. l) Zákona
Smernica NIS	Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii
Správny poriadok	Zákon č. 71/1967 Zb. Správny poriadok v platnom znení
Správny súdny poriadok	Zákon č. 162/2015 Z. z. Správny súdny poriadok v platnom znení
SR	Slovenská republika
Trestný poriadok	Zákon č. 301/2005 Z. z. Trestný poriadok v platnom znení
Trestný zákon	Zákon č. 300/2005 Z. z. Trestný zákon v platnom znení
Úrad alebo NBÚ alebo Národný bezpečnostný úrad	podľa § 34 Kompetenčného zákona
Vyhláška NBÚ č. 164/2018 Z. z.	Vyhláška Národného bezpečnostného úradu č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby)
Vyhláška NBÚ č. 165/2018 Z. z.	Vyhláška Národného bezpečnostného úradu č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov
Vyhláška NBÚ č. 166/2018 Z. z.	Vyhláška Národného bezpečnostného úradu č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov
Vyhláška NBÚ č. 362/2018 Z. z.	Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
Vykonávacie nariadenie Komisie (EÚ) 2018/151	Vykonávacie nariadenie Komisie (EÚ) 2018/151 z 30. januára 2018, ktorým sa stanovujú pravidlá uplatňovania smernice Európskeho parlamentu a Rady (EÚ) 2016/1148, pokiaľ ide o bližšiu špecifikáciu prvkov, ktoré musia poskytovatelia digitálnych služieb zohľadňovať pri riadení rizík v oblasti bezpečnosti sietí a informačných systémov, a parametrov na posudzovanie tohto, či má incident závažný vplyv (Ú. v. EÚ L 26, 31. 1. 2018)
Výnos o štandardoch	Výnos Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy

Zákon o e-Governmente	Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v platnom znení
Zákon o NBS	Zákon č. 566/1992 Zb. o Národnej banke Slovenska v platnom znení
Zákon o bankách	Zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v platnom znení
Zákon o bezpečnosti štátu	Ústavný zákon č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu v platnom znení
Zákon o elektronických komunikáciách	Zákon č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov v platnom znení
Zákon o ISVS	Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v platnom znení
Zákon o kontrole	Zákon č. 10/1996 Z. z. o kontrole v štátnej správe v platnom znení
Zákon o kritickej infraštruktúre alebo ZoKI	Zákon č. 45/2011 Z. z. o kritickej infraštruktúre v platnom znení
Zákon o obrane	Zákon č. 319/2002 Z. z. o obrane Slovenskej republiky v platnom znení
Zákon o OOÚ	Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v platnom znení
Zákon o OUS	Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v platnom znení
Zákon o priestupkoch	Zákon č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov v platnom znení
Zákon o SIS	Zákon č. 46/1993 Z. z. o Slovenskej informačnej službe v platnom znení
Zákon o VS	Zákon č. 198/1994 Z. z. o Vojenskom spravodajstve v platnom znení
Zákon alebo ZoKB	Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v platnom znení
Zákonník práce alebo ZP	Zákon č. 311/2001 Z. z. Zákonník práce v platnom znení
Zmluva o fungovaní EÚ alebo ZFEÚ	Zmluva o fungovaní Európskej únie v platnom znení (Ú. v. EÚ C 326, 26. 10. 2012)
Živnostenský zákon	Zákon č. 455/1991 Zb. o živnostenskom podnikaní (živnostenský zákon) v platnom znení

Úvod

Bolo to relatívne nedávno, 80. roky minulého storočia, keď do bežného života ľudí, podnikov a domácností vstúpila výpočtová technika. Už to zrazu neboli len imaginárne výpočtové strediská a zariadenia vybavené veľkými kotúčmi pamäťových pások, skryté za hrubými stenami a dostupné len úzkemu okruhu zasvätených, ale hmatateľná každodenná skúsenosť. Zo začiatku, ako každá nová technológia, aj táto bola obmedzená na ekonomické možnosti podnikov a jednotlivcov.

Zákony trhu, tlak ponuky – dopytu spôsobili, že približne od roku 1981, kedy je datované uvedenie prvého výpočtového stroja, tzv. „Von Neumannovej" architektúry (strojcovia ho prezieravo nazvali osobný počítač), sa stalo toto zariadenie čoraz kompaktnejšie a výkonnejšie... A kde sa nachádzame v súčasnosti? Pri každodennej rutinnej práci či zábave s výpočtovými zariadeniami si dnes málokto uvedomuje, že merateľný výpočtový výkon bežne dostupného lacného smartfónu sa už vôbec nedá porovnať s výkonom vtedajšieho špičkového osobného počítača od IBM.

Spomínaná Von Neumannova schéma predstavuje teoretickú vnútornú architektúru počítača, ktorá s drobnými vylepšeniami zostala zachovaná dodnes. Navrhol ju v roku 1945 americký matematik John Von Neumann ako model samočinného digitálneho počítača. Teda – nič nové? Isteže áno. Výpočtové zariadenia alebo tiež informačno-komunikačné technológie sú čoraz menšie, čoraz výkonnejšie, vzájomne zosieťované, prepojené rýchlymi komunikačnými kanálmi, so širokým geografickým pokrytím a s čoraz efektívnejšími rozhraniami na komunikáciu stroja s človekom. Samostatne sa učiace počítače sú už samozrejmosťou a v posledných rokoch sú témou postupné kroky aj ku vzniku umelej inteligencie. Kam to smeruje? Lepšie si to môžeme predstaviť po prečítaní niektorého zo známych diel vedeckej fantastiky. Dúfajme spoločne, že nie práve George Orwella.

Riziká sú všade okolo nás

Iste sa zhodneme, že rozmach informačno-komunikačných technológií spôsobil revolúciu v spôsobe života ľudskej civilizácie. Dnes už zrejme nikto nepochybuje o tom, že ľudia sú od informácií závislí. A nie je to len závislosť, ktorú symbolizuje neustále sklonená ľudská tvár nad mobilným telefónom. Veď závislosť od informácií sa týka aj mnohých hospodárskych odvetví a správy vecí verejných. Informačné technológie sú dnes neoddeliteľnou súčasťou života spoločnosti. Avšak rastúca závislosť od informačných technológií znamená zároveň i dramatický nárast rizík a potrebu nepretržitej a systematickej ochrany informačných aktív – teda ochrany majetku, hmotného i nehmotného.

A ako znie zjednodušená definícia vlastníctva (ekonómovia nám to zjednodušenie pre tento účel odpustia)? Za vlastníctvo sa považuje všetko, čo človeku patrí, nad čím má plnú moc. Zvyčajne sa pod pojmom vlastníctvo myslí úplná kontrola nad vecou alebo akoukoľvek potenciálnou hodnotou. Avšak za hodnotu sa okrem hmotných statkov nepochybne považujú aj nehmotné statky a práva, v digitálnej ére – informačné aktíva. Duševné vlastníctvo je zastrešujúci pojem pre rôzne formy nárokov, ktoré sa upínajú k nápadom, myšlienkam alebo iným nehmotným statkom a právam. Pojem „duševné vlastníctvo" reflektuje na to, že predmetom je výsledok tvorivej intelektuálnej činnosti a ten by mal byť rovnako chránený ako iné formy vlastníctva alebo majetku.

Ako každá činnosť, aj používanie technológií prináša isté riziká. Riziko je funkcia pravdepodobnosti, že hrozba (potenciálna príčina nechceného) využije známu alebo neznámu zraniteľnosť, pričom jej následkom nastane udalosť typicky prinášajúca nežiaduci dosah na

hodnoty. O tejto teórii sa dozviete podrobnejšie v ďalších kapitolách. Výraz riziko je však nutné spomenúť pre lepšie pochopenie pojmu „bezpečnosť“ a prečo sa nejaká časť bezpečnosti v posledných rokoch čoraz častejšie označuje ako „kybernetická“.

Ľudia podvedome riešia riziká vo svojom každodennom živote. Riziko, že nestihnete prísť včas do práce, že zabudnete na niečo dôležité, že sa pošmyknete ponáhľajúc sa po zasneženom chodníku, že cestou autom nabúrate vozidlo pred sebou... Riziko, že sa váš šéf zle vyspal a svoju zlosť si vybije na vás, že cestou domov zabudnete manželke kúpiť kvety na výročie zoznámenia. Riziká majú rôznu pravdepodobnosť a rôzny potenciálny dosah. Identifikácia rizík, ich analýza a správne vyhodnotenie je mnohokrát doslova vecou zdravia, života alebo smrti.

Pokiaľ ide o politikov a manažérov, to nástojčivé používanie výrazu „kybernetická bezpečnosť“ spočíva najmä v marketingu. Výraz „kybernetický“ a predpony „kyber“ či „cyber“ znejú príťažlivejšie a prednášajúceho to v očiach poslucháča robí odborne zdatnejším.

Rozdielne ponímanie odborovej kategorizácie bezpečnosti od niektorých kolegov z odvetvia spočíva v chybnom presadzovaní pohľadu z pozície subjektu a v určitom vedomom potláčaní podstaty či existencie objektu.

V technických odboroch autoritatívnou referenciou pre názvoslovie je (a dúfajme, že dlho zostane) príslušná medzinárodná technická norma. Názvoslovie a popis vzťahov v oblasti kybernetickej bezpečnosti, popis jedinečných aspektov tejto činnosti, vzťah k iným bezpečnostným doménam a základné postupy pre všetky zainteresované strany v kybernetickom priestore poskytuje napríklad medzinárodná norma ISO/IEC 27032 Information technology – Security techniques – Guidelines for cybersecurity (v preklade Informačné technológie – Bezpečnostné metódy – Návody pre kybernetickú bezpečnosť).

Odhliadnuc od faktu, že platí táto medzinárodná norma, je možné naďalej tvrdiť, že prídavné meno „kybernetická“ sa k bezpečnosti hodí, len ak hovoríme o bezpečnosti elektronicky spracovaných dát. Elektronicky spracované je aj elektronicky ovládané – teda rovnaká logika platí aj pre riadiace systémy.

Pre poriadok treba uviesť, že technická normalizácia v informačnej bezpečnosti sa nezaoberá niektorými špecifickými odvetviami, ako napríklad národnou obranou a kriminalistikou. Vzhľadom na vysokú úroveň špecializácie sú tieto činnosti prirodzene ponechané na rozvoj samostatných odvetví, pričom nikto z odbornej verejnosti voči tomu nenamieta. Objektom ochrany je zaručenie bezpečnosti informácií, nie pocit bezpečnosti ich vlastníkov.

Dobro, zlo a bezpečnosť. Sokrates sa snáď mýlil?

Sokrates veril, že kto pozná dobro, koná iba dobro, pretože nikto nerobí dobrovoľne zlé veci (tzv. etický intelektualizmus). Tvrdil, že nikto nie je zlý z vlastnej vôle, ale iba z neznalosti dobra, pretože zlo je dôsledok neznalosti toho, čo je dobré.

V tomto tvrdení ale možno nájsť rozpor z hľadiska výrokovej logiky. Pretože:

- ak jeden človek je schopný konať zlo, potom mnohí ľudia sú schopní konať zlo,
- keďže mnohí ľudia sú schopní konať zlo, potom v závislosti od úrovne rizika je niekedy nutné chrániť ľudské hodnoty,
- ak sú všetci ľudia schopní konať zlo, potom je pravdepodobné, že ľudské hodnoty sú občas chránené takými ľuďmi, ktorí sú schopní konať zlo.

Z vyššie uvedeného vyplýva, že ak informačná bezpečnosť je jedným zo spôsobov ochrany ľudských hodnôt, potom je možno existencia informačnej bezpečnosti ako procesu či vedeckej disciplíny dôkazom, že Sokrates sa mýlil...

Samozrejme, táto úvaha má byť len sarkazmom, ktorého cieľom je vyprovokovať diskusiu. Pravda, dokázaná neskôr mnohými filozofmi, je taká, že ľudia nie sú iba zlí alebo iba dobrí. Podstatné je vedieť to efektívne rozpoznať.

Východiská právnej úpravy kybernetickej bezpečnosti

Súčasná spoločnosť je stále viac závislá od informačných a komunikačných technológií (ďalej ako „IKT"), ktoré v poslednom desaťročí zmenili a ovplyvnili takmer každý aspekt spoločenského života. Činnosti a aktivity nielen právnických, ale aj fyzických osôb sa pomaly presúvajú z fyzického do kybernetického priestoru. Napokon sa očakáva, že súčasná povinnosť elektronickej komunikácie so štátnymi orgánmi uložená právnickým osobám a fyzickým osobám – podnikateľom sa pomaly presunie aj na fyzické osoby – nepodnikateľov. Zároveň platí, že IKT sú už dlhodobo súčasťou riadiacich a výrobných systémov, spotrebnej elektroniky, vozidiel, ako aj ďalších výrobkov v rámci internetu vecí.

Je nepochybné, že IKT pri každodenných ľudských aktivitách uľahčujú život, urýchľujú komunikáciu a prístup k informáciám a službám. Na druhej strane však narastajúca závislosť verejného a súkromného sektora od týchto technológí v prípade nedostatočnej ochrany spôsobuje aj ich vyššiu zraniteľnosť a s tým spojené väčšie potenciálne následky kybernetických bezpečnostných incidentov, v dôsledku čoho sa právna regulácia kybernetickej bezpečnosti stáva vysoko aktuálnou. Následky kybernetických bezpečnostných incidentov sa totižto nemusia nevyhnutne prejaviť len v materiálnych škodách, ale v prípade kybernetického bezpečnostného incidentu spočívajúceho v narušení základných obslužných služieb štátu s prepojením na kybernetický priestor aj v oveľa závažnejších škodách na životoch alebo zdraví obyvateľstva, či v ohrození alebo narušení národnej bezpečnosti.

Je štatisticky preukázané, že cielené útoky proti IKT sú na vzostupe a ich dosah spôsobuje rozsiahle ekonomické škody ako vo verejnom, tak aj v súkromnom sektore, nevynímajúc reputačné riziko v podobe negatívnych politických dôsledkov na národnej alebo medzinárodnej úrovni. Rovnako je celosvetovo zaznamenávaná narastajúca sofistikovanosť a efektivita útokov proti IKT, a to najmä v dôsledku narastajúcej organizovanosti pôvodcov týchto útokov v rámci kybernetickej priemyselnej špionáže, kybernetického terorizmu a v neposlednom rade aj kybernetických útokov v oblasti vojenských operácií v rámci vedenia tzv. hybridnej vojny. Kybernetické útoky sú čím ďalej, tým viac zamerané na prvky kritickej infraštruktúry v oblastiach telekomunikácií, bankovníctva, energetiky, zdravotníctva, dopravy alebo verejnej správy.

Nemenej významným faktorom vyplývajúcim zo samotného charakteru kybernetického priestoru je fakt, že akékoľvek, čo i len čiastočné narušenie alebo zlyhanie aktíva v dôsledku kybernetického bezpečnostného incidentu môže znamenať následné ohrozenie alebo priamo narušenie ďalších aktív kdekoľvek na svete a v rámci ktoréhokoľvek informačného systému.

Kybernetický priestor a s ním spojenú bezpečnosť je nutné vnímať ako jeden z kľúčových komponentov bezpečnosti štátu. Napokon, kybernetický priestor bol na summite Organizácie Severoatlantickej zmluvy (ďalej ako „NATO") vo Varšave už v roku 2016 uznaný za piatu operačnú doménu. Kybernetickú bezpečnosť je možné v jednoduchosti charakterizovať ako súhrn právnych a technických požiadaviek na bezpečnosť aktív v rámci kybernetického priestoru vrátane špecifikácie príslušných práv, povinností a zodpovedností jednotlivých aktérov v rámci kybernetického priestoru. Práve s uvedeným bolo potrebné sa vysporiadať v rámci jednotného, uceleného a konzistentného právneho predpisu, na základe ktorého by bolo možné prípadné kybernetické bezpečnostné incidenty riešiť kvalifikovane a z centrálnej úrovne. Zároveň sa ako vhodné javí na základe konzistentnej právnej úpravy rozčleniť a klasifikovať IKT do viacerých skupín (klasifikačných stupňov) a stanoviť minimálne požiadavky, prípadne povinnosti na ich ochranu. Koordinácia činností jednotlivých

aktérov podieľajúcich sa na ochrane kybernetického priestoru je nemenej dôležitým aspektom riadenia kybernetickej bezpečnosti.

Ďalším argumentom, prečo jednotnú právnu úpravu kybernetickej bezpečnosti na národnej úrovni prijať, boli dlhodobé záväzky Slovenskej republiky ako členského štátu NATO a Európskej únie (ďalej ako „EÚ"). V rámci medzinárodnej regulácie kybernetickej bezpečnosti je dlhodobo vyvíjaný tlak riešiť problematiku ochrany kybernetického priestoru formou záväznej právnej úpravy. Vzájomná previazanosť IKT a globálny charakter kybernetického priestoru spôsobujú, že kybernetický bezpečnostný incident môže mať dosah v ktorejkoľvek krajine alebo v rámci akéhokoľvek informačného systému, čo si vyžaduje intenzívnu medzinárodnú spoluprácu a koncepčné a koordinované riadenie ochrany a obrany kybernetického priestoru. Na riešenie bezpečnostných incidentov si jednotlivé krajiny zriaďujú pracoviská typu CERT/CSIRT („Computer emergency response team/Computer Security Incident Response Team").

Jedným z posledných dôvodov prijatia zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti (ďalej ako „Zákon") bolo prijatie Smernice NIS, ktorú mali členské štáty povinnosť do 9. mája 2018 náležite transponovať do svojich vnútroštátnych právnych poriadkov. Cieľom Smernice NIS je dosiahnutie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v rámci EÚ, ktorú by samostatnými partikulárnymi právnymi úpravami na úrovni jednotlivých členských štátov nebolo možné uspokojivo dosiahnuť. Prijatie celoeurópskeho predpisu regulujúceho kybernetickú bezpečnosť v podobe Smernice NIS má svoju oporu v spôsobilosti EÚ v súlade so zásadou prenesenia právomocí, subsidiarity a proporcionality podľa článku 5 Zmluvy o Európskej únii dosahovať vymedzené ciele, v tomto jednotlivom prípade vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v rámci EÚ.

