§ 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 a informačných systémov a oznamovania kybernetických bezpečnostných incidentov v sektore bankovníctva, financií alebo finančného systému podľa osobitného predpisu,[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 vyššiu úroveň bezpečnosti sietí a informačných systémov ako podľa tohto zákona, a ani na platobné systémy a na systémy zúčtovania cenných papierov 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)]

[1)] § 2 ods. 1 písm. g), ods. 3 zákona Národnej rady Slovenskej republiky č. 46/1993 Z. z. o Slovenskej informačnej službe v znení zákona č. 151/2010 Z. z.

§ 2 ods. 1 písm. c) a h), ods. 2 a § 4a zákona Národnej rady Slovenskej republiky č. 198/1994 Z. z. o Vojenskom spravodajstve v znení neskorších predpisov.

Zákon č. 319/2002 Z. z. o obrane Slovenskej republiky neskorších predpisov.

[2)] Napríklad 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 znení neskorších predpisov.

[3] 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 znení neskorších predpisov, 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).

[4] Napríklad čl. 127 ods. 2 Zmluvy o fungovaní Európskej únie v platnom znení (Ú. v. EÚ C 202, 7. 6. 2016), 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 Národnej rady Slovenskej republiky č. 566/1992 Zb. o Národnej banke Slovenska v znení neskorších predpisov, § 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.

[5] 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).

[6] Zákon č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

[7] Napríklad 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 (Ú. v. EÚ L257, 28. 8. 2014), 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 znení neskorších predpisov, zákon č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov.

Súvisiace ustanovenia:

§ 3

Súvisiace predpisy:

zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností; zákon č. 46/1993 Z. z. o Slovenskej informačnej službe; zákon č. 198/1994 Z. z. o Vojenskom spravodajstve; zákon č. 319/2002 Z. z. o obrane Slovenskej republiky; zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy; zákon č. 398/2015 Z. z. o európskom ochrannom príkaze v trestných veciach; zákon č. 91/2016 Z. z. o trestnej zodpovednosti právnických osôb; zákon č. 541/2004 Z. z. o využívaní jadrovej energie (atómový zákon); zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov

(zákon o ochrane pred odpočúvaním); zákon č. 351/2011 Z. z. o elektronických komunikáciách; nariadenie vlády č. 216/2004 Z. z., ktorým sa ustanovujú oblasti utajovaných skutočností; výnos Ministerstva financií SR č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy; 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); nariadenie Európskeho parlamentu a Rady (ES) č. 460/2004 o zriadení Európskej agentúry pre bezpečnosť sietí a informácií – agentúra ENISA

Z literatúry:

BRVNIŠŤAN, M. *Ochrana utajovaných skutočností v spektre historického vývoja*. Bratislava : Akadémia policajného zboru, 2013

K ods. 1

Podľa odseku 1 ZoKB ustanovuje minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti, a to zavedením bezpečnostných opatrení rámcovo načrtnutých v § 20 ZoKB, pričom § 20 zároveň vymedzuje, čo sa bezpečnostnými opatreniami rozumie. Konkrétne bezpečnostné opatrenia však sú/budú vydané všeobecne záväzným právnym predpisom v rozsahu definovanom v splnomocňovacích ustanoveniach podľa § 32 ZoKB.

K ods. 2

Ustanovenie § 2 odsek 2 ZoKB vymedzuje siete a informačné systémy (vrátane informačného obsahu) v určitých odvetviach hospodárstva, na ktoré sa vzťahujú špecifické obmedzenia pôsobnosti ZoKB. Dôvodom je to, že tieto odvetvia sú už regulované inými právnymi aktmi EÚ, resp. sú regulované inými právnymi predpismi na národnej úrovni. Ide o špecifické odvetvia ošetrené predpismi s požiadavkami na bezpečnosť sietí a informačných systémov, ktorých účinok je vyšší alebo aspoň rovnocenný s úrovňou, ktorú predpisuje ZoKB. To znamená, že tieto predpisy majú prednosť pred ZoKB a v zmysle smernice NIS by sa v týchto prípadoch nemal vykonávať ani proces identifikácie PZS. Vymedzenie sietí a informačných systémov vylúčených z pôsobnosti ZoKB je podrobnejšie rozpísané v odseku 2 písmenách a) až f).

K ods. 2 písm. a)

Podľa tohto ustanovenia sa špecifické obmedzenia pôsobnosti ZoKB vzťahujú na siete a informačné systémy, ktoré spracúvajú utajované skutočnosti. Dôvodom je, že tieto systémy sú regulované osobitným právnym predpisom, ktorým je **zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností**. Podľa § 2 písm. a) citovaného zákona sa za utajovanú skutočnosť považuje informácia alebo vec určená „pôvodcom utajovanej skutočnosti“ podľa písm. e),

ktorú je potrebné vzhľadom na záujem SR chrániť a ktorá môže vzniknúť len v oblastiach, ktoré ustanovila vláda nariadením č. 216/2004 Z. z., ktorým sa ustanovujú oblasti utajovaných skutočností. V zmysle § 3 citovaného zákona (t. j. zákona č. 215/2004 Z. z.) sa tieto utajované skutočnosti členia podľa stupňa utajenia na prísne tajné, tajné, dôverné a vyhradené.

Z uvedeného vyplýva, čo súčasná prax aj potvrdzuje, že tvorba zoznamov utajovaných skutočností je voľne ponechaná na jednotlivé rezorty, pričom neexistuje ich vzájomná koordinácia. Dôsledkom je rozdielne „stanovovanie stupňov" pri rovnakých „druhoch" utajovaných skutočností, pričom nie sú zohľadnené ani špecifiká systémov EÚ a NATO, ktoré majú diametrálne odlišný spôsob ich vytvárania. Na základe voľnosti určovania zoznamov utajovaných skutočností oprávnenými osobami/pôvodcami utajovaných skutočností a rozdielnosti spomenutého stanovovania stupňov je tým pádom ponechaná aj slobodná možnosť určovania si vzťahu k ZoKB. V praxi táto voľnosť prispeje k vytváraniu nehomogénneho prostredia v oblasti vytvárania a začleňovania utajovaných skutočností, čo sa prejaví negatívne pri vzájomnej komunikácii inštitúcií, výmene informácií vrátane prepájania súvisiacich informačných systémov a sietí.

K ods. 2 písm. b)

a) Ustanovenia ZoKB sa z povahy jeho predmetu úpravy nevzťahujú na činnosti Slovenskej informačnej služby. Ide o siete a informačné systémy, ktoré spracovávajú informácie v zmysle § 2 ods. 1 písm. g) a ods. 3 **zákona č. 46/1993 Z. z. o Slovenskej informačnej službe**, a to informácie týkajúce sa aktivít a ohrození v kybernetickom priestore, ak ohrozujú bezpečnosť štátu, a ak je to potrebné na zabránenie aktivitám a ohrozeniam podľa § 2 ods. 1 a 2 zákona č. 46/1993 Z. z. o Slovenskej informačnej službe a na realizáciu zahraničnopolitických záujmov SR, kde informačná služba vykonáva primerané bezpečnostné opatrenia. V zmysle citovaného ustanovenia ide o rozsah činnosti ohrozujúcej ústavné zriadenie, územnú celistvosť a zvrchovanosť SR, činnosti smerujúcej proti bezpečnosti SR, aktivity cudzích spravodajských služieb, organizovanej trestnej činnosti, terorizmu vrátane informácií o účasti na terorizme, jeho financovaní alebo podporovaní, činnosti spočívajúcej v politickom a náboženskom extrémizme, extrémizme prejavujúcom sa násilným spôsobom a škodlivom sektárskom zoskupení, aktivitách a ohrozeniach v kybernetickom priestore, ak ohrozujú bezpečnosť štátu, činnosti nelegálnej medzinárodnej prepravy osôb a migrácie osôb, alebo v prípade skutočností spôsobilých vážne ohroziť alebo poškodiť hospodárske záujmy SR, spôsobilých ohroziť alebo

spôsobiť únik informácií a vecí chránených podľa osobitného predpisu[46] alebo medzinárodných zmlúv, alebo medzinárodných dohovorov, ale ide aj o informácie, ktoré vznikajú v zahraničí a smerujú proti ústavnému zriadeniu a bezpečnosti SR a o informácie potrebné na realizáciu jej zahraničnopolitických záujmov.