Kybernetická bezpečnosť Slovenskej republiky, resp. ochrana kybernetického priestoru neboli pred prijatím Zákona výslovne a komplexne upravené v žiadnom platnom právnom predpise Slovenskej republiky. Zároveň v Slovenskej republike nebol prijatý ani len taký osobitný právny predpis, ktorý by sa problematike kybernetickej bezpečnosti venoval čo i len čiastočne alebo okrajovo, hoci sa viaceré právne predpisy čo do svojej pôsobnosti kybernetickej bezpečnosti týkajú.

Čo sa týka terminológie v oblasti kybernetickej bezpečnosti, slovo „kybernetický", ako ani jeho ďalšie gramatické tvary či modifikácie sa nevyskytuje v žiadnom inom všeobecne záväznom právnom predpise mimo Zákona, rovnako ako ani v terminologických slovníkoch.

Téme kybernetickej bezpečnosti bola čiastočne venovaná pozornosť v dokumente „Národná stratégia pre informačnú bezpečnosť v Slovenskej republike" a v nadväzujúcom „Akčnom pláne na roky 2009 až 2013 k dokumentu Národná stratégia pre informačnú bezpečnosť v Slovenskej republike".

Prvým koncepčným a strategickým dokumentom pre oblasť kybernetickej bezpečnosti prijatým na národnej úrovni bola však až Koncepcia kybernetickej bezpečnosti SR, ktorá definuje východiská a ciele Slovenskej republiky v oblasti kybernetickej bezpečnosti. Koncepcia kybernetickej bezpečnosti SR je základným a východiskovým dokumentom pre následnú tvorbu právnych predpisov (najmä vytvorenie a prijatie legislatívneho rámca kybernetickej bezpečnosti), štandardov, metodických pokynov, pravidiel, bezpečnostných politík a iných nástrojov potrebných na zaistenie kybernetickej bezpečnosti.

Koncepcia kybernetickej bezpečnosti SR stanovuje východiská a ciele Slovenskej republiky v oblasti kybernetickej bezpečnosti a je považovaná za základný a východiskový dokument aj pri príprave a vypracovaní samotného Zákona. Aj napriek tomu, že do účinnosti Zákona absentovala komplexná právna úprava pre oblasť kybernetickej bezpečnosti v podobe konkrétneho právneho predpisu v Slovenskej republike, v právnom poriadku Slovenskej

republiky je možné identifikovať viaceré právne predpisy, ktoré sa problematiky kybernetickej bezpečnosti týkajú a ktorých exemplifikatívny výpočet uvádzame nižšie.

Koncepcia kybernetickej bezpečnosti SR navrhla prijať a prioritne riešiť sedem kľúčových opatrení, a to:

- opatrenie č. 1: Vytvorenie inštitucionálneho rámca riadenia kybernetickej bezpečnosti,
- opatrenie č. 2: Vytvorenie a prijatie legislatívneho rámca kybernetickej bezpečnosti,
- opatrenie č. 3: Rozpracovanie a aplikácia základných mechanizmov zabezpečenia správy kybernetického priestoru,
- opatrenie č. 4: Podpora, vypracovanie a zavedenie systému vzdelávania v oblasti kybernetickej bezpečnosti,
- opatrenie č. 5: Stanovenie a aplikácia kultúry riadenia rizík a systému komunikácie medzi zainteresovanými stranami,
- opatrenie č. 6: Aktívna medzinárodná spolupráca,
- opatrenie č. 7: Podpora vedy a výskumu v oblasti kybernetickej bezpečnosti.

So zámerom dosiahnutia cieľov a priorít v rámci opatrenia č. 2 Koncepcia kybernetickej bezpečnosti SR stanovila práve vytvorenie a prijatie legislatívneho rámca kybernetickej bezpečnosti v podobe osobitného zákona o kybernetickej bezpečnosti, a teda prijatie dnes známeho Zákona. Koncepcia kybernetickej bezpečnosti SR určila, že nový zákon o kybernetickej bezpečnosti má formálne zabezpečiť koordináciu a realizáciu jednotnej štátnej politiky v oblasti kybernetickej bezpečnosti, explicitne stanoviť vecnú pôsobnosť a kompetencie orgánov verejnej moci a ostatným aktérom pôsobnosť a rozsah ich aplikácie. Rovnako má stanoviť na jednej strane povinnosti pre subjekty využívajúce informačné a komunikačné technológie v kybernetickom priestore a na druhej strane zároveň garantovať práva a právom chránené záujmy ostatných fyzických a právnických osôb. Uznesenie vlády č. 328 zo 17. júna 2015 uložilo úlohu pripraviť a predložiť návrh zákona o kybernetickej bezpečnosti riaditeľovi Národného bezpečnostného úradu.

V zmysle uvedeného a vzhľadom na to, že na jednej strane štátne orgány môžu v zmysle čl. 2 ods. 2 Ústavy Slovenskej republiky konať iba na základe ústavy, v jej medziach a v rozsahu a spôsobom, ktorý ustanoví zákon, a na strane druhej súkromnoprávnym subjektom možno v súlade s čl. 2 ods. 3 Ústavy Slovenskej republiky ukladať povinnosti len na základe zákona, aj právna regulácia v oblasti kybernetickej bezpečnosti mohla byť uskutočnená len formou zákona obsahujúceho podrobné vymedzenie povinností subjektov, ktoré sú primárne dôležité pre fungovanie štátu, ako aj ostatných subjektov, ktorých sa kybernetická bezpečnosť a ochrana kybernetického priestoru bezprostredne dotýka.

Základným cieľom Zákona je zvýšiť bezpečnosť kybernetického priestoru, v tejto súvislosti identifikovať príslušné povinnosti a zodpovednosti povinných osôb v zmysle Zákona, identifikovať technické a organizačné požiadavky na zaistenie kybernetickej bezpečnosti či nastaviť mechanizmus aktívnej spolupráce medzi súkromným sektorom a verejnou správou s cieľom vyššej efektivity pri riešení kybernetických bezpečnostných incidentov.

Chronológia/história právnej úpravy

EÚ – ENISA

ENISA je odborným centrom pre kybernetickú bezpečnosť v Európe, ktorá bola založená v roku 2004 na základe Nariadenia Európskeho parlamentu a Rady (ES) č. 460/2004 o zriadení Európskej agentúry pre bezpečnosť sietí a informácií. ENISA bola zriadená s cieľom zabezpečenia vysokej a účinnej úrovne bezpečnosti sietí a informácií v rámci

Spoločenstva a s cieľom vybudovať kultúru bezpečnosti sietí a informácií v prospech občanov, spotrebiteľov, podnikov a organizácií verejného sektora EÚ.

Nariadením Európskeho parlamentu a Rady (ES) č. 1007/2008, ktorým sa mení a dopĺňa nariadenie (ES) č. 460/2004 o zriadení Európskej agentúry pre bezpečnosť sietí a informácií, pokiaľ ide o dobu jej trvania, došlo k predĺženiu mandátu ENISA do 13. marca 2012 a Nariadením Európskeho parlamentu a Rady (EÚ) č. 580/2011, ktorým sa mení a dopĺňa nariadenie (ES) č. 460/2004 o zriadení Európskej agentúry pre bezpečnosť sietí a informácií, pokiaľ ide o jej trvanie, k predĺženiu do 13. septembra 2013.

Nariadením Európskeho parlamentu a Rady (EÚ) č. 526/2013 o Agentúre Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA) a o zrušení nariadenia (ES) č. 460/2004 došlo k zrušeniu Nariadenia o zriadení ENISA a posilneniu ENISA tak, aby úspešne prispievala k úsiliu inštitúcií EÚ a členských štátov rozvinúť európsku schopnosť čeliť výzvam spojeným so sieťovou a informačnou bezpečnosťou. V zmysle predmetného nariadenia ENISA vykonáva úlohy, ktoré sú jej zverené so zámerom prispieť k vysokej úrovni sieťovej a informačnej bezpečnosti v rámci EÚ a s cieľom zvýšiť povedomie o sieťovej a informačnej bezpečnosti a rozvinúť a presadzovať v spoločnosti kultúru sieťovej a informačnej bezpečnosti v prospech občanov, spotrebiteľov, podnikov a organizácií verejného sektora v EÚ, a tak prispieť k zriadeniu a riadnemu fungovaniu vnútorného trhu.

ENISA úzko spolupracuje s členskými štátmi a so súkromným sektorom na poskytovaní poradenstva a riešení pre oblasť kybernetickej bezpečnosti. Významnou úlohou ENISA je podpora organizácie a vykonávania cvičení v oblasti sieťovej a informačnej bezpečnosti v EÚ a poskytovanie poradenstva o cvičeniach členským štátom na vnútroštátnej úrovni. Takýmto cvičením v správe ENISA pre oblasť sieťovej a informačnej bezpečnosti je celoeurópske cvičenie Cyber Europe týkajúce sa počítačových incidentov a krízového riadenia pre verejný aj súkromný sektor z členských štátov EÚ a Európskeho združenia voľného obchodu. Organizačné a technické zabezpečenie cvičenia v rámci Slovenskej republiky je zabezpečované prostredníctvom CSIRT.SK (Úrad podpredsedu vlády SR pre investície a informatizáciu). Na cvičení sa však podieľajú aj ďalšie zložky štátu pravidelne participujúce na cvičeniach kybernetickej obrany v rámci Slovenskej republiky, a to Úrad, Ministerstvo obrany Slovenskej republiky (prostredníctvom Centra pre kybernetickú obranu Slovenskej republiky), SIS a pod., výnimočne aj aktéri zo súkromného sektora.

SR – Ministerstvo financií SR – Národná stratégia informačnej bezpečnosti 2008 – 2013

Vláda Slovenskej republiky schválila svojím uznesením č. 570/2008 Národnú stratégiu pre informačnú bezpečnosť v Slovenskej republike (2008 – 2013), ktorá okrem iného priniesla návrh na vytvorenie „Národného strediska pre riešenie počítačových incidentov" (CSIRT.SK) a v časovom horizonte do 5 rokov úlohu predložiť legislatívny zámer zákona o informačnej bezpečnosti. Návrh organizačného zabezpečenia informačnej bezpečnosti počítal aj s vytvorením národného inštitútu pre informačnú bezpečnosť ako neutajovanej časti národnej informačnej a komunikačnej infraštruktúry v podobe Národného úradu pre informačnú bezpečnosť SR (NÚIB SR).

SR – Ministerstvo financií SR – Návrh systému vzdelávania v oblasti informačnej bezpečnosti v SR

Vláda Slovenskej republiky schválila svojím uznesením č. 391/2009 Systém vzdelávania v oblasti informačnej bezpečnosti v SR. Dokument bol zameraný na identifikáciu skupín používateľov v rámci digitálneho priestoru, a to od skupiny laikov až po skupinu špecialistov, na odhad ich kvalifikačných potrieb a na návrh obsahu vzdelávania v informačnej

bezpečnosti pre jednotlivé skupiny. Problematika sa nezaoberala prípravou špecialistov na ochranu časti digitálneho priestoru spadajúceho pod zákon o OUS.

Výstupom uvedeného dokumentu bolo teda stanovenie základných cieľov, návrh úloh a aktivít v oblasti vzdelávania v informačnej bezpečnosti a návrh opatrení, ktorý bol premietnutý do úloh určených v uznesení vlády.

Išlo najmä o vypracovanie štandardu základných znalostí v oblasti informačnej bezpečnosti pre jednotlivé skupiny od laikov až po špecialistov a implementáciu systému systematického vzdelávania v oblasti informačnej bezpečnosti pre cieľové skupiny s jeho zaradením do všetkých vzdelávacích programov organizovaných štátom v súčinnosti s Ministerstvom školstva SR.

Ako vyplýva z Koncepcie kybernetickej bezpečnosti SR, aj keď odborná príprava špecialistov štátnej správy prebiehala najmä v gescii Ministerstva financií Slovenskej republiky, zvyšovanie povedomia a vzdelávania v oblasti kybernetickej či informačnej bezpečnosti nie je všeobecne obsahovou súčasťou systému vzdelávania v Slovenskej republike (základné, stredné a vysoké školy) ani systému formovania spoločenského povedomia. Vzdelávanie teda nie je riešené na úrovni špecializovaných odborov, ale nanajvýš na úrovni špecializovaných predmetov v rámci vybraných vzdelávacích inštitúcií.

SR – NBÚ – Návrh novelizácie zákona o utajovaných skutočnostiach, snaha o rozšírenie úpravy na informačnú bezpečnosť pre NBÚ

Národný bezpečnostný úrad (ďalej ako „Úrad“) sa svojím návrhom zákona o ochrane utajovaných informácií a o ochrane kybernetického priestoru a o zmene a doplnení niektorých zákonov z roku 2009 pokúsil o novelizáciu vtedajšieho zákona o OUS v rozsahu rozšírenia predmetu úpravy tohto zákona o *„podmienky na ochranu kybernetického priestoru, práva a povinnosti fyzických osôb a právnických osôb pri ochrane kybernetického priestoru*“ a pôsobnosť Úradu a pôsobnosť ďalších orgánov verejnej moci nielen vo vzťahu k ochrane utajovaných informácií, ale aj vo vzťahu k *ochrane kybernetického priestoru*. Uvedený počin Národného bezpečnostného úradu je možné v podmienkach Slovenskej republiky vnímať ako prvú snahu o legislatívnu úpravu a reguláciu kybernetického priestoru. Zároveň sa týmto návrhom zákona Úrad už v roku 2009 pokúsil o nadobudnutie kompetencie gescie nad právnou úpravou kybernetického priestoru. Je však potrebné konštatovať, že uvedený návrh zákona bol po veľkom množstve pripomienok vznesených v rámci medzirezortného pripomienkového konania napokon Úradom stiahnutý a navrhovaná právna úprava kybernetického priestoru odložená na neskoršie obdobie.

SR – Ministerstvo financií SR – Návrh zákona o informačnej bezpečnosti 2010

Ministerstvo financií SR predložilo v súlade s uznesením vlády SR č. 570/2008 úloha B.3 legislatívny zámer zákona o informačnej bezpečnosti, ktorý bol na základe uznesenia vlády SR č. 136/2010 schválený a ktorým bolo ministrovi financií uložené do 31. mája 2011 predložiť na rokovanie vlády návrh zákona o informačnej bezpečnosti. Za hlavný dôvod na vypracovanie zákona o informačnej bezpečnosti sa považovalo zaistenie primeranej ochrany digitálneho priestoru, keďže narušenie alebo zlyhanie jednej časti digitálneho priestoru môže ohroziť inú jeho podstatnú časť alebo aj celý digitálny priestor. Zároveň je konštatované, že zaistenie informačnej bezpečnosti digitálneho priestoru musí byť trvalé a komplexné, a to si vyžaduje systematický, koordinovaný a legislatívne podporený prístup všetkých zainteresovaných subjektov.

Zákon o informačnej bezpečnosti mal riešiť dva okruhy problémov, a to zaistenie ochrany pre informačné systémy verejnej správy a vytvorenie všeobecného právneho rámca pre ochranu celého digitálneho priestoru Slovenskej republiky.

V zmysle uvedeného zákon o informačnej bezpečnosti mal sledovať nasledovné ciele:

- vytvoriť jednotný legislatívny rámec pre oblasť informačnej bezpečnosti v Slovenskej republike,
- definovať kompetencie orgánov štátnej správy v oblasti informačnej bezpečnosti a spôsob koordinácie orgánov štátnej správy pri riešení spoločných úloh v oblasti informačnej bezpečnosti,
- zaviesť jednotnú terminológiu základných pojmov z oblasti informačnej bezpečnosti,
- vytvoriť štandardizačný rámec informačnej bezpečnosti,
- zaviesť proces riadenia informačnej bezpečnosti vo verejnej správe,
- zaviesť klasifikáciu informačných systémov verejnej správy z hľadiska požiadaviek na informačnú bezpečnosť a definovať minimálne bezpečnostné požiadavky pre jednotlivé kategórie informačných systémov verejnej správy,
- vymedziť postavenie jednotky pre riešenie počítačových incidentov (CSIRT.SK) v Slovenskej republike a úlohy ďalších takýchto útvarov pri ochrane digitálneho priestoru Slovenskej republiky,
- definovať minimálne znalostné štandardy v oblasti informačnej bezpečnosti pre pracovníkov spravujúcich informačné systémy verejnej správy a zaisťujúcich ich ochranu,
- ustanoviť minimálne požiadavky na bezpečnosť elektronickej verejnej správy,
- ustanoviť minimálne požiadavky na bezpečnosť internetu,
- zvýšiť celkové povedomie pracovníkov verejnej správy v oblasti informačnej bezpečnosti.

Rovnako ako návrh zákona o ochrane utajovaných informácií a o ochrane kybernetického priestoru, tak ani návrh zákona o informačnej bezpečnosti napokon nebol do legislatívneho procesu predložený, a to aj napriek tomu, že v roku 2014 bol vypracovaný návrh paragrafového znenia zákona o informačnej bezpečnosti. Právna regulácia kybernetickej bezpečnosti (informačná bezpečnosť kybernetického priestoru) tak v Slovenskej republike nebola do roku 2014 v rámci uceleného právneho predpisu komplexne upravená.

Na základe uznesenia vlády č. 276/2014 novú koncepciu kybernetickej bezpečnosti vypracoval a predložil Úrad vlády SR. Koncepcia bola predložená a následne uznesením vlády č. 328/2015 aj schválená. Hlavnými úlohami vyplývajúcimi z koncepcie bolo predložiť do konca roka 2015 akčný plán. Akčný plán schválila vláda uznesením č. 93/2016. Vláda zároveň uznesením č. 366/2015 schválila novelu zákona č. 110/2004 Z. z. o fungovaní Bezpečnostnej rady Slovenskej republiky v čase mieru, ktorá obsahovala vytvorenie výboru pre kybernetickú bezpečnosť v rámci Bezpečnostnej rady SR.

SR – NBÚ – Kompetenčný zákon

Úrad bol na základe zákona č. 339/2015 Z. z., ktorým sa mení a dopĺňa Kompetenčný zákon, s účinnosťou od 1. januára 2016 určený ako ústredný orgán štátnej správy pre kybernetickú bezpečnosť. V tejto súvislosti je potrebné poznamenať, že išlo o novovytvorenú kompetenciu a Úrad je historicky prvým ústredným orgánom štátnej správy pre kybernetickú bezpečnosť v rámci Slovenskej republiky. Jednou z prvých zmienok o začlenení kybernetickej bezpečnosti do pôsobnosti príslušného ústredného orgánu štátnej správy bol návrh o rozšírení pôsobnosti existujúceho odvetvovo nezávislého ústredného orgánu štátnej správy (Úrad) o ďalší úsek štátnej správy v rámci Koncepcie kybernetickej bezpečnosti SR schválenej uznesením vlády SR č. 328 dňa 16. júna 2015. Koncepcia kybernetickej bezpečnosti SR odporúčala, aby túto pôsobnosť zákonodarca zveril práve Národnému bezpečnostnému úradu.

EÚ – Nariadenie o agentúre ENISA

„Európsky parlament, Rada Európskej únie a Európska komisia dosiahli kompromis ohľadom znenia Nariadenia o kybernetickej bezpečnosti (Cybersecurity Act), ktoré má posilniť postavenie agentúry ENISA a priznať jej postavenie Agentúry EÚ pre kybernetickú bezpečnosť. Kompromisné znenie 19. decembra 2018 schválil Výbor stálych predstaviteľov členských štátov pri EÚ (COREPER).

Návrh nariadenia priznáva agentúre ENISA široký mandát v oblasti kybernetickej bezpečnosti a predpokladá vytvorenie európskeho certifikačného rámca. Agentúra bude môcť poskytovať lepšiu podporu a spoluprácu členským krajinám pri riešení kybernetických bezpečnostných incidentov a reagovaní na kybernetické hrozby a útoky.

Najdôležitejšie zmeny sa týkajú celkového postavenia agentúry ENISA:

- agentúra ENISA dostala trvalý mandát s navýšením personálnych kapacít a finančných prostriedkov,
- agentúra ENISA zvýši pomoc a podporu členským štátom EÚ s cieľom zlepšovania schopností a odborných znalostí najmä v oblasti prevencie, riešenia a koordinácie riešenia kybernetických bezpečnostných incidentov,
- v rámci Certifikačného rámca kybernetickej bezpečnosti bude mať agentúra ENISA úlohy súvisiace s trhovým hospodárstvom, najmä v oblasti prípravy certifikačných rámcov, pričom bude poskytovať odbornú pomoc a spoluprácu vnútroštátnym certifikačným orgánom a zástupcom priemyslu,
- agentúra ENISA posilní svoju podporu členským štátom a inštitúciám EÚ pri tvorbe, vykonávaní a revízii pravidiel a politík v oblasti kybernetickej bezpečnosti.

Nariadenie o kybernetickej bezpečnosti ešte vyžaduje schválenie Európskym parlamentom a Radou Európskej únie, legislatívny proces bude najbližšie pokračovať na plenárnom zasadnutí Európskeho parlamentu. Nariadenie nadobudne účinnosť po uverejnení v Úradnom vestníku EÚ.“[1]

Kybernetická bezpečnosť v kontexte kybernetickej obrany

Vzťah kybernetickej bezpečnosti a kybernetickej obrany je legislatívne vymedzený zákonom o VS, kde je v rámci § 4a (doplnený samotným zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti) explicitne uvedené, že: „*Vojenské spravodajstvo plní úlohy na úseku obrany štátu v kybernetickom priestore … prostredníctvom Centra pre kybernetickú obranu Slovenskej republiky, ktoré je osobitnou organizačnou zložkou Vojenského spravodajstva.* “

V zmysle § 2 ods. 1 zákona o obrane sa pod pojmom obrana štátu rozumie „*súhrn opatrení, ktorými Slovenská republika zachováva mier, bezpečnosť, zvrchovanosť, územnú celistvosť a nedotknuteľnosť hraníc a plní záväzky vyplývajúce z medzinárodných zmlúv o spoločnej obrane proti napadnutiu a z ďalších medzinárodných zmlúv vojenskej povahy*.“

V zmysle čl. 1 ods. 2 zákona o bezpečnosti štátu platí: „*Základnou úlohou verejnej moci v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu je vykonávať všetky potrebné opatrenia na obranu štátu a zachovanie jeho bezpečnosti, na ochranu života a zdravia osôb, na ochranu majetku, na dodržiavanie základných práv a slobôd, na odvrátenie ohrozenia alebo na obnovu narušeného hospodárstva, najmä riadneho fungovania zásobovania, dopravy a verejných služieb v obciach a na riadne fungovanie ústavných orgánov.*“

[1] https://www.nbu.gov.sk/2018/12/19/veduci-predstavitelia- eu-schvalili-nove-pravidla-fungovania-pre-agenturu-enisa/index.html

V zmysle bodu 1.5 tabuľky úloh akčného plánu je úlohou Národného bezpečnostného úradu v súčinnosti s Ministerstvom obrany Slovenskej republiky, Ministerstvom vnútra Slovenskej republiky a Bezpečnostnou radou Slovenskej republiky v období 2017/2018 navrhnúť: a) inštitucionálne riadenie kybernetickej bezpečnosti v núdzovom stave, výnimočnom stave, vojnovom stave a stave vojny a b) kontingenčný plán prechodu zodpovednosti za riadenie kybernetickej bezpečnosti v čase mieru, núdzového a výnimočného stavu do vojnového stavu a stavu vojny podľa zákona o bezpečnosti štátu.

Na základe uvedeného je teda možné konštatovať, že oblasť kybernetickej obrany Slovenskej republiky v čase mieru spadá výlučne do kompetencie Ministerstva obrany Slovenskej republiky, ktoré vykonáva úlohy na úseku obrany štátu v kybernetickom priestore prostredníctvom Centra pre kybernetickú obranu Slovenskej republiky (CSIRT.MIL) ako organizačnej zložky Vojenského spravodajstva.

V zmysle § 27 ods. 9 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti platí: *„Ak úrad (pozn. Národný bezpečnostný úrad) na účely zaistenia kybernetickej bezpečnosti vyčerpá všetky spôsoby riešenia závažného kybernetického bezpečnostného incidentu podľa tohto zákona, predloží predsedovi Bezpečnostnej rady Slovenskej republiky informáciu o predpokladaných vplyvoch kybernetického bezpečnostného incidentu na bezpečnosť štátu ako podklad na riešenie krízovej situácie."*

Bezpečnostná rada Slovenskej republiky je v zmysle § 3 písm. a) Krízového zákona č. 387/2002 Z. z. považovaná za orgán krízového riadenia, ktorý v súčinnosti s vládou Slovenskej republiky (prostredníctvom vládou zriadeného ústredného krízového štábu) spolupracuje pri príprave opatrení na riešenie krízovej situácie, ktorá môže po splnení podmienok ustanovených v osobitnom predpise viesť k vyhláseniu výnimočného stavu, núdzového stavu alebo mimoriadnej situácie. Bezpečnostná rada má teda v čase riadenia štátu v krízových situáciách mimo času vojny a vojnového stavu svoje nezastupiteľné postavenie ako orgán krízového riadenia, ktorý sa skladá z deviatich členov, a to predsedu a podpredsedov Bezpečnostnej rady Slovenskej republiky (jednotlivo predseda vlády SR, minister financií, minister obrany, minister vnútra, minister zahraničných vecí a európskych záležitostí, minister hospodárstva, minister dopravy a výstavby, minister spravodlivosti, minister zdravotníctva).

Bezpečnostná rada Slovenskej republiky zároveň na prípravu a plnenie svojich úloh zriaďuje výbory, ktoré sú jej stálymi pracovnými orgánmi, a to výbor pre zahraničnú politiku, výbor pre obranné plánovanie, výbor pre civilné núdzové plánovanie, výbor pre koordináciu spravodajských služieb, výbor pre energetickú bezpečnosť, výbor pre kybernetickú bezpečnosť. Vymenovanie a odvolanie predsedu výboru pre kybernetickú bezpečnosť schvaľuje Bezpečnostná rada Slovenskej republiky na návrh riaditeľa Národného bezpečnostného úradu.

V súvislosti s monitoringom a vyhodnocovaním bezpečnostných hrozieb v Slovenskej republike bolo v gescii Slovenskej informačnej služby zriadené Národné bezpečnostné analytické centrum, v rámci ktorého informačne participujú a spolupracujú zástupcovia Slovenskej informačnej služby, Vojenského spravodajstva, Národného bezpečnostného úradu, Policajného zboru, Kriminálneho úradu finančnej správy, Ministerstva zahraničných vecí a európskych záležitostí a Úradu vlády.

Otáznym teda naďalej zostáva, ako je vymedzený vzťah medzi kybernetickou bezpečnosťou a kybernetickou obranou počas stavu vyhlásenej vojny, vojnového stavu, výnimočného stavu alebo núdzového stavu. Ako bolo spomenuté vyššie, v zmysle úloh vyplývajúcich z akčného plánu je uvedené vo vzťahu ku kybernetickej bezpečnosti zverené ako úloha Národnému bezpečnostnému úradu.

ZÁKON
č. 69/2018 Z. z.
z 30. januára 2018

o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

(v znení zákona č. 373/2018 Z. z.)

Národná rada Slovenskej republiky sa uzniesla na tomto zákone:

Čl. I

§ 1
Predmet zákona

Tento zákon upravuje

a) organizáciu, pôsobnosť a povinnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti,
b) národnú stratégiu kybernetickej bezpečnosti,
c) jednotný informačný systém kybernetickej bezpečnosti,
d) organizáciu a pôsobnosť jednotiek pre riešenie kybernetických bezpečnostných incidentov (ďalej len „jednotka CSIRT“) a ich akreditáciu,
e) postavenie a povinnosti prevádzkovateľa základnej služby a poskytovateľa digitálnej služby,
f) bezpečnostné opatrenia,
g) systém zabezpečenia kybernetickej bezpečnosti,
h) kontrolu nad dodržiavaním tohto zákona a audit.

Z dôvodovej správy

K § 1

V nadväznosti na smernicu NIS sa upravuje predmet zákona, ktorý zodpovedá požiadavkám transpozície a predstavuje nevyhnutý súbor nástrojov zabezpečenia kybernetickej bezpečnosti. Zákon upravuje práva a povinnosti osôb ako aj právomoc a pôsobnosť orgánov verejnej moci.

Súvisiace ustanovenia

- § 4, § 7, § 8, § 13, § 19, § 20, § 22, § 28 a § 29

Súvisiace predpisy

- Kompetenčný zákon
- Zákon o ISVS
- Zákon o kontrole
- Vyhláška NBÚ č. 164/2018 Z. z.
- Vyhláška NBÚ č. 165/2018 Z. z.
- Vyhláška NBÚ č. 166/2018 Z. z.

- Vyhláška NBÚ č. 362/2018 Z. z.
- Vykonávacie nariadenie Komisie (EÚ) 2018/151
- Koncepcia kybernetickej bezpečnosti SR
- Akčný plán

Transpozičné ustanovenia

- Čl. 1 ods. 2 Smernice NIS

Komentár k § 1

K písm. a)

Aj keď ustálenú definíciu pojmu orgán verejnej moci v právnom poriadku SR nenájdeme, v zmysle právnej teórie, ako aj rozhodovacej činnosti súdov je možné konštatovať, že orgánom verejnej moci je akýkoľvek orgán autoritatívne rozhodujúci o právach, právom chránených záujmoch a povinnostiach subjektov bez ohľadu na to, či tento orgán rozhoduje priamo alebo sprostredkovane.[2] Ďalším rozhodujúcim atribútom, na základe ktorého je možné dôvodiť status orgánu verejnej moci, je skutočnosť, že subjekt, o ktorého právach a povinnostiach orgán verejnej moci rozhoduje, je vo vzťahu k tomuto orgánu v podriadenom postavení. Nie menej dôležitým faktorom imanentne prepojeným s verejnou mocou a charakterom rozhodnutí orgánov verejnej moci je vynútiteľnosť týchto rozhodnutí. **Verejnú moc** vykonáva štát predovšetkým prostredníctvom orgánov moci zákonodarnej, výkonnej a súdnej a za určitých podmienok ju môže vykonávať aj prostredníctvom ďalších subjektov.

Ako vyplýva z úvodu tohto komentára, Zákon (odhliadnuc od jeho vymedzenia ako transpozičného zákona Smernice NIS) vychádza z predpokladu naplnenia konkrétnych kľúčových opatrení definovaných Koncepciou kybernetickej bezpečnosti SR, najmä opatrenia č. 1 „*Vytvorenie inštitucionálneho rámca riadenia kybernetickej bezpečnosti*“. Práve toto Koncepciou kybernetickej bezpečnosti SR zavedené opatrenie viedlo k príprave komplexného návrhu rámcového vymedzenia pôsobností a kompetencií subjektov verejnej správy na úseku kybernetickej bezpečnosti. Predmetné opatrenie zároveň aj identifikuje subjekty verejnej správy na úseku kybernetickej bezpečnosti, ktorými sú:

a) centrálny ústredný orgán štátnej správy pre kybernetickú bezpečnosť,
b) národná jednotka pre riešenie incidentov,
c) vecne príslušné autority pre kybernetickú bezpečnosť a
d) jednotky pre riešenie incidentov.

Aj keď Zákon v tomto smere upúšťa od názvoslovia, ktoré so sebou priniesla Koncepcia kybernetickej bezpečnosti SR vo vzťahu k inštitucionálnemu rámcu riadenia kybernetickej bezpečnosti, Koncepciou kybernetickej bezpečnosti SR pôvodne navrhnuté členenie „inštitúcií“ zodpovedných za riadenie kybernetickej bezpečnosti ponecháva. Zákon tak prináša, pokiaľ ide o názvoslovia, síce pozmenený, ale v podstate nedotknutý inštitucionálny rámec riadenia kybernetickej bezpečnosti reprezentovaný orgánmi verejnej moci, ktoré vykonávajú pôsobnosť v oblasti kybernetickej bezpečnosti. Ide o nasledovné orgány verejnej moci:

a) Úrad,

[2] Uznesenie Ústavného súdu Českej a Slovenskej Federatívnej Republiky (prvého senátu) zo dňa 9. júna 1992 sp. zn. I. ÚS 191/92, ktorým sa stanovili kritériá na určenie, či subjekt koná ako orgán verejnej moci. Východiskom pre rozhodnutie senátu Ústavného súdu Českej a Slovenskej Federatívnej Republiky bolo vymedzenie pojmu orgán verejnej moci.

b) ústredné orgány štátnej správy vykonávajúce pôsobnosť v oblasti kybernetickej bezpečnosti, a to Úrad, Ministerstvo dopravy a výstavby Slovenskej republiky, Ministerstvo financií Slovenskej republiky, Ministerstvo hospodárstva Slovenskej republiky, Ministerstvo obrany Slovenskej republiky, Ministerstvo vnútra Slovenskej republiky, Ministerstvo zdravotníctva Slovenskej republiky, Ministerstvo životného prostredia Slovenskej republiky, Slovenská informačná služba, Úrad podpredsedu vlády pre investície a informatizáciu a Vojenské spravodajstvo,

c) iné orgány štátnej správy vykonávajúce pôsobnosť v oblasti kybernetickej bezpečnosti, a to ministerstvá, ktoré nie sú ústredným orgánom podľa písm. b) (Ministerstvo pôdohospodárstva a rozvoja vidieka Slovenskej republiky, Ministerstvo spravodlivosti Slovenskej republiky, Ministerstvo zahraničných vecí a európskych záležitostí Slovenskej republiky, Ministerstvo práce, sociálnych vecí a rodiny Slovenskej republiky, Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky, Ministerstvo kultúry Slovenskej republiky) a ostatné ústredné orgány štátnej správy, ktoré nie sú ústredným orgánom podľa písm. b) (Úrad vlády Slovenskej republiky, Protimonopolný úrad Slovenskej republiky, Štatistický úrad Slovenskej republiky, Úrad geodézie, kartografie a katastra Slovenskej republiky, Úrad jadrového dozoru Slovenskej republiky, Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, Úrad pre verejné obstarávanie, Úrad priemyselného vlastníctva Slovenskej republiky, Správa štátnych hmotných rezerv Slovenskej republiky), Generálna prokuratúra Slovenskej republiky, Najvyšší kontrolný úrad Slovenskej republiky, Úrad pre dohľad nad zdravotnou starostlivosťou, Úrad na ochranu osobných údajov Slovenskej republiky, Úrad pre reguláciu sieťových odvetví a iné štátne orgány v rozsahu svojej pôsobnosti.

Odhliadnuc od subjektov, ktoré jednotlivé kategórie inštitucionálneho rámca reprezentujú, Zákon pôsobnosť v oblasti kybernetickej bezpečnosti zveruje Úradu, vybraným ústredným orgánom štátnej správy a iným orgánom štátnej správy, kam zaraďujeme napr. Úrad vlády či ústredné orgány štátnej správy podľa Kompetenčného zákona nezaradené medzi ústredné orgány štátnej správy vykonávajúce pôsobnosť v oblasti kybernetickej bezpečnosti podľa § 4 písm. b) Zákona. Dôvod, prečo Zákon medzi ústredné orgány štátnej správy podľa § 4 písm. b) Zákona nezaraďuje všetky ústredné orgány štátnej správy podľa Kompetenčného zákona, je ten, že ústredným orgánom štátnej správy podľa Zákona môže byť len taký orgán, ktorý vykonáva svoju pôsobnosť v niektorom zo sektorov alebo podsektorov identifikovaných v prílohe č. 1 Zákona. Aj keď tým ústredným orgánom štátnej správy, ktoré nemajú, resp. ktoré nevykonávajú pôsobnosť v niektorom zo sektorov alebo podsektorov podľa prílohy č. 1 Zákona, samotný zákon postavenie ústredného orgánu podľa § 4 písm. b) Zákona nepriznáva, tieto neostávajú opomenuté, lebo sa všetky považujú za iný orgán štátnej správy podľa § 4 písm. c) Zákona. Rozlišovanie jednotlivých kategórií subjektov vykonávajúcich pôsobnosť v oblasti kybernetickej bezpečnosti je dôležité z hľadiska ďalšieho pochopenia a najmä správnej identifikácie príslušných oprávnení, povinností a zodpovednosti tých subjektov vykonávajúcich pôsobnosť v oblasti kybernetickej bezpečnosti, ktoré sa v závislosti od príslušnej kategórie definovanej v rámci § 4 Zákona výrazne líšia.