b) **Rozvíjanie politiky a spôsobilostí kybernetickej obrany, ktoré súvisia so spoločnou bezpečnostnou a obrannou politikou,** bolo pre svoj mimoriadny význam zaradené medzi hlavné priority Stratégie Európskej únie pre kybernetickú bezpečnosť schválenej Európskou komisiou 7. februára 2013 s víziou EÚ o otvorenom, bezpečnom a chránenom kybernetickom priestore. Ustanovenia ZoKB sa podľa písmena b) z povahy jeho predmetu úpravy nevzťahujú na činnosti Ministerstva obrany SR a Vojenského spravodajstva pri aktivitách a ohrozeniach v kybernetickom priestore, ak ohrozujú bezpečnosť štátu (kybernetická obrana). To znamená, že ZoKB sa nevzťahuje na siete a informačné systémy spravujúce informácie v zmysle § 2 ods. 1 písm. c) a h), ods. 2 a § 4a **zákona č. 198/1994 Z. z. o Vojenskom spravodajstve**, ako aj **zákona č. 319/2002 Z. z. o obrane Slovenskej republiky**, ktoré sa tejto problematiky priamo týkajú. Podľa uvedených ustanovení ide o aktivity v oblasti terorizmu, jeho financovania alebo podporovania, kybernetického terorizmu, vlastizrady, sabotáže, záškodníctva a iných aktivít a ohrození v kybernetickom priestore, ktorého rozsah v § 3 písm. b) terminologicky zadefinoval ZoKB. Vojenské spravodajstvo tak plní úlohy na úseku kybernetickej bezpečnosti štátu a kybernetickej bezpečnosti prostredníctvom Centra pre kybernetickú obranu SR, kde získava, sústreďuje, analyzuje a vyhodnocuje dôležité informácie na zabezpečenie kybernetickej obrany, informuje dotknuté subjekty a v zmysle svojich právomocí zavádza v tejto oblasti primerané bezpečnostné opatrenia na zabránenie uvedených aktivít.

Zároveň je potrebné uviesť, že na uvedené informačné aktíva, ktoré sa týkajú zabezpečenia obrany SR, bezpečnosti SR a utajovaných skutočností, sa nevzťahuje ani zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy vrátane jeho vykonávacieho predpisu, ktorým je výnos Ministerstva financií SR č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy.

[46] Zákon č. 100/1996 Z. z. o ochrane štátneho tajomstva, služobného tajomstva, o šifrovej ochrane informácií.

K ods. 2 písm. c)

Prudké zníženie počítačovej kriminality je pre svoj osobitný význam druhou z piatich priorít dokumentu s názvom Stratégia Európskej únie pre kybernetickú bezpečnosť schváleného 7. februára 2013.

Ustanovenia ZoKB sa nevzťahujú na ustanovenia osobitných predpisov o vyšetrovaní, odhaľovaní a stíhaní trestných činov v zmysle zákona č. 398/2015 Z. z. o európskom ochrannom príkaze v trestných veciach, ako ani zákona č. 91/2016 Z. z. o trestnej zodpovednosti právnických osôb. Po vecnej stránke ide o vydávanie príkazov súdmi alebo inými justičnými orgánmi členských štátov v trestnom konaní vrátane prijímania následných opatrení na území SR a o položenie základov trestnej zodpovednosti právnických osôb, druhov trestov, ich ukladania a úpravu trestného konania proti právnickým osobám, s previazaním problematiky na zákon č. 300/2005 Z. z Trestný zákon, zákon č. 301/2005 Z. z. Trestný poriadok, ako aj zákon č. 650/2005 Z. z. o vykonaní príkazu na zaistenie majetku alebo dôkazov v Európskej únii.

K ods. 2 písm. d)

Vzhľadom na to, že ZoKB v zmysle § 2 ods. 1 ustanovuje len minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti a požiadavky na bezpečnosť, zabezpečenie integrity a odolnosti sietí a informačných systémov, štandardizáciu, vydávanie a dodržovanie zásad vrátane oznamovania kybernetických bezpečnostných incidentov v sektore bankovníctva, financií, finančných trhov, platobných systémov a systémov zúčtovania cenných papierov výrazne presahujú požiadavky ZoKB, špecifické obmedzenia pôsobnosti ZoKB sa vzťahujú aj na tieto siete a informačné systémy. Táto oblasť je už harmonizovaná a striktne regulovaná prostredníctvom primárneho a sekundárneho práva EÚ a noriem vypracovaných spoločne s európskymi orgánmi dohľadu, a to Európskou centrálnou bankou, Európskym systémom centrálnych bánk a Národnou bankou Slovenska. Pokiaľ ide o požiadavky na oznamovanie incidentov, tieto sú už súčasťou bežných postupov dohľadu vo finančnom odvetví a sú zahrnuté do príručiek týkajúcich sa dohľadu. Podľa smernice NIS, ako aj dôvodovej správy to znamená, 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 ZoKB, použijú sa na zabezpečenie kybernetickej bezpečnosti osobitné predpisy. V zmysle stanoviska Európskej centrálnej banky, smernica NIS transponovaná do ZoKB nemá žiadny vplyv na režim Eurosystému pre dohľad nad platobnými a zúčtovacími systémami podľa práva EÚ. Z uvedeného vyplýva, že na túto oblasť sa požiadavky ZoKB nevzťahujú.