Do pôsobnosti Úradu Zákon zveruje úlohy, ktoré možno rozdeliť do nasledovných kategórií:

Normotvorné/právotvorné

- určovanie a vydávanie štandardov, operačných postupov, metodík a politík správania sa v kybernetickom priestore,
- určovanie zásad na predchádzanie kybernetickým bezpečnostným incidentom a zásad na riešenie kybernetických bezpečnostných incidentov,

- vypracúvanie národnej stratégie kybernetickej bezpečnosti a ročnej správy o stave kybernetickej bezpečnosti v SR,
- vydávanie znalostných štandardov (v spolupráci s MŠVVaŠ) a zabezpečenie budovania bezpečnostného povedomia.

Kompetenčné medzinárodné

- plnenie úloh národného kontaktného miesta pre kybernetickú bezpečnosť a spolupráca s jednotnými kontaktnými miestami iných členských štátov EÚ a NATO,
- notifikačné a oznamovacie povinnosti voči príslušným orgánom EÚ a NATO,
- zabezpečovanie členstva SR v skupine pre spoluprácu a v sieti jednotiek CSIRT,
- prijímanie hlásení o kybernetických bezpečnostných incidentoch zo zahraničia; rozvíjanie medzinárodnej spolupráce.

Kompetenčné vnútroštátne

- riadenie a koordinácia výkonu štátnej správy v oblasti kybernetickej bezpečnosti ako ústredný orgán štátnej správy pre kybernetickú bezpečnosť (vyplýva tak zo Zákona, ako aj z osobitného predpisu[3],
- plnenie úloh národnej jednotky CSIRT s pôsobnosťou pre SR,
- postavenie príslušného orgánu pre digitálne služby,
- akreditácia jednotiek CSIRT,
- riešenie kybernetických bezpečnostných incidentov na národnej úrovni,
- spolupráca s orgánmi verejnej moci, jednotkami CSIRT, prevádzkovateľmi základných služieb a poskytovateľmi digitálnych služieb,
- získavanie, sústreďovanie, analýza a vyhodnocovanie informácií o stave kybernetickej bezpečnosti v SR,
- prijímanie vnútroštátnych hlásení o kybernetických bezpečnostných incidentoch, riešenie kybernetických bezpečnostných incidentov,
- určovanie základnej služby a prevádzkovateľa základnej služby, digitálnej služby a poskytovateľa digitálnej služby,
- vedenie a správa zoznamov (základnej služby, digitálnej služby a akreditovaných jednotiek CSIRT) a registrov (prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb).

Ostatné úlohy

- výkon kontrol a auditov,
- výskum a vývoj v oblasti kybernetickej bezpečnosti.

Ústredným orgánom štátnej správy, ktoré vykonávajú pôsobnosť v oblasti kybernetickej bezpečnosti, Zákon vymedzuje nasledovné úlohy:

Kompetenčné

- plnenie úloh jednotky CSIRT v rámci príslušného sektora a podsektora,
- budovanie bezpečnostného povedomia.

[3] Kompetenčný zákon

Majúce charakter povinnosti

- zriadenie a prevádzka akreditovanej jednotky CSIRT (resp. na základe osobitnej zmluvy využíva akreditovanú jednotku CSIRT iného ústredného orgánu),
- poskytovanie požadovanej súčinnosti a informácií dôležitých na zabezpečenie kybernetickej bezpečnosti Úradu,
- aplikácia bezpečnostných opatrení, metodík a politiky správania sa v kybernetickom priestore,
- identifikácia základnej služby a prevádzkovateľa základnej služby,
- predloženie aktuálneho zoznamu identifikovaných základných služieb a prevádzkovateľov základných služieb Úradu.

Spolupráca

- s Úradom [pri určovaní špecifických sektorových identifikačných kritérií podľa Zákona (§ 18 ods. 3)],
- s ostatnými ústrednými orgánmi a prevádzkovateľmi základných služieb,
- so zahraničnou inštitúciou obdobného zamerania.

Ako je uvedené vyššie, tou najzásadnejšou úlohou vzťahujúcou sa na ústredný orgán štátnej správy podľa § 4 písm. b) Zákona je plnenie úloh kybernetickej bezpečnosti vyplývajúcich zo Zákona vo vzťahu k príslušnému sektoru alebo podsektoru z prílohy č. 1 Zákona, ktorý ústredný orgán „pokrýva“, a teda ktorý je v gescii ústredného orgánu. Pokryť príslušný sektor alebo podsektor podľa prílohy č. 1 Zákona okrem iného znamená zriadiť a prevádzkovať vlastnú akreditovanú jednotku CSIRT alebo využívať inú akreditovanú jednotku CSIRT, takú, ktorá bude pripravená riešiť kybernetické bezpečnostné incidenty a vykonávať preventívne služby a reaktívne služby v rámci príslušného sektora alebo podsektora podľa prílohy č. 1 Zákona. Vzhľadom na skutočnosť, že zriadenie a prevádzka jednotky CSIRT je v zmysle Zákona viazaná výlučne na ústredný orgán podľa § 4 písm. b) Zákona [v zmysle Zákona žiaden iný orgán mimo § 4 písm. b) nemôže zriadiť a prevádzkovať jednotku CSIRT], v prípade, že ústredný orgán nemá zriadenú vlastnú jednotku CSIRT, je povinný zabezpečiť „pokrytie“ svojho sektora alebo podsektora inou akreditovanou jednotkou CSIRT iného ústredného orgánu, a to na základe osobitnej zmluvy podľa § 9 ods. 3 Zákona. Zákon súčasne predpokladá aj prípady, kedy nemusí k dohode dvoch ústredných orgánov o využívaní jednotky CSIRT dôjsť, pričom pre takéto prípady bude ex lege úlohy jednotky CSIRT pre daný „nepokrytý“ sektor alebo podsektor ústredného orgánu podľa prílohy č. 1 Zákona plniť Úrad prostredníctvom svojej národnej jednotky CSIRT. Možno konštatovať, že v čase vypracovania tohto komentára sú v SR už zriadené a v prevádzke dve akreditované jednotky CSIRT, a to národná jednotka CSIRT podľa § 6 Zákona v gescii Úradu a vládna jednotka CSIRT podľa § 11 Zákona v gescii Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu (bývalý CSIRT.SK v gescii Ministerstva financií Slovenskej republiky). Tieto dve jednotky CSIRT však neboli povinné prejsť akreditačným procesom v zmysle Zákona, lebo Zákon ich akreditáciu predpokladá automaticky, tzn. že obe uvedené jednotky CSIRT sú akreditované zo Zákona. Je však potrebné konštatovať, že obidve jednotky už v čase účinnosti Zákona spĺňali podmienky akreditácie podľa § 13 ods. 6 Zákona ich akreditáciou/členstvom v medzinárodných organizáciach FIRST a Trusted Introducer. Pokiaľ ide o jednotky CSIRT ostatných ústredných orgánov, ktoré nie sú v čase vypracovania tohto komentára akreditované, tieto budú musieť akreditáciu vykonávanú Úradom podstúpiť. Vlastnú jednotku CSIRT, aj keď v čase písania tohto komentára ešte Úradom neakreditovanú v zmysle § 13 Zákona, majú zriadenú Vojenské spravodajstvo (Centrum pre

kybernetickú obranu Slovenskej republiky – bývalý CSIRT.MIL Ministerstva obrany Slovenskej republiky) a Slovenská informačná služba.

Vo vzťahu k ústredným orgánom v zmysle § 4 písm. b) Zákona je potrebné poukázať na špecifické postavenie Vojenského spravodajstva pri vykonávaní pôsobnosti v oblasti kybernetickej bezpečnosti, ktoré podľa osobitného predpisu[4] plní špecifické úlohy na úseku kybernetickej obrany. Predovšetkým ide o prípady závažných kybernetických bezpečnostných incidentov podľa Zákona a týkajú sa obrany štátu, ktorú Vojenské spravodajstvo zabezpečuje prostredníctvom opatrení zameraných na riešenie týchto závažných kybernetických bezpečnostných incidentov, a to obrany objektov osobitnej dôležitosti, ďalších dôležitých objektov a prvkov kritickej infraštruktúry[5] pred kybernetickým napadnutím. Špecifickou povinnosťou Úradu vo vzťahu k Vojenskému spravodajstvu je aj povinnosť Úradu informovať Vojenské spravodajstvo, že závažný kybernetický bezpečnostný incident možno zaradiť do kategórie tretieho (III.) stupňa podľa vyhlášky č. 165/2018 Z. z. alebo ide o také skutočnosti, ktoré nasvedčujú tomu, že závažný kybernetický bezpečnostný incident môže byť kybernetickým terorizmom. Ako vyplýva aj zo samotného výpočtu ústredných orgánov podľa § 4 písm. b) Zákona, Vojenské spravodajstvo nie je možné zamieňať s Ministerstvom obrany Slovenskej republiky, pretože Ministerstvo obrany Slovenskej republiky má na základe prílohy č. 1 Zákona ako príslušný ústredný orgán vo svojej gescii podsektor „Obrana“, zatiaľ čo Vojenské spravodajstvo spolu so Slovenskou informačnou službou majú samostatný podsektor „Spravodajské služby“. V tejto súvislosti je však dôležité upozorniť na vymedzenie postavenia Vojenského spravodajstva ako spravodajskej služby, ktorá plní úlohy spravodajského zabezpečenia obrany, obranyschopnosti a bezpečnosti Slovenskej republiky v pôsobnosti Ministerstva obrany Slovenskej republiky, ako aj na taxatívny výpočet úloh Vojenského spravodajstva uvedených v § 2 zákona o VS.

K písm. b)

Jednou z požiadaviek Smernice NIS vo vzťahu k členským štátom povinným Smernicu NIS náležite transponovať do svojich vnútroštátnych právnych poriadkov bola aj požiadavka voči každému členskému štátu v zmysle čl. 7 Smernice NIS prijať národnú stratégiu v oblasti bezpečnosti sietí a informačných systémov. Smernica NIS okrem uvedenej požiadavky zároveň určuje, akým otázkam sa národná stratégia v oblasti bezpečnosti sietí a informačných systémov má venovať. Zákon uvedenú požiadavku v celom rozsahu preniesol do svojho § 7, kde národnú stratégiu v oblasti bezpečnosti sietí a informačných systémov premenoval na Národnú stratégiu kybernetickej bezpečnosti. Národnú stratégiu kybernetickej bezpečnosti má v zmysle § 5 ods. 1 písm. d) Zákona povinnosť vypracovať Úrad, oprávnenie schvaľovať Národnú stratégiu kybernetickej bezpečnosti bolo zverené do kompetencie Vlády Slovenskej republiky. Slovenská republika má na obdobie rokov 2015 – 2020 prijatú Koncepciu kybernetickej bezpečnosti SR, ktorá sa v spojení s jej akčným plánom môže považovať a zároveň akceptovať ako Národná stratégia kybernetickej bezpečnosti v zmysle Zákona. Z uvedeného dôvodu preto prijímanie novej Národnej stratégie kybernetickej bezpečnosti do roku 2020 nie je aktuálne a vzhľadom na naplnenosť úloh akčného plánu ku Koncepcii kybernetickej bezpečnosti SR ani reálne.

K písm. c)

JISKB je nový informačný systém upravený a zavedený Zákonom, ktorého správu a prevádzku zabezpečuje Úrad. JISKB tvorí komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálny systém včasného varovania. Účelom komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov

[4] Zákon o obrane

[5] § 2 písm. a) zákona o kritickej infraštruktúre

je najmä umožniť predkladanie informácií, údajov a hlásení Úradu podľa Zákona prostredníctvom na to určenej funkcionality (predovšetkým ide o hlásenie kybernetických bezpečnostných incidentov, zistenie prekročenia identifikačných kritérií prevádzkovanej služby PZS alebo oznámenie a preukázanie/preukazovanie vykonania reaktívneho opatrenia PZS alebo PDS).

Účelom centrálneho systému včasného varovania je najmä umožniť:

- zasielanie včasného varovania pred kybernetickými bezpečnostnými incidentmi jednotkou CSIRT;
- vyhlasovanie výstrah a varovaní Úradom pred závažným kybernetickým bezpečnostným incidentom.

JISKB tvorí verejná a neverejná časť. Úrad je povinný sprístupniť verejnú časť JISKB do 18 mesiacov odo dňa účinnosti Zákona (t. j. do 1. októbra 2019). Ďalšie podrobnosti JISKB stanovuje § 8 Zákona.

K písm. d)

Každý ústredný orgán podľa § 4 písm. b) Zákona je povinný, pretože má vo svojej gescii aspoň jeden zo sektorov alebo podsektorov podľa prílohy č. 1 Zákona, zriadiť si alebo na základe osobitnej zmluvy využívať akreditovanú jednotku CSIRT, ktorej primárnou úlohou je v rámci dotknutého sektora alebo podsektora v zmysle prílohy č. 1 Zákona riešiť kybernetické bezpečnostné incidenty a vykonávať preventívne služby a reaktívne služby v zmysle § 15 Zákona. Dôležitým poznávacím znakom každej jednotky CSIRT v zmysle Zákona je skutočnosť, že táto jednotka CSIRT je zriadená a prevádzkovaná výlučne niektorým z ústredných orgánov podľa § 4 písm. b) Zákona a súčasne musí byť Úradom akreditovaná a spĺňať podmienky akreditácie podľa § 14 Zákona. Z uvedeného teda vyplýva, že nie každý ERT („*Emergency Response Team*“), RRT („*Rapid Reaction Team*“), SOC („*Security Operation Centre*“), dokonca ani medzinárodne akreditovaný alebo certifikovaný CSIRT/CERT („*Computer Security Incident Response Team/Computer Emergency Response Team*“), pokiaľ nie je zriadený a prevádzkovaný príslušným ústredným orgánom v zmysle § 4 písm. b) Zákona, môže byť za jednotku CSIRT v zmysle Zákona považovaný. Na druhej strane je však potrebné dodať, že v zmysle vyhlášky NBÚ č. 166/2018 Z. z. platí: „jednotka CSIRT disponuje minimálnym počtom aspoň troch pracovníkov, ktorí zabezpečujú plnenie úloh jednotky CSIRT.“ Z uvedeného teda vyplýva, že jedinou povinnosťou vo vzťahu k personálnemu obsadeniu jednotky CSIRT z „vnútorných“ zdrojov je práve skôr citovaný § 5 ods. 3 tejto vyhlášky, pričom nie je vylúčené, aby ostatní pracovníci jednotky CSIRT nemohli byť v inom ako pracovnom pomere vo vzťahu k tejto jednotke CSIRT. Nie je teda možné jednoznačne vysloviť záver o výlučnom internom, teda štátnom personálnom obsadení jednotky CSIRT. Predmetom Zákona je nastavenie požiadaviek na minimálne personálne obsadenie jednotky CSIRT. Predmetom úpravy v Zákone však nie je právna forma vzťahu pracovníkov a jednotky CSIRT. Na tomto mieste je potrebné uviesť, že existujú aj názory, podľa ktorých personálne obsadenie jednotky CSIRT má mať formu interného pracovno-právneho vzťahu. Podľa autorov takýto názor nemá oporu v Zákone a vyhláške NBÚ č. 166/2018 Z. z. Akreditované jednotky CSIRT sa zároveň zaraďujú do zoznamu akreditovaných jednotiek CSIRT vedeného Úradom, ktorý je súčasťou verejnej časti JISKB.

V zmysle Zákona sú primárne zriadené dve jednotky CSIRT, jedna v pôsobnosti Úradu s označením národná jednotka CSIRT a druhá v pôsobnosti ÚPVII s označením vládna jednotka CSIRT. Aj keď § 6 Zákona vo vzťahu k národnej jednotke CSIRT používa v súvislosti s akreditáciou inú terminológiu („Národná jednotka CSIRT je zaradená v zozname akreditovaných jednotiek CSIRT.“) ako ustanovenie § 11 vo vzťahu k vládnej jednotke CSIRT („Vládna jednotka CSIRT sa zaraďuje do zoznamu akreditovaných jednotiek CSIRT.“), je

možné vysloviť záver o akreditácii oboch spomínaných jednotiek automaticky zo Zákona. To však obe uvedené jednotky nezbavuje ich povinnosti naďalej spĺňať podmienky akreditácie podľa § 14 Zákona počas celého životného cyklu jednotky CSIRT. Zároveň je potrebné poukázať na to, že Zákon je zároveň novelizačným predpisom k Zákonu o VS, ktorý okrem iného dopĺňa o § 4a týkajúci sa Centra pre kybernetickú obranu Slovenskej republiky ako osobitnú organizačnú zložku Vojenského spravodajstva. Aj keď predmetná organizačná zložka Vojenského spravodajstva existovala už pred účinnosťou Zákona, Zákon jej priradil konkrétny názov (Centrum pre kybernetickú obranu Slovenskej republiky) a zveril mu konkrétne úlohy a kompetencie vyplývajúce zo Zákonom doplneného Zákona o VS.

K písm. e)

Vzhľadom na skutočnosť, že prevažná väčšina povinností v zmysle Zákona je naviazaná na povinné osoby v zmysle Zákona, a to prevádzkovateľa základnej služby a poskytovateľa digitálnej služby, je pochopiteľné, že Zákon sa postavením a povinnosťami týchto povinných osôb zaoberá.

Postavenie prevádzkovateľa základnej služby upravuje ustanovenie § 3 písm. l) Zákona, obsahuje definíciu prevádzkovateľa základnej služby v spojení s definíciou pojmu základná služba v zmysle § 3 písm. k) Zákona. Podmienkou identifikácie konkrétneho prevádzkovateľa ako prevádzkovateľa základnej služby je prevádzka aspoň jednej základnej služby vymedzenej § 3 písm. k) Zákona. Aby však bolo možné o základnej službe v zmysle § 3 písm. k) hovoriť, je nevyhnutné, aby konkrétna služba naplnila identifikačné kritériá prevádzkovanej služby v zmysle § 18 Zákona, ktorými sa rozumejú dosahové kritériá podľa § 18 ods. 2 Zákona a špecifické sektorové kritériá podľa § 18 ods. 3 Zákona, obe určené vyhláškou NBÚ č. 164/2018 Z. z. Aj napriek tomu, že špecifické sektorové kritériá určuje v spolupráci s Úradom ústredný orgán podľa § 4 písm. b) Zákona, jediným subjektom splnomocneným na vydanie všeobecne záväzného predpisu identifikujúceho uvedené kritériá je samotný Úrad. Z uvedeného dôvodu je možné ustanovenie § 9 ods. 1 písm. e) v spojení s § 18 ods. 3 Zákona vnímať skôr ako povinnosť ústredného orgánu podľa § 4 písm. b) Zákona poskytnúť Úradu súčinnosť (spolupracovať) pri identifikácii špecifických sektorových kritérií. Až naplnením aspoň jedného dosahového kritéria a aspoň jedného špecifického sektorového kritéria podľa vyhlášky NBÚ č. 164/2018 Z. z. je možné konkrétnu službu považovať za základnú službu a jej prevádzkovateľa za prevádzkovateľa základnej služby. Prevádzkovateľovi základnej služby následne patria príslušné povinnosti podľa Zákona, najmä podľa § 17 až § 20, § 24 a § 27 Zákona. Prevádzkovateľa základnej služby Úrad zaradí do registra prevádzkovateľov základnej služby a jeho základnú službu, príp. základné služby (jeden prevádzkovateľ môže prevádzkovať aj viac ako jednu základnú službu) do zoznamu základných služieb.

Postavenie poskytovateľa digitálnej služby vyplýva z § 3 písm. n) Zákona, ktoré definuje poskytovateľa digitálnej služby v spojení s vymedzením pojmu digitálna služba v zmysle § 3 písm. m) Zákona. Primárnym predpokladom identifikácie konkrétneho poskytovateľa ako poskytovateľa digitálnej služby je, aby uvedený poskytovateľ poskytoval aspoň jednu digitálnu služby vymedzenú § 3 písm. m) Zákona, a teda aspoň jednu službu v zmysle prílohy č. 2 Zákona. Skutočnosť, že konkrétny poskytovateľ služieb je súčasne poskytovateľom aspoň jednej digitálnej služby podľa prílohy č. 2, automaticky nezakladá jeho status poskytovateľa základnej služby, lebo Zákon vo svojom § 3 písm. n) limituje potenciálny okruh poskytovateľov digitálnych služieb tým, že v zmysle Zákona musí poskytovateľ okrem poskytovania digitálnej služby zamestnávať aspoň 50 zamestnancov a mať ročný obrat alebo celkovú ročnú bilanciu viac ako 10 000 000 eur. Je vhodné poznamenať, že ročný obrat má byť odvodený od zverejnených celkových hospodárskych výsledkov subjektu, pretože v povinnom vykazovaní bilancie nebude možné odlíšiť, ktorá časť obratu, resp. bilancie sa

týkala výhradne digitálnej služby. Poskytovateľovi digitálnej služby následne patria príslušné povinnosti podľa Zákona, najmä podľa § 21, § 22, § 25 a § 27 Zákona. Poskytovateľ digitálnej služby je Úradom zaradený do registra poskytovateľov digitálnej služby a jeho digitálna služba, príp. digitálne služby (jeden poskytovateľ môže poskytovať aj viac ako jednu digitálnu službu) do zoznamu digitálnych služieb. Z uvedeného vyplýva, že zoznam digitálnych služieb nebude pozostávať výlučne zo zoznamu kategórií digitálnych služieb podľa prílohy č. 2 Zákona, ale v zozname budú uvedené konkrétne typy služieb s uvedením príslušnej kategórie podľa prílohy č. 2 Zákona.

K písm. f)

Bezpečnostné alebo ochranné opatrenia (z anglického: „measures" alebo „controls") – v kontexte Zákona sa tento výraz používa pre praktiky, postupy, procedúry a mechanizmy technického alebo procesného charakteru, ktoré môžu pomôcť znížiť známe zraniteľnosti, chrániť systém alebo organizáciu pred kybernetickými hrozbami. V prípade, že sa hrozba už uplatnila a spôsobila škodlivú udalosť, majú bezpečnostné opatrenia túto udalosť odhaliť a obmedziť jej vplyv. Následné bezpečnostné opatrenia majú umožniť zotavenie systému alebo organizácie zo škodlivej udalosti, resp. incidentu. Pojem opatrenia sa často používa aj v zmysle právneho konania, ktoré potenciálne zaručí odškodnenie strát vyvolaných škodlivou udalosťou.

Opatrenia sa rozdeľujú do dvoch skupín, a to do skupiny technických a skupiny organizačných opatrení. Technické opatrenia sú praktiky, postupy a mechanizmy na zníženie bezpečnostných rizík pomocou prostriedkov fyzickej a technologickej povahy. Technickými opatreniami sú zvyčajne bezpečnostné technológie, t. j. integrovaný súbor informačných a komunikačných technológií používaných na zvýšenie bezpečnosti a ochrany informačných a fyzických aktív. Komplexnosť bezpečnostných technológií, ich rýchly rozvoj a rozličný spôsob ich implementácie, ktorý je závislý od konkrétneho infraštruktúrneho prostredia a od konkrétnej architektúry, neumožňujú, aby na úrovni legislatívy boli technické opatrenia opísané detailnejším spôsobom. Nepísanou, avšak logickou požiadavkou je tiež udržanie platformovej nezávislosti odporúčaných technických opatrení.

Organizačné opatrenia sú zdokumentované praktiky, postupy a procesy na zníženie bezpečnostných rizík pomocou zmeny bezpečnostnej stratégie a cieľov, pomocou zmien procesov a úpravou návrhu podnikovej alebo aplikačnej architektúry. Špeciálnou podkategóriou organizačných opatrení sú bezpečnostné opatrenia týkajúce sa riadenia ľudských zdrojov a označujeme ich ako tzv. personálne opatrenia.

V Zákone sú bezpečnostné opatrenia bližšie opísané v ustanovení § 20.

K písm. g)

Systém je účelovo usporiadaný celok, množina predmetov, javov, dejov a poznatkov zložená z jednotlivých komponentov, medzi ktorými jestvujú presne vymedzené vzťahy a ktoré sledujú vopred určený cieľ. Vopred určeným cieľom Zákona je najmä zaviesť bezpečnostné požiadavky a požiadavky na hlásenie kybernetických bezpečnostných incidentov pre prevádzkovateľa základných služieb a pre poskytovateľa digitálnych služieb. Komponentmi takéhoto systému bezpečnostných požiadaviek sú jednotlivé bezpečnostné opatrenia. Bolo by nákladovo aj časovo neefektívne implementovať bezpečnostné opatrenia odťažito, bez vzájomných väzieb. Neefektívnosť by sa prejavila aj v praktickej účinnosti opatrení, čo by negatívne ovplyvnilo schopnosť povinných osôb zaručiť požadovanú úroveň kybernetickej bezpečnosti. Predísť tomu je možné tak, že o opatreniach (sledujúc vopred určený cieľ) sa bude rozhodovať vždy v kontexte kultúry konkrétnej organizácie, ako aj v kontexte dotknutého infraštruktúrneho prostredia a existujúcej architektúry prevádzkovateľa základných služieb alebo poskytovateľa digitálnych služieb. Spôsob

dokumentovania, preukazovania zhody vedie k integrácii viacerých individuálnych bezpečnostných opatrení do jedného integrovaného systému manažérstva. Riešením je teda oprieť sa o vhodný integrovaný manažérsky systém.

Pre informačnú bezpečnosť existuje rokmi vyskúšaný manažérsky systém, ktorý poznáme pod názvom Systém riadenia informačnej bezpečnosti (Information Security Management System), komplexne opísaný v triede medzinárodných noriem ISO/IEC 27000. Pod pojmom systém zabezpečenia kybernetickej bezpečnosti sa v Zákone chápe systém riadenia informačnej bezpečnosti so zameraním na bezpečnosť informácií v kybernetickom priestore.

K písm. h)

Zákon vo svojich ustanoveniach § 28 a § 29 podrobne upravuje kontrolu a audit, avšak komplexným spôsobom už neupravuje systém vykonávania kontroly podľa § 28, ale v súlade s legislatívnymi pravidlami vlády odkazuje na už existujúci systém výkonu kontroly podľa osobitného právneho predpisu, a to Zákona o kontrole (konkrétne ide o § 8 až § 13). Súčasne z § 28 Zákona vyplýva, že kontrolu nad dodržiavaním ustanovení Zákona je oprávnený vykonávať Úrad. Aj napriek skutočnosti, že Zákon neobsahuje explicitne vymedzené oprávnenie Úradu na výkon kontroly voči akémukoľvek subjektu v zmysle Zákona (Zákon sa zmieňuje len o výkone kontroly voči prevádzkovateľovi základnej služby a poskytovateľovi digitálnej služby), sme toho názoru, že v zmysle § 28 ods. 1 Zákona je Úrad oprávnený na výkon kontroly aj v ústrednom orgáne podľa § 4 písm. b) Zákona, v inom orgáne štátnej správy podľa § 4 písm. c) Zákona alebo v jednotke CSIRT, lebo v zmysle § 28 ods. 1 Zákona je kontrola zameraná na dodržiavanie ustanovení Zákona, čo znamená, že aj na dodržiavanie akéhokoľvek ustanovenia Zákona akýmkoľvek povinným subjektom v zmysle Zákona. Otáznym sa môže javiť uplatnenie známej básnickej otázky „Quis custodiet ipsos custodes?“ (Kto bude strážiť strážcov?), a teda, kto bude kontrolovať samotný Úrad, lebo aj tomu zo Zákona vyplývajú príslušné povinnosti. V zmysle § 72, § 73 a § 74 zákona o OUS je na účel kontroly činnosti Národného bezpečnostného úradu zriadený Osobitný kontrolný výbor NR SR na kontrolu činnosti NBÚ. Keďže ide o poslaneckú kontrolu, problematickou môže byť spôsobilosť členov kontrolného výboru (poslancov) posudzovať zákonnosť Úradu vo vzťahu k jeho postupom v zmysle Zákona.

Audit kybernetickej bezpečnosti v zmysle § 29 Zákona je osobitným druhom kontroly zameranej na pravidelne sa opakujúce preverovanie účinnosti prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených Zákonom u prevádzkovateľa základnej služby. Špecifikom auditu kybernetickej bezpečnosti je, že tento má povinnosť zabezpečiť sám prevádzkovateľ základnej služby prostredníctvom orgánu posudzovania zhody podľa osobitného predpisu[6] a v rozsahu stanovenom podľa všeobecne záväzného právneho predpisu, ktorý vydá Úrad podľa § 32 ods. 1 písm. f) Zákona. Súčasne § 29 Zákona stanovuje oprávnenie Úradu vykonať audit u prevádzkovateľa aj samostatne alebo prostredníctvom orgánu posudzovania zhody a upravuje otázky týkajúce sa úhrady nákladov spojených s auditom kybernetickej bezpečnosti u prevádzkovateľa základnej služby.

Z judikatúry

Rozsudok Najvyššieho súdu Slovenskej republiky č. k. 7Sž/139/01, podľa záverov ktorého: „Ak je zrejmé, že podkladom na vydanie rozhodnutia o uložení sankcie sú zistenia kontroly, ktorá

[6] Čl. 2 ods. 13 nariadenia Európskeho parlamentu a Rady (ES) č. 765/2008 z 9. júla 2008, ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v súvislosti s uvádzaním výrobkov na trh a ktorým sa zrušuje nariadenie (EHS) č. 339/93 (Ú. v. EÚ L 218, 13. 8. 2008).

bola vykonaná v rozpore so zákonom č. 10/1996 Z. z. o kontrole v štátnej správe, je to dôvodom, aby súd takéto rozhodnutie ako nezákonné zrušil.“

§ 2
Pôsobnosť zákona

(1) Tento zákon ustanovuje minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti.

(2) Tento zákon sa nevzťahuje na

a) požiadavky na zabezpečenie sietí a informačných systémov podľa všeobecného predpisu o ochrane utajovaných skutočností,

b) osobitné ustanovenia o úlohách a oprávneniach orgánu štátu pri ochrane kybernetického priestoru podľa osobitného predpisu,[1)]

c) ustanovenia osobitných predpisov o vyšetrovaní, odhaľovaní a stíhaní trestných činov,[2)]

d) požiadavky týkajúce sa bezpečnosti sietí, infraštruktúr a informačných systémov a oznamovania kybernetických bezpečnostných incidentov v sektore bankovníctva, financií alebo finančného systému podľa osobitných predpisov,[3)] vrátane štandardov a zásad vydaných alebo prijatých Európskou centrálnou bankou, Európskym systémom centrálnych bánk, Eurosystémom alebo európskymi orgánmi dohľadu,[4)] ak ich účinok je aspoň rovnocenný s účinkom povinností podľa tohto zákona, vrátane rozhodnutí, štandardov a zásad vydaných alebo prijatých Národnou bankou Slovenska, ak ich cieľom je dosiahnuť rovnocennú alebo vyššiu úroveň bezpečnosti sietí, infraštruktúr a informačných systémov ako podľa tohto zákona, a ani na platobné systémy a na systémy zúčtovania a vyrovnania cenných papierov a ich infraštruktúry dohliadané alebo prevádzkované Európskou centrálnou bankou alebo Eurosystémom podľa osobitných predpisov,[5)]

e) požiadavky na zabezpečenie sietí a informačných systémov v sektore podľa osobitného predpisu,[6)] ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov ako podľa tohto zákona,

f) osobitné predpisy.[7)]

Z dôvodovej správy

K § 2

Ustanovenie upravuje pôsobnosť zákona vo vzťahu k smernici NIS a národnej úprave zabezpečenia sietí a informačných systémov.

V odseku 1 sa vymedzuje cieľ zákona, ktorým je najmä stanoviť minimálne požiadavky na štandardné zabezpečenie významných informačných systémov v Slovenskej republike. V členských štátoch je totiž rôzna úroveň pripravenosti na zabezpečenie kybernetickej bezpečnosti, čo vedie k fragmentácii prístupov v Európskej únii. To má za následok rozdielnu úroveň ochrany spotrebiteľov a podnikov a narúša celkovú úroveň bezpečnosti sietí a informačných systémov v rámci Únie. Neexistencia spoločných požiadaviek na prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb zase znemožňuje, aby sa na úrovni Únie vytvoril globálny a účinný mechanizmus spolupráce. Minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti v tomto zákone nebránia prevádzkovateľom základných služieb a poskytovateľom digitálnych služieb uplatňovať prísnejšie bezpečnostné opatrenia.

V odseku 2 sa vymedzuje negatívnym spôsobom vecná pôsobnosť. Špecifické obmedzenia pôsobnosti sa vzťahujú na siete a informačné systémy, ktoré spracúvajú utajované skutočnosti. Dôvodom je, že tieto systémy sú regulované osobitným predpisom, ktorým je zákon

č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v platnom znení.

Negatívne vymedzenie ďalej definuje, že ak osobitný právny predpis obsahuje ustanovenia na zabezpečenie sietí a informačných systémov, ktoré vychádzajú z rovnakých základov ako požiadavky na zabezpečenie kybernetickej bezpečnosti upravené v tomto zákone, použijú sa na zabezpečenie kybernetickej bezpečnosti osobitné predpisy. Ide napríklad o príslušné ustanovenia zákona č. 492/2009 Z. z. o platobných službách, zákon č. 541/2004 Z. z. o mierovom využívaní jadrovej energie, zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy. Zákon o kybernetickej bezpečnosti sa ďalej nevzťahuje na zákon č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov, nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (Ú. v. EÚ L257, 28. 8. 2014), zákon Národnej rady Slovenskej republiky č. 46/1993 Z. z. o Slovenskej informačnej službe v znení neskorších predpisov, zákon Národnej rady Slovenskej republiky č. 198/1994 Z. z. o Vojenskom spravodajstve v znení neskorších predpisov.

Ustanovenia tohto zákona sa z povahy jeho predmetu úpravy nevzťahujú na činnosti Slovenskej informačnej služby a Ministerstva obrany Slovenskej republiky pri aktivitách a ohrozeniach v kybernetickom priestore, ak ohrozujú bezpečnosť štátu (kybernetická obrana).

Smernicou NIS nie sú dotknuté opatrenia prijímané členskými štátmi na zabezpečenie ich základných štátnych funkcií, najmä na zabezpečenie národnej bezpečnosti vrátane opatrení na ochranu informácií, ktorých sprístupnenie členské štáty považujú za odporujúce základným záujmom ich bezpečnosti, a na udržanie verejného poriadku, najmä na účely umožnenia vyšetrovania, odhaľovania a stíhania trestných činov.