K ods. 2 písm. e)

a) Podľa tohto ustanovenia sa na siete a informačné systémy v sektore jadrovej energetiky patriacej pod **zákon č. 541/2004 Z. z. o využívaní jadrovej energie (atómový zákon)** vzťahujú špecifické obmedzenia pôsobnosti ZoKB, pretože citovaný zákon obsahuje ustanovenia na zabezpečenie sietí a informačných systémov, ktoré vychádzajú z rovnakých základov ako požiadavky na zabezpečenie kybernetickej bezpečnosti upravené v ZoKB. Na zabezpečenie týchto sietí a informačných systémov sa preto použijú osobitné predpisy. Podľa zákona č. 541/2004 Z. z. je využívanie jadrovej energie možné len na mierové účely a v súlade s národnými stratégiami, medzinárodnými zmluvami, ktorými je Slovenská republika viazaná, ako aj v súlade s právnymi aktmi EÚ a právnymi aktmi Európskeho spoločenstva pre atómovú energiu. Podľa § 3 ods. 8 citovaného zákona právny, regulačný a organizačný rámec jadrovej bezpečnosti sa udržiava a zdokonaľuje na základe prevádzkových skúseností, poznatkov získaných z analýz bezpečnosti prevádzkovaných jadrových zariadení, vývoja technológií a výsledkov výskumu v oblasti bezpečnosti. Štátna správa a dozor je podľa § 4 v pôsobnosti Úradu pre jadrový dozor SR, ktorý kontroluje dodržiavanie povinností v zmysle osobitných predpisov. Pre uvedený sektor sa uplatňujú prísne pravidlá a kontrolné mechanizmy medzinárodného charakteru.

b) Podľa ods. 2 písm. e) sa špecifické obmedzenia pôsobnosti ZoKB vzťahujú aj na siete a informačné systémy v sektore verejnej správy patriace pod **zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy,** ak je ich cieľom dosiahnuť vyššiu úroveň zabezpečenia sietí a informačných systémov ako v ZoKB. Tento osobitný právny predpis obsahuje ustanovenia na zabezpečenie sietí a informačných systémov, ktoré vychádzajú z rovnakých základov ako požiadavky na zabezpečenie kybernetickej bezpečnosti upravené v ZoKB. Podľa § 4 ods. 2 písm. f) citovaného zákona informačnú bezpečnosť informačných systémov verejnej správy riadi a koordinuje ÚPVII. Povinné osoby musia podľa § 3 ods. 4 písm. b), c) a i) zabezpečovať plynulú, bezpečnú a spoľahlivú prevádzku informačných systémov verejnej správy, ktoré sú v ich správe, vrátane organizačného, odborného a technického zabezpečenia, zabezpečovať informačný systém verejnej správy proti zneužitiu a zabezpečovať, aby bol informačný systém verejnej správy v súlade so štandardmi pre informačné systémy verejnej správy. Podrobnosti k uvedeným povinnostiam sú vydané všeobecne záväzným právnym predpisom, výnosom Ministerstva financií SR č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy, ktorý určuje bezpečnostné štandardy vzťahujúce sa na technické prostriedky,

sieťovú infraštruktúru, programové prostriedky a údaje, štandardy pre architektúru riadenia a štandardy minimálneho technického zabezpečenia. ÚPVII podľa § 4 ods. 2 písm. d) zákona č. 275/2006 Z. z. kontroluje dodržiavanie povinností ustanovených týmto zákonom. Poverovanie výkonu kontroly dodržiavania štandardov bezpečnosti sietí a informačných systémov podľa písmena f) na základe uzatvárania dohôd s fyzickými osobami alebo právnickými osobami tento osobitný predpis vylučuje. Ide o jednu zo zásadných bezpečnostných požiadaviek na zabezpečenie informačných systémov verejnej správy ustanovenú týmto osobitným predpisom, ktorá prevyšuje § 5 ods. 2 ZoKB, ktorý umožňuje NBÚ uzatvárať dohody s fyzickými osobami na účel výkonu kontroly.

K ods. 2 písm. f)

a) Povinnosti vyplývajúce zo ZoKB sa nevzťahujú na PZS a PDS poskytujúcich dôveryhodné služby v zmysle **nariadenia 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)**, ktorí podliehajú bezpečnostným požiadavkám ustanoveným v tomto nariadení.
b) Ustanovenia ZoKB sa nevzťahujú na **zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov (zákon o ochrane pred odpočúvaním)**. Tento zákon ustanovuje podmienky použitia informačno-technických prostriedkov bez predchádzajúceho súhlasu toho, komu zasahuje do súkromia orgán štátu, ktorý informačno-technický prostriedok používa. Informačno-technický prostriedok možno použiť len vtedy, ak je to v demokratickej spoločnosti nevyhnutné na zabezpečenie ochrany ústavného zriadenia, vnútorného poriadku a zahraničnopolitických záujmov štátu, bezpečnosti a obrany štátu, 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; informačno-technické prostriedky v pôsobnosti Slovenskej informačnej služby a Vojenského spravodajstva možno použiť aj mimo územia SR v rozsahu úloh podľa osobitných predpisov. Použitím informačno-technického prostriedku sa môže základné právo alebo sloboda obmedziť len v nevyhnutnom rozsahu a nie dlhšie, ako je to nevyhnutné na dosiahnutie zákonom uznaného cieľa, na ktorý slúži.
c) ZoKB sa nevzťahuje na PZS a PDS poskytujúcich verejné komunikačné siete alebo verejne dostupné elektronické komunikačné služby v zmysle

smernice Európskeho parlamentu a Rady 2002/21/ES o spoločnom regulačnom rámci pre elektronické komunikačné siete a služby (rámcová smernica; Ú. v. ES L 108, 24. 4. 2002, s. 33), ktoré podliehajú osobitným požiadavkám týkajúcim sa bezpečnosti a integrity ustanoveným v uvedenej smernici, transponovanej do **zákona č. 351/2011 Z. z. o elektronických komunikáciách**, ktorý zaraďuje Internet a počítačové siete medzi elektronické komunikačné siete. Z hľadiska informačnej bezpečnosti ide o aspekty, ako sú fyzická bezpečnosť sietí, dodržiavanie technických noriem, štandardov, prevádzková bezpečnosť, elektromagnetické vyžarovanie, úprava podmienok odpočúvania komunikácie, šírenie reklamných správ, ochrana osobných údajov a údajov spojených s prevádzkou komunikačných sietí. Podľa tohto zákona majú príslušné kompetentné orgány rozsiahle regulačné a kontrolné právomoci. V prvom rade je to ústredný orgán štátnej správy, ktorými sú Ministerstvo dopravy a výstavby SR a Úrad pre reguláciu elektronických komunikácií a poštových služieb (ďalej v tomto texte ako „úrad“) ako národný regulátor a cenový orgán v oblasti elektronických komunikácií. Ustanovením § 64 uvedeného zákona sa ukladá podnikom (t. j. povinným osobám), ktoré poskytujú verejné siete alebo verejné služby, povinnosť 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. Opatrenia sa prijímajú najmä s cieľom predchádzať bezpečnostným incidentom a minimalizovať vplyv bezpečnostných incidentov na užívateľov a vzájomne prepojené siete. V zmysle nariadenia Európskeho parlamentu a Rady (ES) č. 460/2004 o zriadení Európskej agentúry pre bezpečnosť sietí a informácií – agentúra ENISA, úrad poskytuje informácie o narušení bezpečnosti alebo integrity, ktoré mali významný vplyv na prevádzku sietí alebo služieb regulačným orgánom v členských štátoch. Úrad každoročne predkladá Európskej komisii a agentúre ENISA súhrnnú správu o oznámeniach a o opatreniach, ktoré v tejto súvislosti vykonal. Pri uplatňovaní pôsobnosti úradu vymedzenej uvedeným zákonom a pôsobnosti NBÚ ustanovenej ZoKB si tieto úrady vymieňajú informácie a podklady dôležité na zabezpečenie kybernetickej bezpečnosti v rozsahu a spôsobom ustanoveným na základe uzatvorených dohôd o spolupráci. Údaje, ktoré sú predmetom telekomunikačného tajomstva, môže úrad sprístupniť NBÚ len v záujme bezpečnosti štátu, na účely riešenia kybernetického bezpečnostného incidentu, na účel ich zberu, spracovávania a uchovávania v rozsahu potrebnom na identifikáciu kybernetického bezpečnostného incidentu a zabezpečenia kybernetickej bezpečnosti podľa ZoKB.

Z dôvodovej správy

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.

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 (atómový zákon), 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, 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, zákon Národnej rady Slovenskej republiky č. 198/1994 Z. z. o Vojenskom spravodajstve.

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.

§ 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,