Súvisiace ustanovenia

- § 20

Súvisiace predpisy

- § 2 ods. 1 písm. g), ods. 3 Zákona o SIS
- § 2 ods. 1 písm. c) a h), ods. 2 a § 4a Zákona o VS
- Zákon o obrane
- Zákon č. 398/2015 Z. z. o európskom ochrannom príkaze v trestných veciach a o zmene a doplnení niektorých zákonov
- Zákon č. 91/2016 Z. z. o trestnej zodpovednosti právnických osôb a o zmene a doplnení niektorých zákonov v platnom znení
- § 28c, § 28d, § 45 ods. 8 a § 64 ods. 4 zákona č. 492/2009 Z. z. o platobných službách a o zmene a doplnení niektorých zákonov
- Nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 zo 4. júla 2012 o mimoburzových derivátoch, centrálnych protistranách a archívoch obchodných údajov (Ú. v. EÚ L 201, 27. 7. 2012) v platnom znení
- § 14 zákona č. 429/2002 Z. z. o burze cenných papierov v platnom znení
- Delegované nariadenie Komisie (EÚ) 2017/584 zo 14. júla 2016, ktorým sa dopĺňa smernica Európskeho parlamentu a Rady 2014/65/EÚ, pokiaľ ide o regulačné technické predpisy bližšie určujúce organizačné požiadavky na obchodné miesta (Ú. v. EÚ L 87, 31. 3. 2017)
- Čl. 127 ods. 2 Zmluvy o fungovaní EÚ
- Čl. 12 ods. 12.1, čl. 22 Protokolu (č. 4) o Štatúte Európskeho systému centrálnych bánk a Európskej centrálnej banky v platnom znení (Ú. v. EÚ C 202, 7. 6. 2016)

- § 2 Zákona o NBS
- § 2 ods. 9 zákona č. 747/2004 Z. z. o dohľade nad finančným trhom a o zmene a doplnení niektorých zákonov v znení zákona č. 132/2013 Z. z.
- Čl. 3 ods. 3.1, čl. 22 Protokolu (č. 4) o Štatúte Európskeho systému centrálnych bánk a Európskej centrálnej banky v platnom znení (Ú. v. EÚ C 202, 7. 6. 2016)
- Nariadenie Európskej centrálnej banky (EÚ) č. 795/2014 z 3. júla 2014 o požiadavkách v oblasti dohľadu nad systémovo dôležitými platobnými systémami (Ú. v. EÚ L 217, 23. 7. 2014)
- Zákon č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov v platnom znení
- Zákon o ISVS
- Nariadenie eIDAS
- Zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) v platnom znení
- Zákon o elektronických komunikáciách

Transpozičné ustanovenia

- Čl. 1 ods. 1, 3, 4, 6 a 7 Smernice NIS

Komentár k § 2

K odseku 1

Zákon vo svojom § 20, ako aj vo vykonávacích predpisoch [najmä vo vyhláške vydanej podľa § 32 ods. 1 písm. c) Zákona] ustanovuje minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti, ktoré bude musieť každá povinná osoba v zmysle Zákona dodržiavať, a to bez ohľadu na jej konkrétne špecifiká, prevádzkové prostredie či potreby. Aj keď Zákon vo svojom § 20 uvádza len oblasti, pre ktoré sa majú bezpečnostné opatrenia podľa § 20 ods. 1 Zákona prijať (všeobecné a sektorové bezpečnostné opatrenia), vyhláška NBÚ č. 362/2018 Z. z. okrem iného obsahuje už exaktný výpočet konkrétnych bezpečnostných opatrení pre tú-ktorú oblasť identifikovanú § 20 ods. 3 Zákona. Uvedené opatrenia budú prevádzkovatelia základných služieb povinne a bez obmedzenia implementovať, pokiaľ nie je daná niektorá z výnimiek pôsobnosti samotného Zákona uvedená v § 2 ods. 2 Zákona.

K odseku 2

Účelom § 2 ods. 2 je vymedziť a súčasne obmedziť pôsobnosť Zákona (či už úplne, alebo v konkrétnom rozsahu) vo vzťahu ku konkrétnym oblastiam, sektorom, osobitným predpisom a pod. Ustanovenie § 2 ods. 2 Zákona teda vo svojich písm. a) až f) vyčerpávajúcim spôsobom negatívne vymedzuje tie oblasti, na ktoré sa pôsobnosť Zákona v konkrétne určenom rozsahu v zmysle príslušného písmena k § 2 ods. 2 Zákona nevzťahuje. Uvedený prístup zákonodarcu je prístup, ktorý prevzal zo Smernice NIS, ktorej požiadavkou v zmysle čl. 1 ods. 7 je: „*Ak sa podľa právneho aktu Únie špecifického pre určité odvetvie vyžaduje, aby prevádzkovatelia základných služieb alebo poskytovatelia digitálnych služieb buď zaisťovali bezpečnosť ich sietí a informačných systémov, alebo aby oznamovali incidenty, uplatňujú sa ustanovenia tohto právneho aktu Únie špecifického pre určité odvetvie pod podmienkou, že tieto požiadavky majú aspoň rovnocenný účinok ako povinnosti stanovené v tejto smernici.*“

Na základe uvedeného však chceme upozorniť na časté dezinterpretácie § 2 ods. 2 Zákona v tom zmysle, že pri uplatnení niektorej z výnimiek predpokladaných konkrétnym písmenom ustanovenia § 2 ods. 2 Zákona pôsobnosť Zákona nie je daná vôbec. Uvedené nie je pravdou, lebo § 2 ods. 2 v niektorých príslušných písmenách [najmä a), d) a e)] súčasne stanovuje aj rozsah vylúčenia pôsobnosti Zákona, ktorý v označených prípadoch nie je absolútny. Uvedené platí aj v zmysle zmeny a doplnenia § 2 ods. 2 písm. d) Zákona prostredníctvom zákona, ktorým sa mení a dopĺňa zákon č. 371/2014 Z. z. o riešení krízových situácií na finančnom trhu a o zmene a doplnení niektorých zákonov.[7] Uvedenou zmenou sme sa zaoberali v komentári k § 2 ods. 2 písm. d) Zákona.

Nepresnosťou trpí aj samotná dôvodová správa k Zákonu, ktorá napr. vo vzťahu k zákonu č. 541/2004 Z. z. o mierovom využívaní jadrovej energie uvádza nasledovné: „*Negatívne vymedzenie ďalej definuje, že ak osobitný právny predpis obsahuje ustanovenia na zabezpečenie sietí a informačných systémov, ktoré vychádzajú z rovnakých základov ako požiadavky na zabezpečenie kybernetickej bezpečnosti upravené v tomto zákone, použijú sa na zabezpečenie kybernetickej bezpečnosti osobitné predpisy. Ide napríklad o príslušné ustanovenia zákona č. 492/2009 Z. z. o platobných službách, zákona č. 541/2004 Z. z. o mierovom využívaní jadrovej energie…*“ S uvedeným nie je možné sa stotožniť, lebo § 2 ods. 2 písm. e) Zákona je jednoznačný v tom, že na uplatnenie výnimky z pôsobnosti Zákona sa vyžaduje, aby osobitný predpis (v tomto konkrétnom prípade aj zákon č. 541/2004 Z. z. o mierovom využívaní jadrovej energie) stanovoval také požiadavky na bezpečnosť sietí a informačných systémov, ktorých cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov, zatiaľ čo základy, z ktorých majú tie-ktoré požiadavky vychádzať, sú irelevantné. V opačnom prípade by na uplatnenie výnimky postačovala identifikácia ustanovení osobitného predpisu na zabezpečenie sietí a informačných systémov, ktoré vychádzajú z rovnakých základov ako požiadavky na zabezpečenie kybernetickej bezpečnosti v zmysle Zákona bez posúdenia zamýšľanej úrovne bezpečnosti týchto ustanovení alebo požiadaviek. S takýmto názorom však nemožno súhlasiť.

Ak v zmysle ustanovenia § 2 ods. 2 písm. d) Zákona má byť účinok požiadaviek týkajúcich sa bezpečnosti sietí, infraštruktúr a informačných systémov „aspoň rovnocenný s účinkom povinností podľa Zákona“, implicitne z toho vyplýva nutnosť posúdiť tento účinok. Samotná deklarácia existencie akýchkoľvek iných požiadaviek vyplývajúcich prípadne z osobitných predpisov nie je dostatočná na posúdenie účinku ani porovnania, či tento účinok je alebo nie je rovnocenný s účinkom povinností podľa Zákona. Inou alternatívou by bolo nahradiť takéto posúdenie právne relevantným rozhodnutím príslušnej autority.

K odseku 2 písm. a)

Prvá výnimka sa týka zabezpečenia sietí a informačných systémov podľa zákona o OUS. Citovaný zákon síce nepozná pojem sieť a informačný systém v zmysle chápania Zákona, dá sa však vyvodiť, že výnimka sa týka tých sietí a informačných systémov, v ktorých sa vytvárajú, spracúvajú, prenášajú, ukladajú alebo chránia utajované skutočnosti, a teda informácie alebo veci určené pôvodcom utajovanej skutočnosti, ktoré vzhľadom na záujem Slovenskej republiky treba chrániť pred vyzradením, zneužitím, poškodením, neoprávneným rozmnožením, zničením, stratou alebo odcudzením a ktorá môže vznikať len v oblastiach, ktoré ustanoví vláda Slovenskej republiky svojím nariadením. Dôvodom, prečo Zákon uvedenú výnimku do svojho § 2 ods. 2 písm. a) zakomponoval, je skutočnosť, že zákon o ochrane utajovaných skutočností v spojení s jeho vykonávacími právnymi predpismi komplexne ustanovuje osobitné požiadavky na zaistenie bezpečnosti utajovaných skutočností (napr. bezpečnosti v rámci technických prostriedkov – zariadení alebo systémov

[7] Legislatívny proces č. LP/2018/517

určených na vytváranie, spracúvanie, prenos, ukladanie a ochranu utajovaných skutočností, ako ich vo všeobecnosti poníma zákon o ochrane utajovaných skutočností) v oblastiach personálnej, administratívnej, fyzickej a objektovej bezpečnosti, bezpečnosti technických prostriedkov a šifrovej ochrany informácií. Osobitne však upozorňujeme na skutočnosť, že aj napriek tomu, že pôsobnosť Zákona v rozsahu jeho požiadaviek na zabezpečenie sietí a informačných systémov podľa zákona o ochrane utajovaných skutočností nie je daná, ostatné povinnosti v zmysle Zákona (napr. povinnosť identifikácie prevádzkovateľa základnej služby alebo povinnosť hlásenia kybernetických bezpečnostných incidentov) sú naďalej platné. Napokon, prevádzkovateľ základnej služby v rámci prílohy č. 1 Zákona, podsektor „Utajované skutočnosti", je daný, a to správca a prevádzkovateľ sietí a informačných systémov, ktoré sa týkajú utajovaných skutočností, pričom zastávame názor, že na tohto prevádzkovateľa základnej služby sa vzťahujú všetky povinnosti v zmysle Zákona, s výnimkou povinností vo vzťahu k požiadavkám na zabezpečenie sietí a informačných systémov utajovaných skutočností (§ 20 Zákona v spojení s vyhláškou č. 362/2018 Z. z.).

K odseku 2 písm. b)

Uvedená výnimka sa v zásade týka troch typov subjektov, ktoré plnia príslušné úlohy a majú svoje osobitné oprávnenia pri ochrane (pozn. autorov „aj obrane") kybernetického priestoru podľa osobitného predpisu,[8] a to Slovenská informačná služba, Vojenské spravodajstvo a ozbrojené sily, ktorými sa, okrem (už menovaných) spravodajských služieb, rozumejú súdy, prokuratúra, ozbrojené zbory (napr. Policajný zbor, Zbor väzenskej a justičnej stráže) a Ozbrojené sily Slovenskej republiky.

Slovenská informačná služba v zmysle svojich oprávnení podľa osobitného predpisu[8] získava, sústreďuje a vyhodnocuje informácie o aktivitách a ohrozeniach v kybernetickom priestore, ak ohrozujú bezpečnosť štátu a súčasne, ak je to potrebné na zabránenie aktivitám podľa § 2 ods. 1 a 2 tohto osobitného zákona (napr. aktivity a ohrozenia v kybernetickom priestore) a na realizáciu zahraničnopolitických záujmov Slovenskej republiky. Slovenská informačná služba vykonáva primerané bezpečnostné opatrenia. Z uvedeného teda vyplýva, že Slovenská informačná služba ako orgán štátu s osobitnými úlohami a oprávneniami pri ochrane kybernetického priestoru je pri plnení týchto úloh alebo výkone týchto oprávnení vyňatá z pôsobnosti Zákona. Zákon sa teda na plnenie osobitných úloh a výkon oprávnení Slovenskej informačnej služby podľa predchádzajúcej vety nevzťahuje.

Vojenské spravodajstvo v zmysle svojich oprávnení podľa osobitného predpisu[8] získava, sústreďuje a vyhodnocuje informácie dôležité pre zabezpečenie obrany a obranyschopnosti Slovenskej republiky na území Slovenskej republiky a v zahraničí zamerané na terorizmus, jeho financovanie alebo podporovanie, na kybernetický terorizmus, vlastizradu, sabotáž a záškodníctvo, ako aj na aktivity a ohrozenia v kybernetickom priestore. Rovnako ako v prípade Slovenskej informačnej služby, tak aj u Vojenského spravodajstva platí, že ak je to potrebné na zabránenie aktivitám a ohrozeniam podľa § 2 ods. 1 tohto osobitného zákona (napr. aktivity a ohrozenia v kybernetickom priestore), Vojenské spravodajstvo vykonáva primerané bezpečnostné opatrenia. Z uvedeného teda vyplýva, že aj Vojenské spravodajstvo, obdobne ako Slovenská informačná služba ako orgán štátu s osobitnými úlohami a oprávneniami pri ochrane (obrane) kybernetického priestoru, je pri plnení týchto úloh alebo výkone týchto oprávnení vyňaté z pôsobnosti Zákona; to znamená, že Zákon sa naň nevzťahuje.

Ozbrojené sily (v zmysle ich obsahového vymedzenia podľa § 2 ods. 3 osobitného zákona[8] v zmysle svojich oprávnení podľa tohto osobitného predpisu[8] zabezpečujú obranu Slovenskej republiky (vrátane kybernetického priestoru) prostredníctvom opatrení

[8] § 2 ods. 1 písm. g), ods. 3 Zákona o SIS; § 2 ods. 1 písm. c) a h), ods. 2 a § 4a Zákona o VS; Zákon o obrane.

zameraných v zmysle Zákona na riešenie závažných kybernetických bezpečnostných incidentov a obranu objektov osobitnej dôležitosti, ďalších dôležitých objektov a prvkov kritickej infraštruktúry pred kybernetickým napadnutím. Aj napriek skutočnosti, že obrana Slovenskej republiky podľa predchádzajúcej vety sa zabezpečuje práve Vojenským spravodajstvom, je potrebné konštatovať, že vzhľadom na skutočnosť, že systém obrany štátu tvorí súhrn prvkov a opatrení štátu, prostredníctvom ktorých sa uskutočňuje zabezpečenie obrany štátu a plnenie záväzkov vyplývajúcich z medzinárodných zmlúv o spoločnej obrane proti napadnutiu a z ďalších medzinárodných zmlúv, ktorými je Slovenská republika viazaná, je možné do výnimky podľa § 2 ods. 2 písm. b) Zákona subsumovať aj ozbrojené sily, ktoré v čase vojny alebo vojnového stavu zabezpečujú riadenie obrany Slovenskej republiky, ktorej súčasťou je aj riadenie obrany kybernetického priestoru ako piatej operačnej domény v zmysle záverov zo summitu NATO vo Varšave konaného v dňoch 8. až 9. júla 2016. Na plnenie úloh obrany štátu ozbrojenými silami tak pôsobnosť Zákona nie je daná, a to najmä z dôvodu, že Zákon je právnym predpisom koncipovaným pre stav mieru, zatiaľ čo obrana štátu je zameraná na stavy odlišné od stavu mieru (najmä vojnového stavu a vojny), kedy nielen úlohy riadenia obrany štátu, ale riadenie štátu ako také preberajú ozbrojené sily (v zmysle kontingenčného plánu prechodu zodpovedností za riadenie štátu, ktorý mal byť v termíne 12/2017 vypracovaný v súlade s úlohou bodu 1.8 akčného plánu). Zároveň je potrebné si uvedomiť, že v prípade vyhlásenia vojnového stavu, príp. stavu vojny by sa Zákon neuplatňoval vôbec. Slovenská republika ako subjekt medzinárodného práva by postupovala v zmysle všeobecne platných zásad práva ozbrojeného konfliktu a uplatňovali by sa zákony platné pre daný stav, v ktorom sa Slovenská republika nachádza (napr. v čase vojny, vojnového stavu, výnimočného stavu alebo núdzového stavu by sa uplatňoval osobitný predpis[9]).

K odseku 2 písm. c)

Pôsobnosť Zákona nie je daná ani vo vzťahu k ustanoveniam osobitných predpisov týkajúcich sa vyšetrovania, odhaľovania a stíhania trestných činov, a to predovšetkým na vyšetrovanie, odhaľovanie a stíhanie trestných činov podľa zákona č. 398/2015 Z. z. o európskom ochrannom príkaze v trestných veciach a o zmene a doplnení niektorých zákonov, zákona č. 91/2016 Z. z. o trestnej zodpovednosti právnických osôb a o zmene a doplnení niektorých zákonov v platnom znení, ako aj podľa ďalších osobitných predpisov týkajúcich sa vyšetrovania, odhaľovania a stíhania trestných činov. Nepochybne sa to týka aj vyšetrovania, odhaľovania a stíhania trestných činov v zmysle Trestného zákona v spojení s Trestným poriadkom, zákona č. 154/2010 Z. z. o európskom zatýkacom rozkaze alebo zákona č. 236/2017 Z. z. o európskom vyšetrovacom príkaze v trestných veciach a o zmene a doplnení niektorých zákonov. Z uvedeného teda vyplýva, že popri ustanoveniach osobitných predpisov týkajúcich sa ochrany kybernetického priestoru a obrany kybernetického priestoru sú to rovnako aj ustanovenia vo vzťahu ku kriminalite, jej vyšetrovaniu, odhaľovaniu a stíhaniu, pričom nemusí ísť nevyhnutne len o počítačovú kriminalitu.

Pojem počítačová kriminalita v slovenskom práve nie je explicitne definovaný. Jednotná, záväzná definícia tohto pojmu sa nenachádza v žiadnom zákone či zmluve, ktorú by bola Slovenská republika viazaná dodržiavať. Pre účely trestného práva sa na Slovensku používajú odkazy na definície v Dohovore rady Európy o počítačovej kriminalite z roku 2007. Slovenská republika v rámci Dohovoru využíva možnosť podmieniť trestnosť nezákonného prístupu tým, že musí byť spáchaný porušením bezpečnostných opatrení s úmyslom získať počítačové údaje alebo s iným nečestným úmyslom, alebo vo vzťahu k počítačovému systému prepojenému s iným počítačovým systémom. Podľa platného Trestného zákona sú určené niektoré skutkové podstaty jednotlivých trestných činov, ktoré spoločne možno

[9] Zákon o bezpečnosti štátu

zahrnúť pod pojem počítačová kriminalita. V prenesenom význame by bolo možné pod pojem počítačová kriminalita zahrnúť aj trestné činy spáchané prostredníctvom počítačového systému.

K odseku 2 písm. d)

Opätovne je potrebné poukázať na výnimku v ustanovení § 2 písm. d), ktorá predstavuje často pertraktované plošné neuplatňovanie Zákona vo vzťahu k sieťam a informačným systémom a oznamovaniu kybernetických bezpečnostných incidentov v sektore bankovníctva, financií alebo finančného systému.

Je potrebné znovu zdôrazniť, že výnimka z pôsobnosti Zákona je daná len vo vzťahu k požiadavkám týkajúcim sa opatrení určených na zaručenie bezpečnosti sietí a informačných systémov v tomto sektore a oznamovania kybernetických bezpečnostných incidentov. Úmyselne ukončujeme vetu predčasne, aby sme mohli upozorniť na to, že vo zvyšných povinnostiach vyplývajúcich zo Zákona (napr. identifikácia prevádzkovateľa základnej služby) sa Zákon uplatní aj vo vzťahu k sektoru bankovníctva, financií alebo finančného systému, teda je daná jeho pôsobnosť, lebo napr. povinnosť identifikácie prevádzkovateľa základnej služby nie je možné považovať ani za požiadavku týkajúcu sa bezpečnosti sietí a informačných systémov v menovanom sektore a ani za požiadavku na oznamovanie kybernetických bezpečnostných incidentov. Pokiaľ by sme teda výklad zamerali na úmyselne predčasne ukončenú vetu „Tento zákon sa nevzťahuje na požiadavky týkajúce sa bezpečnosti sietí a informačných systémov a oznamovania kybernetických bezpečnostných incidentov v sektore bankovníctva, financií alebo finančného systému podľa osobitných predpisov.“, nie je podľa nášho názoru možné jednoducho vyvodiť záver o plošnom neuplatnení ustanovení Zákona vo vzťahu k menovaného sektoru, lebo Zákon, s výnimkou požiadaviek týkajúcich sa opatrení majúcich za cieľ zaistiť bezpečnosť sietí a informačných systémov a požiadavky oznamovania kybernetických bezpečnostných incidentov, obsahuje aj ďalšie požiadavky zodpovedajúce uloženým povinnostiam konkrétnych, vybraných subjektov.

Pokiaľ sa predmetnou vetou budeme zaoberať ďalej a do výkladu začleníme aj časť „vrátane štandardov a zásad vydaných alebo prijatých Európskou centrálnou bankou, Európskym systémom centrálnych bánk, Eurosystémom alebo európskymi orgánmi dohľadu, ak ich účinok je aspoň rovnocenný s účinkom povinností podľa tohto zákona“, je možné vysloviť záver, že Zákonom nie sú dotknuté len požiadavky týkajúce sa bezpečnosti sietí a informačných systémov a požiadavky oznamovania kybernetických bezpečnostných incidentov podľa osobitného predpisu[10], ale aj požiadavky týkajúce sa bezpečnosti sietí a informačných systémov a požiadavky oznamovania kybernetických bezpečnostných incidentov v zmysle štandardov a zásad vydaných alebo prijatých Európskou centrálnou bankou, Európskym systémom centrálnych bánk, Eurosystémom alebo európskymi orgánmi dohľadu. Uvedené doplnenie nám však nezúžilo už predtým dané vylúčenie pôsobnosti Zákona na požiadavky týkajúce sa bezpečnosti sietí a informačných systémov a požiadavky oznamovania kybernetických bezpečnostných incidentov. Zúžilo len zoznam prípadných požiadaviek uplatňujúcich sa na sektor bankovníctva, financií alebo finančného systému,

[10] Napríklad § 28c, § 28d, § 45 ods. 8 *a* § 64 ods. 4 zákona č. 492/2009 Z. z. *o platobných službách a o zmene a doplnení niektorých zákonov, nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 zo 4. júla 2012 o mimoburzových derivátoch, centrálnych protistranách a archívoch obchodných údajov (Ú. v. EÚ L 201, 27. 7. 2012) v platnom znení,* § 14 zákona č. 429/2002 Z. z. *o burze cenných papierov v platnom znení, delegované nariadenie Komisie (EÚ) 2017/584 zo 14. júla 2016, ktorým sa dopĺňa smernica Európskeho parlamentu a Rady 2014/65/EÚ, pokiaľ ide o regulačné technické predpisy bližšie určujúce organizačné požiadavky na obchodné miesta (Ú. v. EÚ L 87, 31. 3. 2017).*

a to popri tých, ktoré vyplývajú z osobitného predpisu[10] a rozšírilo ich aj na požiadavky vyplývajúce zo štandardov a zásad vydaných alebo prijatých Európskou centrálnou bankou, Európskym systémom centrálnych bánk, Eurosystémom alebo európskymi orgánmi dohľadu. Zákon však zároveň aplikovateľnosť požiadaviek v zmysle skôr citovaných osobitných predpisov alebo iných „zdrojov" zužuje na tie, ktorých účinok je aspoň rovnocenný s účinkom povinností podľa Zákona. V zmysle uvedeného chceme vyjadriť názor, že prípadná aplikácia výnimky z pôsobnosti Zákona vyžaduje posúdenie účinkov požiadaviek na bezpečnosť sietí a informačných systémov a oznamovanie kybernetických bezpečnostných incidentov v zmysle Zákona a v zmysle osobitného predpisu[10]. Pri posudzovaní účinkov je potrebné zohľadňovať aj účinky vyplývajúce zo štandardov a zásad vydaných alebo prijatých Európskou centrálnou bankou, Európskym systémom centrálnych bánk, Eurosystémom alebo európskymi orgánmi dohľadu vo vzťahu k požiadavkám na bezpečnosť sietí a informačných systémov v sektore bankovníctva, financií alebo finančného systému a oznamovanie kybernetických bezpečnostných incidentov v tomto sektore. Pokiaľ si predmetné ustanovenie dočítame ako celok, a teda doplníme aj o časť „vrátane rozhodnutí, štandardov a zásad vydaných alebo prijatých Národnou bankou Slovenska, ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov ako podľa tohto zákona", opätovne musíme konštatovať, že tak ako v prípade štandardov a zásad vydaných alebo prijatých Európskou centrálnou bankou, Európskym systémom centrálnych bánk, Eurosystémom alebo európskymi orgánmi dohľadu, tak aj v prípade štandardov a zásad vydaných alebo prijatých Národnou bankou Slovenska nedochádza k rozšíreniu pôvodne vylúčenej pôsobnosti Zákona, čo sa jeho špecifických požiadaviek týka, ale len k rozšíreniu zdroja požiadaviek o tie, ktoré vyplývajú zo štandardov a zásad vydaných alebo prijatých Národnou bankou Slovenska. V zmysle súčasného znenia Zákona platí, že cieľom požiadaviek vydaných alebo prijatých Národnou bankou Slovenska musí byť dosiahnutie vyššej (nie rovnocennej) úrovne bezpečnosti sietí a informačných systémov, ako to stanovuje Zákon. Vo vzťahu k Národnej banke Slovenska je možné z textu explicitne vyvodiť, že výluka sa týka len požiadaviek týkajúcich sa vyššej úrovne bezpečnosti sietí a informačných systémov. Súčasne je však potrebné dodať, že v zmysle návrhu zákona, ktorým sa mení a dopĺňa zákon č. 371/2014 Z. z. o riešení krízových situácií na finančnom trhu a o zmene a doplnení niektorých zákonov, ktorý je v čase písania tohto komentára v legislatívnom procese, má dôjsť k doplneniu slovného spojenia „vyššiu úroveň bezpečnosti sietí a informačných systémov" slovom „rovnocennú". Po vyhlásení uvedeného znenia v Zbierke zákonov by tak požiadavka na Národnú banku Slovenska v zmysle § 2 ods. 2 písm. d) Zákona bola znížená v tom zmysle, že na aplikáciu vylúčenia pôsobnosti Zákona v rozsahu podľa § 2 ods. 2 písm. d) Zákona by postačovala „rovnocenná alebo vyššia úroveň bezpečnosti sietí a informačných systémov". Uvedené však nič nemení na záveroch vyslovených vyššie, a teda, že o prípadnom vylúčení Zákona v zmysle § 2 ods. 2 písm. d) Zákona v sektore bankovníctva, financií alebo finančného systému podľa osobitného predpisu10 je možné hovoriť len vtedy, pokiaľ je daná aspoň rovnocennosť účinkov požiadaviek týkajúcich sa bezpečnosti sietí a informačných systémov a oznamovania kybernetických bezpečnostných incidentov. V opačnom prípade, pokiaľ uvedená rovnocennosť daná nie je, v sektore bankovníctva, financií alebo finančného systému podľa osobitného predpisu10 sa uplatnia všetky požiadavky Zákona týkajúce sa bezpečnosti sietí a informačných systémov a oznamovania kybernetických bezpečnostných incidentov.

Poslednou časťou, ktorá podľa všetkého spôsobuje najväčšie komplikácie pri jej výklade a ktorá je zrejme príčinou často prezentovaného názoru vyňatí pôsobnosti Zákona ako celku vo vzťahu k sieťam a informačným systémom v sektore bankovníctva, financií alebo finančného systému bez rozlíšenia horeuvedených špecifík, je časť v znení *„a ani na platobné systémy a na systémy zúčtovania cenných papierov dohliadané alebo prevádzkované*

Európskou centrálnou bankou alebo Eurosystémom podľa osobitných predpisov[11]“. Až v tomto kontexte, a to vzhľadom na prepojenie úvodnej časti vety *„a ani na“* v spojení s textovým úvodom § 2 ods. 2 Zákona *„Tento zákon sa nevzťahuje na“*, je možné vyvodiť záver o celkovom vyňatí pôsobnosti Zákona vo vzťahu k platobným systémom a systémom zúčtovania cenných papierov dohliadaných alebo prevádzkovaných Európskou centrálnou bankou alebo Eurosystémom.

Ustanovenie § 2 ods. 2 písm. d) Zákona sa odkazuje na osobitné predpisy, napríklad na zákon č. 492/2009 Z. z. o platobných službách. Ak by mala byť splnená podmienka, že sa podľa právneho aktu špecifického pre určité odvetvie vyžaduje, aby prevádzkovatelia základných služieb alebo poskytovatelia digitálnych služieb zaisťovali bezpečnosť ich sietí a informačných systémov, dalo by sa logicky očakávať, že tieto osobitné predpisy v príslušných ustanoveniach určujú odvetvovo špecifické požiadavky týkajúce sa bezpečnosti sietí, infraštruktúry a informačných systémov v sektore bankovníctva, financií alebo finančného systému. To však taktiež nie je pravdou. Zákon č. 492/2009 Z. z. o platobných službách stanovuje v § 28c ods. 1 iba všeobecnú požiadavku, aby poskytovateľ platobných služieb určil rámec s vhodnými opatreniami na zmiernenie prevádzkového rizika a bezpečnostného rizika a s kontrolným mechanizmom na riadenie týchto rizík, ktoré súvisia s poskytovaním platobných služieb. Rozhodnutie o prijatí vhodných opatrení teda zákon č. 492/2009 Z. z. o platobných službách ponecháva na poskytovateľa platobných služieb. V tom prípade je však ustanovenie § 2 ods. 2 písm. d) Zákona rekurzívne.

Ak je zároveň podmienkou, aby účinok opatrení vyplývajúcich zo zákona č. 492/2009 Z. z. o platobných službách bol aspoň rovnocenný s účinkom povinností podľa Zákona alebo aby ich cieľom malo byť dosiahnuť rovnocennú alebo vyššiu úroveň bezpečnosti sietí, infraštruktúr a informačných systémov ako podľa Zákona, bolo by nutné posudzovať účinok opatrení s účinkom povinností podľa Zákona. Rovnako tak by bolo nutnosťou posudzovať bezpečnostné ciele a stanoviť, či je možné dosiahnuť rovnocennú alebo vyššiu úroveň bezpečnosti sietí, infraštruktúr a informačných systémov, ako vyžaduje Zákon. Problémom je to, že na účely posudzovania a porovnávania úrovní bezpečnosti sietí a infraštruktúry informačných systémov by musela jestvovať formálne určená metrika alebo spoločne dohodnuté, všeobecne uznané štandardy posudzovania týchto bezpečnostných úrovní, inak nebude možné efektívne analyzovať, či príslušné požiadavky iných právnych predpisov majú šancu dosiahnuť rovnocennú alebo vyššiu úroveň bezpečnosti sietí, infraštruktúr a informačných systémov ako podľa Zákona. Zároveň však platí, že pre posúdenie „úrovne“ bezpečnosti by mal byť pri posudzovaní vyžadovaný analytický detail až na infraštruktúrnej a sieťovej vrstve IT architektúry. Pokiaľ teda budú v budúcnosti jestvovať spoločne akceptované alebo zákonom presadené štandardy posudzovania bezpečnosti systémov a sietí, potom je možné očakávať, že sa podobné ustanovenie azda bude môcť reálne uplatniť v praxi. Alternatívou posudzovania by mohlo byť autoritatívne rozhodnutie kompetentného orgánu, ktorý by mohol rovnocennosť, prevahu, príp. nenaplnenie prevahy požiadaviek vo vzťahu k bezpečnosti na strane osobitného predpisu konštatovať.

V súčasnej dobe, tak ako je naformulovaný, je § 2 ods. 2 písm. d) Zákona pre skutočnú úroveň kybernetickej bezpečnosti v sektore bankovníctva, financií a finančného systému skôr kontraproduktívny. Pre získanie komplexného pohľadu je tu však potrebné poznamenať, že toto ustanovenie nenavrhli pôvodne autori zákona, ale vzniklo až v rámci

[11] Napríklad čl. 3 ods. 3.1, čl. 22 Protokolu (č. 4) o Štatúte Európskeho systému centrálnych bánk a Európskej centrálnej banky v platnom znení (Ú. v. EÚ C 202, 7. 6. 2016), nariadenie Európskej centrálnej banky (EÚ) č. 795/2014 z 3. júla 2014 o požiadavkách v oblasti dohľadu nad systémovo dôležitými platobnými systémami (Ú. v. EÚ L 217, 23. 7. 2014).

medzirezortného pripomienkového konania necitlivými zásahmi niektorých povinne pripomienkujúcich subjektov do textu návrhu Zákona.

Pokiaľ ide o odkaz na ustanovenie § 28d zákona č. 492/2009 Z. z. o platobných službách, tu je vytvorená požiadavka na bezodkladné oznamovanie incidentov zo strany poskytovateľov platobných služieb do Národnej banky Slovenska. Samotné oznamovanie identifikovaných incidentov je v procese riešenia incidentov dôležitou úlohou, avšak túto je možné plniť len za podmienky, že incidenty je vôbec komu oznamovať. V kontexte požiadavky § 28d zákona č. 492/2009 Z. z. o platobných službách na bezodkladné informovanie Národnej banky Slovenska o incidente, ktorá vyplýva z ustanovenia § 2 ods. 2 písm. d) Zákona, však táto podmienka, žiaľ, v súčasnej dobe nie je splnená, keďže Národná banka Slovenska dodnes nezabezpečila technické, technologické a personálne vybavenie vlastnej jednotky pre riešenie kybernetických bezpečnostných incidentov. Zároveň sa počas celej prípravy Zákona Národná banka Slovenska efektívne vyhla tomu, aby sa prihlásila k úlohe ústredného orgánu pre sektor Bankovníctvo, ktorým je podľa prílohy č. 1 Zákona Ministerstvo financií Slovenskej republiky.

K odseku 2 písm. e)

Ďalšia výnimka z pôsobnosti Zákona sa opätovne vzťahuje na požiadavky na zabezpečenie sietí a informačných systémov, a to v sektore podľa osobitného predpisu.[12] Zákon predmetnú výnimku viaže výlučne na dva explicitne stanovené právne predpisy a neumožňuje použitie ďalších právnych predpisov. Pri posudzovaní možnosti aplikácie predmetnej výnimky je nevyhnutné brať na zreteľ vyhodnotenie požiadaviek na zabezpečenie sietí a informačných systémov z hľadiska ich vplyvu na dosiahnutú úroveň bezpečnosti sietí a informačných systémov podľa osobitného predpisu a podľa Zákona. Len v prípade, pokiaľ cieľom požiadaviek podľa osobitného predpisu je zabezpečenie sietí a informačných systémov na vyššej úrovni bezpečnosti sietí a informačných systémov v porovnaní so Zákonom, je možné túto výnimku z pôsobnosti Zákona uplatniť. Zároveň však musíme upozorniť, že aj v prípade legálneho uplatnenia tejto výnimky pôsobnosť Zákona nie je daná len v rozsahu požiadaviek Zákona týkajúcich sa bezpečnosti sietí a informačných systémov, nie ostatných požiadaviek, ktoré Zákon obsahuje. Zákonodarca v tomto prípade vyžaduje splnenie podmienky, aby cieľom požiadaviek na zabezpečenie sietí a informačných systémov vyplývajúcich z osobitného predpisu bolo dosiahnutie vyššej úrovne bezpečnosti sietí a informačných systémov v porovnaní s cieľom požiadaviek v zmysle Zákona. Preto konštatácia alebo vyhodnotenie vzájomnej rovnocennosti požiadaviek v zmysle porovnávaných právnych predpisov nebude postačujúca. Požiadavky na bezpečnosť sietí a informačných systémov v zmysle Zákona vyplývajú, resp. sú dané požiadavkami na prijatie bezpečnostných opatrení v zmysle § 20 Zákona v spojení s vyhláškou Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení. Z uvedeného dôvodu zastávame názor, že pokiaľ existuje záujem o aplikáciu výnimky v zmysle § 2 ods. 2 písm. e) Zákona, je nevyhnutné uskutočniť komparáciu želaných účinkov požiadaviek tak v zmysle Zákona, ako aj osobitného predpisu a vyhodnotenie, že účinky požiadaviek v zmysle osobitného predpisu (pokiaľ ide o úroveň bezpečnosti) prevažujú nad účinkami požiadaviek v zmysle Zákona. Inak sa uplatnia požiadavky Zákona a pôsobnosť Zákona je daná v rozsahu jeho požiadaviek na zabezpečenie sietí a informačných systémov v sektoroch podľa osobitného predpisu. Vieme pripustiť, že posúdenie cieľov by mohlo byť nahradené a potvrdené autoritatívnym rozhodnutím orgánu s príslušnou právomocou.

[12] Zákon č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov v platnom znení; Zákon o ISVS.

V súvislosti so zabezpečením sietí a informačných systémov podľa osobitného predpisu,[13] v spojení s § 2 ods. 2 písm. e) Zákona síce platí, že ustanovenia tohto osobitného predpisu majú prednosť pred Zákonom, ak cieľom požiadaviek v zmysle osobitného predpisu je dosiahnutie vyššej úrovne bezpečnosti sietí a informačných systémov podľa Zákona, súčasne však platí, že posúdenie a porovnanie zamýšľanej úrovne bezpečnosti sietí a informačných systémov v zmysle Zákona a v zmysle osobitného predpisu môže byť komplikované a rovnako nie je zrejmé, kto takéto posúdenie vykoná a je oprávnený zhodnotiť vyššie zamýšľanú úroveň bezpečnosti na jednej alebo druhej strane. Autori tohto komentára zastávajú názor, že aj napriek pochybnostiam o tom, kto je spôsobilý na posúdenie a súčasné porovnanie požiadaviek v zmysle Zákona a osobitného predpisu z pohľadu výslednej (zamýšľanej) úrovne bezpečnosti sietí a informačných systémov, je možné vysloviť pochybnosť o vyššej úrovni bezpečnosti na strane požiadaviek v zmysle osobitného predpisu[12] v porovnaní s požiadavkami v zmysle Zákona. Uvedená pochybnosť je daná najmä tým, že Zákon aj v zmysle § 20 Zákona vyžaduje vykonanie klasifikácie informácií a kategorizácie sietí a informačných systémov, ktorú v Zákone o ISVS v spojení s Výnosom o štandardoch nenájdeme. Súčasne platí, že požiadavky Zákona vyplývajú zo základných štandardov informačnej bezpečnosti,[14] pri ktorých niet pochýb (čo sa aktuálneho vedeckého poznania týka) o úrovni bezpečnosti z pohľadu jednotlivých požiadaviek. Ďalším špecifikom § 20 je to, že tento nestanovuje konkrétne požiadavky na bezpečnosť sietí a informačných systémov, ale len vymenúva oblasti, pre ktoré sa majú bezpečnostné opatrenia prijímať. Z uvedeného dôvodu nie je možné vnímať § 20 Zákona izolovane od vyhlášky NBÚ č. 362/2018 Z. z. vydanej podľa § 32 ods. 1 písm. c) Zákona, lebo práve tento osobitný právny predpis obsahuje konkrétne opatrenia na identifikáciu oblastí v rámci § 20 ods. 3 Zákona, ktoré je potrebné prijať v celom rozsahu, v prípade ústredných orgánov a iných orgánov štátnej správy v rozsahu primeranom. Ak by sme aj boli ochotní bez akejkoľvek hlbšej a najmä kvalifikovanej analýzy uviesť, že cieľom požiadaviek osobitného predpisu je vyššia úroveň bezpečnosti sietí a informačných systémov v zmysle Zákona, netreba zabúdať na to, že nie všetky siete a informačné systémy ústredných orgánov a iných orgánov štátnej správy spadajú pod definičné vymedzenie informačného systému verejnej správy podľa osobitného predpisu, a teda nie všetky siete a informačné systémy ústredných orgánov a iných orgánov štátnej správy je možné považovať za informačné systémy v pôsobnosti povinnej osoby (správca informačného systému verejnej správy) podporujúce služby verejnej správy, služby vo verejnom záujme a verejné služby. V zmysle uvedeného je preto možné vyvodiť záver, že ústredný orgán a iný orgán štátnej správy je povinný minimálne vo vzťahu k tým sieťam a informačným systémom, ktoré nie sú informačnými systémami verejnej správy na účely zaistenia kontinuity, riadenia rizík a riešenia kybernetických bezpečnostných incidentov, prijať primerané a vhodné bezpečnostné opatrenia podľa § 20 Zákona.

Uvedenú nejednoznačnosť aplikácie alebo výluky z aplikácie Zákona v zmysle § 2 ods. 2 Zákona by bolo možné vyriešiť na úrovni samotného Úradu alebo iného kompetentného orgánu, ktorý by ako ústredný orgán štátnej správy pre oblasť kybernetickej bezpečnosti v spolupráci s príslušným ústredným orgánom štátnej správy, v ktorého gescii príslušný osobitný predpis je, mohol rovnocennosť, prevahu, príp. nenaplnenie prevahy požiadaviek vo vzťahu k bezpečnosti na strane osobitného predpisu konštatovať. V opačnom prípade sme toho názoru, že voľba, podľa ustanovení ktorého predpisu bude príslušný ústredný orgán alebo iný orgán štátnej správy postupovať, je na rozhodnutí samotného orgánu, pričom je vhodné zdôrazniť, že prípadný nesúlad ústredného orgánu alebo iného orgánu štátnej správy podľa § 10 Zákona nie je možné v zmysle Zákona Úradom sankcionovať.

[13] Zákon o ISVS

[14] ISO 2700x

Pokiaľ by sme sa mali hlbšie zamerať na požiadavky zákona o ISVS, tak v zmysle jeho § 1 ods. 1 písm. b) upravuje základné podmienky na zabezpečenie integrovateľnosti a bezpečnosti informačných systémov verejnej správy. Zákon o ISVS neurčuje žiadne požiadavky na zaručenie kybernetickej bezpečnosti ani nevyžaduje žiadne opatrenia kybernetickej bezpečnosti. Podľa Zákona o ISVS sú povinné osoby, ktoré sú správcami, povinné zabezpečovať plynulú, bezpečnú a spoľahlivú prevádzku informačných systémov verejnej správy, ktoré sú v ich správe, vrátane organizačného, odborného a technického zabezpečenia a zabezpečovať informačný systém verejnej správy proti zneužitiu. Táto požiadavka na bezpečnosť je natoľko všeobecná, že nie je ani efektívne možné vyžadovať posúdenie, či je účinok nejakých opatrení aspoň rovnocenný s účinkom povinností podľa Zákona, alebo či je ich cieľom dosiahnuť rovnocennú alebo vyššiu úroveň bezpečnosti sietí, infraštruktúry informačných systémov ako podľa Zákona. Podľa § 4 ods. 2 písm. d) zákona o ISVS ministerstvo kontroluje dodržiavanie povinností ustanovených týmto zákonom, pričom vykonávaním niektorých činností pri kontrole dodržiavania štandardov, s výnimkou kontroly dodržiavania štandardov týkajúcich sa bezpečnosti, môže ministerstvo poveriť inú fyzickú osobu alebo právnickú osobu, pričom rozsah týchto činností ministerstvo určí v poverení v rámci svojich právomocí.

V zákone o ISVS však jestvuje prepojenie prostredníctvom splnomocňovacieho ustanovenia v § 13 ods. 1 písm. a) na v zákone bližšie neurčené štandardy. Takýmto štandardom je v konečnom dôsledku Výnos o štandardoch prijatý až o mnoho rokov neskôr. Je zjavné, že v tomto štandarde použili jeho autori štruktúru inšpirujúc sa medzinárodnou technickou normou ISO/IEC 27001.

Štruktúra bezpečnostných cieľov, resp. návrhu bezpečnostných opatrení v Zákone, rovnako ako aj štruktúra bezpečnostných cieľov Výnosu o štandardoch vychádzajú z rovnakej technickej normy, a teda dá sa tvrdiť, že sú veľmi podobné, ak nie totožné. Z toho sa v konečnom dôsledku dá vyvodiť záver, že podmienka ustanovenia § 2 ods. 2 písm. e) Zákona o neuplatnení požiadaviek Zákona v prípade, že cieľom osobitného predpisu je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov ako podľa Zákona, nemôže nastať. Bezpečnostné ciele budú totožné v oboch prípadoch.

Čo sa týka zákona č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon), nie je možné súhlasiť s niektorými názormi, že na zabezpečenie sietí a informačných systémov v rámci pôsobnosti tohto zákona sa paušálne uplatnia výhradne ustanovenia tohto osobitného predpisu. Základným rozporom totiž je, že zákon č. 541/2004 Z. z. o mierovom využívaní jadrovej energie nestanovuje žiadne, resp. iba nepriame a veľmi všeobecné požiadavky na zaistenie bezpečnosti sietí a informačných systémov, a to prostredníctvom požiadaviek na bezpečnosť komponentov jadrového zariadenia. Isteže, pri mierovom využívaní jadrovej energie zohrávajú siete a informačné systémy a služby kľúčovú úlohu. Avšak z kontextu zákona č. 541/2004 Z. z. je zrejmé, že jeho cieľom je najmä zaistenie bezpečného nakladania s rádioaktívnym odpadom a s vyhoretým jadrovým palivom a ochrana pred ionizujúcim žiarením v súvislosti s prevádzkou jadrových zariadení, nie samotná kybernetická bezpečnosť. Ciele v súvislosti s kybernetickou alebo informačnou bezpečnosťou v zákone č. 541/2004 Z. z. priamo spomenuté nie sú ani jedenkrát, pričom akékoľvek požiadavky na opatrenia v oblasti kybernetickej bezpečnosti v zákone č. 541/2004 Z. z. absentujú úplne. S informačnou a kybernetickou bezpečnosťou nepriamo súvisia iba niektoré ustanovenia zákona č. 541/2004 Z. z., ktoré ošetrujú postupy v oblasti fyzickej a objektovej bezpečnosti a havarijnom plánovaní. Fakt, že tieto parciálne ustanovenia vychádzajú z rovnakých základov ako požiadavky na zabezpečenie kybernetickej bezpečnosti upravené v Zákone, nie je dostatočným dôvodom, aby problematika mierového využívania jadrovej energie úplne obchádzala požiadavky na zaistenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Európskej únii. Aj v tomto prípade platí, že ak by zo

zákona č. 541/2004 Z. z. o mierovom využívaní jadrovej energie vyplývali akékoľvek konkrétne požiadavky na opatrenia v kybernetickej bezpečnosti, bolo by najprv potrebné posúdiť, či je účinok týchto opatrení aspoň rovnocenný s účinkom povinností podľa Zákona, alebo či je ich cieľom dosiahnuť rovnocennú alebo vyššiu úroveň bezpečnosti sietí, infraštruktúr a informačných systémov ako podľa Zákona. Zároveň by bolo nutnosťou posudzovať bezpečnostné ciele a stanoviť, či uplatnením ustanovení zákona č. 541/2004 Z. z. je možné dosiahnuť rovnocennú alebo vyššiu úroveň bezpečnosti sietí, infraštruktúr a informačných systémov, ako vyžaduje Zákon. Tu by však rovnako ako pre sporné požiadavky ustanovenia § 2 ods. 2 písm. d) Zákona by pre účely posudzovania a porovnávania úrovní bezpečnosti sietí a infraštruktúry informačných systémov musela jestvovať formálne určená metrika alebo spoločne dohodnuté, všeobecne uznané štandardy posudzovania týchto bezpečnostných úrovní. V opačnom prípade nebude možné efektívne analyzovať, či požiadavky zákona č. 541/2004 Z. z. môžu dosiahnuť rovnocennú alebo vyššiu úroveň bezpečnosti sietí, infraštruktúr a informačných systémov ako podľa Zákona.

K odseku 2 písm. f)

Poslednou výnimkou z pôsobnosti Zákona je vyňatie jeho pôsobnosti vo vzťahu k neurčitému a jednoznačne nevymedzenému okruhu osobitných predpisov (výpočet osobitných predpisov je len exemplifikatívny). V zmysle § 2 ods. 2 písm. f) platí, že Zákon sa nevzťahuje na osobitné predpisy, pričom sa nepožaduje ani komparácia zamýšľaných cieľov požiadaviek konkrétneho osobitného predpisu s požiadavkami Zákona. Ide tak o jednoznačné a absolútne vyňatie pôsobnosti Zákona vo vzťahu k exemplifikatívnemu výpočtu osobitných predpisov, ktorých rozsah môže byť oproti tomu vypočítanému Zákonom samotným širší.

Pokiaľ ide o nariadenie eIDAS, je možné vysloviť záver, že pôsobnosť Zákona nie je daná pri poskytovaní dôveryhodných služieb, a to ani vtedy, pokiaľ sú tieto služby poskytované prevádzkovateľom základnej služby alebo poskytovateľom digitálnej služby. Dôvodom je skutočnosť, že poskytovatelia dôveryhodných služieb (kvalifikovaní a nekvalifikovaní) sú povinní v zmysle čl. 19 s ohľadom na riziká zaistiť prostredníctvom vhodných technických a organizačných opatrení na riadenie týchto rizík primeranú úroveň bezpečnosti, najmä opatrenia na prevenciu a minimalizáciu vplyvu bezpečnostných incidentov a na oznámenie nepriaznivých účinkov všetkých takýchto incidentov zainteresovaným stranám.

Zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) ustanovuje podmienky, za akých možno použiť informačno-technické prostriedky bez súhlasu toho, voči ktorému sa informačno-technické prostriedky majú použiť, a určuje presný rozsah subjektov, ktoré sú oprávnené informačno-technické prostriedky používať (Policajný zbor, Slovenská informačná služba, Vojenské spravodajstvo, Zbor väzenskej a justičnej stráže a Colná správa) s povinnosťou použitia údajov získaných informačno-technickými prostriedkami výlučne na dosiahnutie účelu pri plnení úloh štátu, spĺňajúcich podmienku nevyhnutnosti použitia informačno-technických prostriedkov, a to nevyhnutnosť použitia informačno-technických prostriedkov na zabezpečenie ochrany ústavného zriadenia, vnútorného poriadku a zahraničnopolitických záujmov štátu, bezpečnosti a obrany štátu, na získavanie informácií zo zahraničných zdrojov, predchádzanie a objasňovanie trestnej činnosti alebo na ochranu práv a slobôd iných a ak dosiahnutie tohto účelu inak by bolo neúčinné alebo podstatne sťažené.

Pokiaľ ide o Zákon o elektronických komunikáciách, výluka pôsobnosti Zákona je daná aj vo vzťahu k prevádzkovateľom základných služieb a poskytovateľom digitálnych služieb poskytujúcich v zmysle zákona o elektronických komunikáciách elektronické komunikačné siete alebo elektronické komunikačné služby. Zákon o elektronických komunikáciách

vo svojom § 64 ustanovuje, že každý podnik poskytujúci verejné siete alebo verejné služby je povinný prijať zodpovedajúce technické a organizačné opatrenia na ochranu bezpečnosti svojich sietí a služieb, ktoré s ohľadom na stav techniky musia zabezpečiť úroveň bezpečnosti, ktorá je primeraná existujúcemu riziku. Podnik poskytujúci verejné siete alebo služby je povinný prijať opatrenia s cieľom predchádzať bezpečnostným incidentom a minimalizovať vplyv bezpečnostných incidentov na užívateľov a vzájomne prepojené siete, udržiavať integritu svojich sietí s cieľom zaručiť kontinuitu poskytovania služieb prostredníctvom týchto sietí, bezodkladne informovať Úrad pre reguláciu elektronických komunikácií a poštových služieb (ďalej v tomto odseku ako „úrad“) o narušení bezpečnosti alebo integrity, ktoré mali významný vplyv na prevádzku sietí alebo služieb, umožniť bezpečnostný audit vykonaný buď úradom, alebo ním určenou kvalifikovanou osobou či spolupracovať s úradom. Podnik poskytujúci verejné siete a pridružené prostriedky je súčasne povinný zabezpečiť, aby jeho sieť a pridružené prostriedky zodpovedali technickým normám a technickým špecifikáciám pre siete alebo služby (zabezpečenie zhody s technickými normami a technickými špecifikáciami pre siete a služby) z hľadiska bezpečnosti prevádzky siete, udržiavania integrity siete, interoperability služieb a pripojenia koncových zariadení.

Pri uplatňovaní pôsobnosti Úradu pre reguláciu elektronických komunikácií a poštových služieb vymedzenej zákonom o elektronických komunikáciách a pôsobnosti Národného bezpečnostného úradu podľa Zákona platí, že si tieto úrady v zmysle § 8 ods. 3 zákona o elektronických komunikáciách vymieňajú informácie a podklady dôležité na zabezpečenie kybernetickej bezpečnosti v rozsahu a spôsobom ustanoveným na základe uzatvorených dohôd o spolupráci. V prípade výmeny informácií prijímajúci úrad zabezpečí rovnakú úroveň dôvernosti ako úrad, ktorý informáciu poskytne.

§ 3
Vymedzenie základných pojmov

Na účely tohto zákona sa rozumie

a) sieťou a informačným systémom elektronická komunikačná sieť, informačný systém, každé zariadenie a komunikačný systém alebo údaje, ktoré sú v nich vytvárané, ukladané, spracúvané, získavané alebo prenášané prostredníctvom elektronickej komunikačnej siete alebo informačného systému, na účely prevádzkovania, používania, ochrany a udržiavania týchto sietí a systémov,

b) kybernetickým priestorom globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi,

c) kontinuitou strategická a taktická schopnosť organizácie plánovať a reagovať na udalosti a incidenty s cieľom pokračovať vo výkone činností na prijateľnej, vopred stanovenej úrovni,

d) dôvernosťou záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom,

e) dostupnosťou záruka, že údaj alebo informácia je pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď je údaj a informácia potrebná a požadovaná,

f) integritou záruka, že bezchybnosť, úplnosť alebo správnosť informácie neboli narušené,

g) kybernetickou bezpečnosťou stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov,