PRIESTUPKY A SPRÁVNE DELIKTY PODĽA ZÁKONA O KYBERNETICKEJ BEZPEČNOSTI

OFFENSES AND ADMINISTRATIVE OFFENSES UNDER THE CYBER SECURITY ACT

Viera Jakušová[1]

DOI: https://doi.org/10.24040/pros.13.11.2020.svp.105-117

Abstrakt

Príspevok vymedzuje pojmy kybernetická bezpečnosť a kybernetický priestor z hľadiska medzinárodného štandardu, ako aj z hľadiska právnej úpravy Slovenskej republiky upravenej v zákone č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. V príspevku sú analyzované skutkové podstaty priestupkov a správnych deliktov v oblasti kybernetickej bezpečnosti v zmysle uvedeného zákona.

Kľúčové slová

Zákon o kybernetickej bezpečnosti. Kybernetická bezpečnosť. Kybernetický priestor. Správnoprávna zodpovednosť. Priestupky. Správne delikty.

Abstract

The contribution defines the terms cyber security and cyberspace from the point of view of international standards, as well as in terms of legislation of the Slovak Republic regulated in Act No. 69/2018 Coll. on Cyber Security as amended by later regulations. The contribution analyzes the facts of the offenses and administrative offenses in the field of cyber security in accordance with the law.

Keywords

Cyber Security Act. Cyber security. Cyberspace. Administrative responsibility. Offenses. Administrative offenses.

[1] Mgr. Viera Jakušová, 2. ročník, denná forma doktorandského štúdia, viera.jakusova@flaw.uniba.sk, Katedra správneho a environmentálneho práva, Právnická fakulta Univerzity Komenského v Bratislave.

Úvod

Cieľom príspevku je rozbor skutkových podstát priestupkov a správnych deliktov v oblasti kybernetickej bezpečnosti, ktoré vymedzuje zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „ZoKB“). Konkrétne, definovať, kto je prevádzkovateľom základnej služby v zmysle ZoKB a aká skutočnosť môže byť problematická v prípade tohto prevádzkovateľa ako špeciálneho subjektu priestupku podľa ZoKB. Okrem iného je tiež dôležité vymedziť pojem kybernetická bezpečnosť, ako z hľadiska medzinárodného štandardu, tak aj z hľadiska právnej úpravy Slovenskej republiky upravenej v ZoKB. V súvislosti s uvedeným je potrebné aj definovať pojem kybernetický priestor, nakoľko je s pojmom kybernetickej bezpečnosti previazaný.

1. Kybernetická bezpečnosť a súvisiace pojmy

ZoKB všeobecne upravuje organizáciu, pôsobnosť a povinnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti, národnú stratégiu kybernetickej bezpečnosti, jednotný informačný systém kybernetickej bezpečnosti, organizáciu a pôsobnosť jednotiek pre riešenie kybernetických bezpečnostných incidentov a ich akreditáciu, postavenie a povinnosti prevádzkovateľa základnej služby a poskytovateľa digitálnej služby, bezpečnostné opatrenia, systém zabezpečenia kybernetickej bezpečnosti, kontrolu nad dodržiavaním tohto zákona a audit.[2] ZoKB tiež ustanovuje minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti.[3]

Pôsobnosť orgánov verejnej moci v oblasti kybernetickej bezpečnosti je definovaná v § 4 ZoKB.[4]

[2] Pozri § 1 ZoKB.
[3] Pozri § 2 ods. 1 ZoKB.
[4] Pôsobnosť vykonávajú nasledujúce orgány: Národný bezpečnostný úrad (ďalej len „NBÚ“), 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. ZoKB pomenováva na svoje účely tieto orgány verejnej moci aj ako ústredné orgány. Pôsobnosť na úseku kybernetickej bezpečnosti majú aj ministerstvá a ostatné ústredné orgány štátnej správy, ktoré nie sú ústredným orgánom, Generálna prokuratúra Slovenskej republiky, Najvyšší kontrolný úrad Slovenskej republiky, Úrad pre dohľad nad zdravotnou starostlivosťou, Úrad na ochranu osobných údajov Slovenskej republiky, Úrad pre

Na to, aby sme prešli k analýze priestupkov a správnych deliktov podľa ZoKB, tak je potrebné definovať pojem kybernetická bezpečnosť. Podľa § 3 písm. g) ZoKB je 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.

Pojem kybernetickej bezpečnosti je definovaný aj viacerými medzinárodnými štandardami. Tieto štandardy nie sú právne záväzné, avšak legislatíva sa na ne častokrát odvoláva, nakoľko dávajú presnejšie formulované odpovede na otázky, ktoré súvisia s kybernetickou bezpečnosťou.[5]

Štandard možno z formálneho hľadiska definovať ako: „dokument, ktorý vznikol na základe konsenzu a bol schválený uznaným orgánom, ktorý poskytuje pre všeobecné a opakované použitie pravidlá, smernice alebo charakteristiky činností alebo ich výsledkov zamerané na dosiahnutie optimálneho stupňa usporiadania v danom kontexte.“[6]

Pojem kybernetická bezpečnosť je v zmysle medzinárodného štandardu ISO/IEC 27032:2012 Information technology - Security techniques - Guidelines for cybersecurity definovaný ako zachovanie dôvernosti, integrity a dostupnosti informácií v kybernetickom priestore. Možno povedať, že tu pôjde len o informácie, ktoré sú prenášané a uložené v kybernetickom priestore. Zainteresované strany stanovujú pre vytvorenie a zachovanie bezpečnosti v kybernetickom priestore opatrenia, na ktoré sa vzťahuje kybernetická bezpečnosť. Medzi zainteresované strany v kybernetickom priestore možno zaradiť užívateľov (jednotlivci, súkromné a verejné organizácie) a poskytovateľov (poskytovatelia Internetu a poskytovatelia aplikačných služieb).[7]

V súvislosti s uvedeným považujeme za významné definovať aj pojem kybernetický priestor, nakoľko určuje obsah pojmu kybernetická bezpečnosť. Možno povedať, že neexistuje

---

reguláciu sieťových odvetví a iné štátne orgány v rozsahu svojej pôsobnosti. ZoKB tieto orgány označuje aj ako iné orgány štátnej správy. Pozri § 4 ZoKB.

[5] ANDRAŠKO, J. Bezpečnosť informačných systémov verejnej správy vo svetle zákona o kybernetickej bezpečnosti a zákona o informačných technológiách vo verejnej správe. In: *Revue pro právo a technologie*. [Online]. 2019, č. 20, s. 9. [cit. 2020-10-29]. Dostupné na internete: https://journals.muni.cz/revue/article/view/12536.

[6] ISO/IEC Guide 2:2004 Standardization and related activities - General vocabulary, s. 10.

[7] ANDRAŠKO, J. Bezpečnosť informačných systémov verejnej správy vo svetle zákona o kybernetickej bezpečnosti a zákona o informačných technológiách vo verejnej správe. In: *Revue pro právo a technologie*. [Online]. 2019, č. 20, s. 12. [cit. 2020-10-29]. Dostupné na internete: https://journals.muni.cz/revue/article/view/12536.

jednoznačná, všeobecne akceptovaná definícia pojmu kybernetický priestor. Kybernetický priestor možno chápať ako systém systémov (SoS) zložený z rôznych digitálnych zariadení spojených počítačovými sieťami, pripojenými na Internet (vrátane programového vybavenia, údajov, aplikačných programov, technickej infraštruktúry) a ľudí, ktorí v tomto priestore pôsobia, činností, ktoré v ňom prebiehajú, pravidiel, ktoré upravujú činnosti a vzťahy v priestore. Iné definície chápu kybernetický priestor ako virtuálny systém informácií, vzťahov, činností, ktoré vznikajú pri spracovaní informácií prostredníctvom digitálnych informačných a komunikačných technológií, ktorý však neexistuje v materiálnej forme.[8]

Podľa § 3 písm. b) ZoKB je 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.

Významným špecifikom kybernetickej bezpečnosti je skutočnosť, že jednotlivé komponenty kybernetického priestoru majú rôznych vlastníkov, správcov, prevádzkovateľov, ale aj používateľov. Nedodržiavanie minimálnych bezpečnostných zásad, metód ochrany a minimálnych bezpečnostných opatrení v oblasti kybernetickej bezpečnosti, resp. ich chýbajúca unifikácia, zvyšujú mieru zraniteľnosti prevádzkovaných elektronických informačných, komunikačných a riadiacich systémov a v prípade kybernetického útoku môže spôsobiť aj ohrozenie vybranej časti, alebo celého kybernetického priestoru. Konkrétne sem možno zaradiť základné bezpečnostné oblasti fungovania štátu, ako sú bezpečnostné záujmy SR v zahraničnej a obrannej politike, ochrana ústavného zriadenia, verejného poriadku, bezpečnosť občana a štátu, sociálna a ekonomická stabilita štátu, ochrana životného prostredia.[9]

2. Priestupky podľa ZoKB

V oblasti kybernetickej bezpečnosti môže dochádzať k protiprávnym konaniam zo strany subjektov určených v ZoKB a následne je možné na základe tohto zákona vyvodiť voči takýmto subjektom administratívnoprávnu zodpovednosť.

[8] ANDRAŠKO, J. a kol. *Zákon o kybernetickej bezpečnosti. Komentár*. Bratislava: Wolters Kluwer s.r.o., 2018. s. 96.
[9] Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020 [Online]. 2015, s. 7. [cit. 2020-11-06]. Dostupné na internete: https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Koncepcia-kybernetickej-bezpecnosti-SR-na-roky-2015-2020-A4.pdf

ZoKB vymedzuje skutkové podstaty, sankcie a vecnú príslušnosť na prejednanie priestupkov v oblasti kybernetickej bezpečnosti v § 30. ZoKB v § 30 ods. 3 a 5 upravuje, že na priestupky a ich prejednávanie sa vzťahuje zákon č. 372/1990 Zb. o priestupkoch a o zmene a doplnení niektorých zákonov (ďalej len „ZoP"), a že pokuty za priestupky sú príjmom štátneho rozpočtu. Tieto ustanovenia sú z legislatívno-technického hľadiska nadbytočné, pretože vyplývajú priamo aj zo ZoP, v ktorom je rovnaké znenie ustanovení uvedené v § 13 ods. 3 a § 51.[10]

ZoKB definuje skutkové podstaty jednotlivých priestupkov, ktorých sa môže dopustiť podľa tohto zákona len fyzická osoba. Pre porovnanie, páchateľom priestupkov v zmysle ZoP môže byť jedine fyzická osoba a nie právnická osoba, čo nepriamo vyplýva z § 5 ZoP.[11] Páchateľom môže byť len fyzická osoba, keďže pojmy dovŕšenia veku a nepríčetnosti nie je možné právnickej osobe pričítať. Fyzická osoba musí naplniť všetky znaky skutkovej podstaty priestupku a tiež byť priestupkovo, resp. deliktuálne zodpovedná. Vznik tejto zodpovednosti je podľa ZoP viazaný na dovŕšenie pätnásteho roku veku. Vo všeobecnosti teda môžeme hovoriť o tzv. všeobecnom subjekte priestupku.[12]

V analyzovanom ustanovení § 30 ZoKB však môžeme vidieť, že nepôjde o všeobecný subjekt priestupku, nakoľko z uvedeného ustanovenia nepriamo vyplýva, že fyzická osoba musí splniť ďalšie podmienky, na to aby jej vznikla priestupková zodpovednosť. Na tomto mieste je vhodné preto uviesť, že okrem všeobecného subjektu priestupku rozoznávame aj tzv. osobitný (špeciálny) subjekt priestupku. Špeciálny subjekt priestupku sa vyznačuje tým, že páchateľom nemôže byť ktokoľvek, ale iba taká fyzická osoba, ktorá spĺňa ešte ďalšie osobitné vlastnosti.[13]

V § 30 písm. a) ZoKB sa chráni povinnosť mlčanlivosti, ktorá súvisí so zachovávaním kybernetickej bezpečnosti. Pri naplnení objektívnej stránky dochádza k tomu, že táto mlčanlivosť bola porušená a mohlo dôjsť k vyzradeniu skutočností, ktoré mohli narušiť kybernetickú bezpečnosť. Nie je tu právne relevantné, akým spôsobom došlo k porušeniu mlčanlivosti a aký dôsledok porušenie malo (či došlo iba k ohrozeniu alebo až k porušeniu kybernetickej bezpečnosti).[14] Povinnosť zachovávať mlčanlivosť trvá aj po skončení dohody o

[10] HORVAT, M. In ANDRAŠKO, J. a kol. *Vybrané kapitoly práva informačných technológií II.* Bratislava: Právnická fakulta UK, 2020. s. 95.
[11] Zo zákona: *„Za priestupok nie je zodpovedný ten, kto v čase jeho spáchania nedovŕšil pätnásty rok svojho veku."* Pozri § 5 ods. 1 ZoP.
[12] HORVAT, M. In SREBALOVÁ, M. a kol. *Zákon o priestupkoch. Komentár.* Bratislava: C. H. Beck, 2015.
[13] HORVAT, M. In SREBALOVÁ, M. a kol. *Zákon o priestupkoch. Komentár.* Bratislava: C. H. Beck, 2015.
[14] HORVAT, M. In ANDRAŠKO, J. a kol. *Vybrané kapitoly práva informačných technológií II.* Bratislava: Právnická fakulta UK, 2020. s. 95.

spolupráci podľa § 5 ods. 3 ZoKB[15], pracovnoprávneho vzťahu alebo obdobného pracovného vzťahu vrátane služobného pomeru.[16] Z uvedeného vyplýva, že priestupkovo zodpovednou osobou bude len tá osoba, ktorá je v pracovnoprávnom vzťahu alebo v obdobnom pracovnom vzťahu vrátane služobného pomeru k NBÚ, alebo má uzatvorenú dohodu o spolupráci s NBÚ. V tomto prípade musí NBÚ pri vyvodzovaní zodpovednosti skúmať, či tu tento vzťah existoval a existuje.[17]

Nositeľmi tejto povinnosti budú najmä zamestnanci NBÚ, resp. pracovníci kontroly, kontrolovaných subjektov, prevádzkovateľov základných a digitálnych služieb. Okrem toho táto povinnosť dopadá aj na toho, kto uzatvoril s NBÚ písomnú dohodu o spolupráci podľa § 5 ods. 2 ZoKB.[18] Pre doplnenie je možno uviesť, že k naplneniu skutkovej podstaty nemôže dôjsť, ak boli vyzradené skutočnosti, ktoré boli už verejne známe.[19]

Skutkové podstaty priestupkov uvedených v § 30 písm. b) až e) ZoKB sú vymedzené konkrétnymi povinnosťami, ktorých porušenie sa považuje za protiprávne. Pôjde o prípady, keď fyzická osoba poskytne nepravdivé údaje v oznámení podľa § 17 ods. 5, poruší niektorú z povinností podľa § 19 ods. 1 až 4, 6 alebo ods. 7, neprijme bezpečnostnú dokumentáciu podľa § 20 ods. 5 ZoKB a keď nepostupovala v súlade s technickými, organizačnými alebo personálnymi opatreniami prijatými prevádzkovateľom základnej služby, pričom sa predpokladá, že takéto opatrenia musia byť podľa § 20 ods. 1 ZoKB prijaté.

Vo všetkých prípadoch platí, že subjektom je prevádzkovateľ základnej služby. Prevádzkovateľom základnej služby je orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu službu.[20] Takouto službou je podľa § 3 písm. k) ZoKB základná služba, ktorá je zaradená v zozname základných služieb a

1. závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1 k ZoKB[21],

[15] Zo zákona: *„Na účely zabezpečenia plnenia úloh podľa tohto zákona môže úrad uzatvoriť písomnú dohodu o spolupráci s fyzickou osobou.“* Pozri § 5 ods. 3 ZoKB.
[16] Pozri § 12 ods. 1 ZoKB.
[17] HORVAT, M. In ANDRAŠKO, J. a kol. *Vybrané kapitoly práva informačných technológií II.* Bratislava: Právnická fakulta UK, 2020. s. 95.
[18] GÁBRIŠ,T. In ANDRAŠKO, J. a kol. *Zákon o kybernetickej bezpečnosti. Komentár.* Bratislava: Wolters Kluwer s.r.o., 2018. s. 365.
[19] Pozri § 12 ods. 1 ZoKB.
[20] Pozri § 3 písm. l) ZoKB.
[21] Príloha č. 1 k ZoKB vymedzuje sektory: bankovníctvo, doprava, digitálna infraštruktúra, elektronické komunikácie, energetika, infraštruktúra finančných trhov, pošta, priemysel, voda a atmosféra, verejná správa a zdravotníctvo.

2. je informačným systémom verejnej správy[22], alebo
3. je prvkom kritickej infraštruktúry.[23]

Problematickým sa javí najmä tá skutočnosť, že tento špeciálny subjekt bude zodpovedať podľa tohto ustanovenia len vtedy, ak bude prevádzkovateľom v podobe fyzickej osoby a nie právnickej osoby (čo zrejme v praxi nenastane). Výklad tohto ustanovenia potom môže viesť aj k tomu, že zodpovedať bude konkrétna fyzická osoba (pravdepodobne zamestnanec prevádzkovateľa), ktorá bola v mene prevádzkovateľa povinná zabezpečovať plnenie daných povinností. Zistenie páchateľa môže byť v praxi problematické, a to najmä v prípadoch, ak pôjde o zložitú organizačnú štruktúru toho-ktorého prevádzkovateľa. Bližšie podrobnosti k výkladu týchto ustanovení neposkytuje ani dôvodová správa k ZoKB.[24]

Vecne príslušným orgánom na prejednanie daných priestupkov je NBÚ[25], ktorý môže za spáchané priestupky uložiť pokutu od 100 eur do 5 000 eur.[26] Pri určení výmery pokuty sa prihliadne na závažnosť priestupku, najmä na spôsob jeho spáchania a na jeho následky, na okolnosti, za ktorých bol spáchaný, na mieru zavinenia, na pohnútky a na osobu páchateľa, ako aj na to, či a akým spôsobom bol za ten istý skutok postihnutý v disciplinárnom konaní.[27]

Vzhľadom na subsidiárne použitie ZoP je možné páchateľovi uložiť aj sankciu prepadnutia veci, a to v prípade, ak je zachovaná proporcionalita medzi jej hodnotou a povahou priestupku. Ak by bola v nápadnom nepomere k povahe priestupku, nemožno túto sankciu uložiť.[28]

Sankcie zákazu činnosti a pokarhania podľa § 11 ods. 1 ZoP nie je možné páchateľovi priestupkov uložiť. Sankciu zákazu činnosti je možné uložiť len za priestupky uvedené

---

[22] Zo zákona: *„Informačným systémom je na účely tohto zákona funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických prostriedkov a programových prostriedkov."* Pozri § 2 ods. 2 zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ITVS"). Zákon o ITVS je všeobecným právnym predpisom, ktorý nadobudol účinnosť dňa 1. mája 2019, a ktorým sa zrušuje zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších právnych predpisov.

[23] Zo zákona: *„Prvkom kritickej infraštruktúry sa na účely zákona rozumie najmä inžinierska stavba, služba vo verejnom záujme a informačný systém v sektore kritickej infraštruktúry, ktorých narušenie alebo zničenie by malo podľa sektorových kritérií a prierezových kritérií závažné nepriaznivé dôsledky na uskutočňovanie hospodárskej a sociálnej funkcie štátu, a tým na kvalitu života obyvateľov z hľadiska ochrany ich života, zdravia, bezpečnosti, majetku, ako aj životného prostredia."* Pozri § 2 písm. a) zákona č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších predpisov.

[24] ANDRAŠKO, J. a kol. *Zákon o kybernetickej bezpečnosti. Komentár.* Bratislava: Wolters Kluwer s.r.o., 2018. s. 490.

[25] Pozri § 30 ods. 4 ZoKB.

[26] Pozri § 30 ods. 2 ZoKB.

[27] Pozri § 12 ods. 1 ZoP.

[28] HORVAT, M. In ANDRAŠKO, J. a kol. *Vybrané kapitoly práva informačných technológií II.* Bratislava: Právnická fakulta UK, 2020. s. 96.

v osobitnej časti ZoP alebo v inom zákone a na čas v nich ustanovený.[29] ZoKB priamo neumožňuje uložiť tento druh sankcie. Rovnako nemožno uložiť za spáchané priestupky ani pokarhanie, nakoľko ho nie je možné uložiť spolu s pokutou.[30]

3. Správne delikty podľa ZoKB

ZoKB upravuje správne delikty v § 31. Možno povedať, že v tomto prípade tu ide o správne delikty právnických osôb a podnikajúcich fyzických osôb[31], pretože sa od iných druhov správnych deliktov odlišujú špecificky vymedzeným subjektom a subjektívnou stránkou.[32] V uvedenom ustanovení môžeme badať ešte jeden druh správneho deliktu, a to, iný správny delikt fyzickej osoby, samozrejme, ak to okolnosti pripustia. V praxi však ako subjekt deliktu budú vystupovať primárne právnické osoby[33], a to aj v prípade § 31 ods. 5 ZoKB.[34]

V prvých piatich odsekoch ZoKB vymedzuje skutkové podstaty správnych deliktov. Subjektom správneho deliktu podľa odseku 1 a 2 je prevádzkovateľ základnej služby. Objektívna stránka skutkovej podstaty správneho deliktu vymedzeného v § 31 ods. 1 ZoKB spočíva v porušení povinnosti podľa § 19 ods. 2 až 4 alebo ods. 7[35] alebo v porušení povinnosti udržiavať bezpečnostnú dokumentáciu aktuálnu a zodpovedajúcu reálnemu stavu podľa § 20 ods. 5 ZoKB.[36]

---

[29] Pozri § 14 ods. 1 ZoP.
[30] Pozri § 11 ods. 2 ZoP.
[31] Inak nazývané aj zmiešané správne delikty.
[32] HAMUĽÁKOVÁ, Z. In VRABKO, M. a kol. 2018. *Správne právo hmotné. Všeobecná časť*. 2. vyd. Bratislava: C.H. Beck, s.234.
[33] HORVAT, M. In ANDRAŠKO, J. a kol. *Vybrané kapitoly práva informačných technológií II.* Bratislava: Právnická fakulta UK, 2020. s. 97.
[34] Zo zákona: *„Úrad uloží pokutu od 300 eur do 100 000 eur tomu, kto na výzvu úradu neposkytne informácie podľa § 7 ods. 3.“* Pozri § 31 ods. 5 ZoKB.
[35] Prevádzkovateľ základnej služby je povinný uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností. Prevádzkovateľ základnej služby je povinný dňom zaradenia do registra prevádzkovateľov základných služieb o tejto skutočnosti informovať podnik na poskytovanie elektronických komunikačných služieb alebo sietí podľa osobitného predpisu, ku ktorému je sieť alebo informačný systém základnej služby pripojená. Prevádzkovateľ základnej služby je povinný informovať v nevyhnutnom rozsahu tretiu stranu o hlásenom kybernetickom bezpečnostnom incidente za predpokladu, že by sa plnenie zmluvy podľa odseku 2 stalo nemožným, ak úrad nerozhodne inak. Prevádzkovateľ základnej služby je povinný hlásiť zmeny v údajoch podľa § 17 ods. 5 do 30 dní odo dňa ich vzniku prostredníctvom jednotného informačného systému kybernetickej bezpečnosti. Pozri § 19 ods. 2 - 4, 7 ZoKB.
[36] NBÚ môže v týchto prípadoch uložiť pokutu od 300 eur do 30 000 eur prevádzkovateľovi základnej služby. Pozri § 31 ods. 1 ZoKB.

V prípade § 31 ods. 2 ZoKB spočíva objektívna stránka v porušení povinnosti: oznamovacej podľa § 17 ods. 1, dodržiavať všeobecné bezpečnostné opatrenia podľa § 19 ods. 1, riešiť a bezodkladne hlásiť kybernetický bezpečnostný incident, spolupracovať s NBÚ a ústredným orgánom pri riešení hláseného kybernetického bezpečnostného incidentu, poskytnúť potrebnú súčinnosť a informácie získané z vlastnej činnosti, v čase kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní, oznámiť orgánu činnému v trestnom konaní alebo Policajnému zboru skutočnosti, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka, ak sa o ňom hodnoverným spôsobom dozvie podľa § 19 ods. 6.[37]

Pri analýze týchto ustanovení vo vzťahu k § 30 ZoKB možno dospieť k záveru, že ak by boli porušené tieto povinnosti fyzickou osobou, tá by sa dopustila priestupku, a ak by boli porušené právnickou osobou, išlo by o správny delikt podľa § 31 ZoKB. O dvojitom postihu tu nemožno hovoriť, keďže by išlo o rozdielne subjekty, ktoré je možné postihnúť súbežne. Vo veci by nemohlo byť uskutočnené ani spoločné konanie.[38]

Subjektom správneho deliktu podľa § 31 ods. 3 ZoKB je poskytovateľ digitálnej služby, ktorý sa dopustí správneho deliktu tým, že poruší povinnosť podľa § 21 ods. 5, § 22 ods. 4 alebo § 23 ods. 2. NBÚ v tomto prípade uloží pokutu od 300 eur do 30 000 eur. Rovnaký špeciálny subjekt je vymedzený aj v § 31 ods. 4 ZoKB, ktorému môže NBÚ uložiť pokutu od 300 eur až do výšky 1 % celkového ročného obratu za predchádzajúci účtovný rok, najviac však 300 000 eur, ak poruší povinnosť podľa § 21 ods. 1, § 22 ods. 3, § 24 ods. 3, § 25 ods. 1 alebo ods. 2 alebo povinnosť vykonať reaktívne opatrenie na základe rozhodnutia úradu podľa § 27 ods. 5.

[37] Medzi ďalšie povinnosti možno zaradiť: prijať bezpečnostnú dokumentáciu podľa § 20 ods. 5, nahlásiť závažný kybernetický bezpečnostný incident podľa § 24 ods. 1 alebo odoslať neúplné hlásenie podľa § 24 ods. 5, riešiť kybernetický bezpečnostný incident na základe rozhodnutia NBÚ podľa § 27 ods. 3, vykonať reaktívne opatrenie na základe rozhodnutia NBÚ podľa § 27 ods. 5 alebo oznámiť a preukázať vykonanie reaktívneho opatrenia a jeho výsledok podľa § 27 ods. 6, predložiť ochranné opatrenie na schválenie alebo vykonať schválené ochranné opatrenie podľa § 27 ods. 8, povinnosť preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených ZoKB vykonaním auditu kybernetickej bezpečnosti do dvoch rokov odo dňa zaradenia prevádzkovateľa základnej služby do registra prevádzkovateľov základných služieb, a to v rozsahu stanovenom podľa všeobecne záväzného právneho predpisu podľa § 29 ods. 1 a 2, povinnosť predložiť záverečnú správu o výsledkoch auditu úradu spolu s opatreniami na nápravu a s lehotami na ich odstránenie do 30 dní od ukončenia auditu podľa § 29 ods. 4, vykonať opatrenie na nápravu v lehote podľa záverečnej správy o výsledkoch auditu podľa § 29. NBÚ môže v týchto prípadoch uložiť pokutu prevádzkovateľovi základnej služby od 300 eur až do výšky 1 % celkového ročného obratu za predchádzajúci účtovný rok, najviac však 300 000 eur. Pozri § 31 ods. 2 ZoKB.

[38] HORVAT, M. In ANDRAŠKO, J. a kol. *Vybrané kapitoly práva informačných technológií II.* Bratislava: Právnická fakulta UK, 2020. s. 97.

Subjektom podľa § 31 ods. 5 ZoKB sú v spojení s § 7 ods. 3 ZoKB[39] ústredné orgány a iné orgány štátnej správy, tak ako sú vymedzené v § 4 ZoKB. Ak tieto orgány neposkytnú na výzvu NBÚ informácie, tak im môže byť uložená sankcia pokuty vymedzená minimálnou sadzbou 300 eur a maximálnou výškou 100 000 eur.[40]

Vo všetkých prípadoch uvedených správnych deliktov ide o porušovacie správne delikty, t. j. ak dôjde len k ohrozeniu objektu chráneného skutkovou podstatou, tak ešte nemožno hovoriť o dokonaní správneho deliktu.[41] Takisto, na prejednanie týchto správnych deliktov je vecne príslušným NBÚ.

ZoKB v § 31 ods. 7[42] upravuje otázku recidívy, v prípade ktorej dochádza k sprísneniu pokút. Za recidívu sa považuje len spáchanie toho istého deliktu porušením tej istej povinnosti.[43] V tomto prípade je dôležité, kedy došlo k opätovnému porušeniu povinnosti, t. j. kedy došlo k dokonaniu správneho deliktu, a nie kedy nadobudne právoplatnosť rozhodnutie o uznaní viny a uložení pokuty.[44]

Pri ukladaní pokuty za správny delikt úrad prihliadne na závažnosť správneho deliktu, najmä na spôsob jeho spáchania, trvanie, následky a na okolnosti, za ktorých bol spáchaný.[45]

Čo sa týka určenia výšky pokuty v rámci určeného rozpätia, tak to je vecou voľného uváženia správneho orgánu, neznamená to však, že môže byť uložená v ľubovoľnej výške. Voľná úvaha aj pri takomto rozhodovaní je myšlienkový proces, v rámci ktorého má príslušný orgán zvažovať závažnosť porušenia predpisov vo vzťahu ku každému zisteniu, jeho následky, dobu protiprávnosti, aby uložená pokuta spĺňala nielen požiadavku represie, ale aj preventívny účel s prognózou budúceho pozitívneho správania sa dotknutej osoby.[46]

---

[39] Zo zákona: *„Ústredný orgán a iný orgán štátnej správy spolupracujú s úradom na vypracovaní národnej stratégie kybernetickej bezpečnosti a na tento účel sú povinné poskytnúť mu informácie v potrebnom rozsahu.“* Pozri § 7 ods. 3 ZoKB.
[40] Pozri § 31 ods. 5 ZoKB.
[41] HORVAT, M. In ANDRAŠKO, J. a kol. *Vybrané kapitoly práva informačných technológií II.* Bratislava: Právnická fakulta UK, 2020. s. 97.
[42] Zo zákona: *„NBÚ uloží pokutu až do dvojnásobku výšky súm uvedených alebo vypočítaných podľa odsekov 1 až 6, ak do jedného roka odo dňa nadobudnutia právoplatnosti rozhodnutia o uložení pokuty dôjde k opätovnému porušeniu povinností, za ktoré bola pokuta uložená.“* Pozri § 31 ods. 7 ZoKB.
[43] HORVAT, M. In ANDRAŠKO, J. a kol. *Vybrané kapitoly práva informačných technológií II.* Bratislava: Právnická fakulta UK, 2020. s. 99.
[44] HORVAT, M. In ANDRAŠKO, J. a kol. *Vybrané kapitoly práva informačných technológií II.* Bratislava: Právnická fakulta UK, 2020. s. 99.
[45] Pozri § 31 ods. 6 ZoKB.
[46] Rozsudok Najvyššieho súdu Slovenskej republiky sp. zn. 2Sžp/16/2011.

ZoKB určuje subjektívnu a objektívnu lehotu na vyvodenie zodpovednosti.[47] Subjektívna lehota je ustanovená ako dvojročná a začína plynúť od subjektívneho okamihu, ktorým je zistenie NBÚ, že došlo s porušeniu povinnosti. Objektívna lehota je ustanovená ako štvorročná a počíta sa od objektívneho okamihu, ktorým je deň, kedy reálne došlo k porušeniu povinnosti, ktorá zakladá skutkovú podstatu podľa § 30 ods. 1 až 5 ZoKB. Pre doplnenie možno uviesť, že plynutie subjektívnej lehoty je možné len v rámci lehoty objektívnej, a teda subjektívna lehota nesmie nikdy presiahnuť objektívnu. [48]V týchto lehotách musí rozhodnutie o vine a uloženej pokute nadobudnúť právoplatnosť, nepostačuje, že sa konanie začalo alebo, že bolo rozhodnutie len vydané v tejto lehote.[49]

Pre porovnanie, v ZoP je stanovená len objektívna lehota, ktorá je vyjadrená v § 20 ods. 1 ZoP, kedy priestupok nemožno prejednať, ak od jeho spáchania uplynuli dva roky.

Pokuta za správny delikt je splatná do 30 dní odo dňa nadobudnutia právoplatnosti rozhodnutia o jej uložení a je príjmom štátneho rozpočtu.[50]

Záver

Kybernetickú bezpečnosť môžeme charakterizovať ako stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje spracúvané údaje alebo služby poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov. Tiež je definovaná ako určité zachovanie dôvernosti, integrity a dostupnosti informácií v kybernetickom priestore. Pojem kybernetický priestor možno zjednodušene definovať ako virtuálny systém informácií, vzťahov, činností, ktoré vznikajú pri spracovaní informácií prostredníctvom digitálnych informačných a komunikačných technológií, ktorý však neexistuje v materiálnej forme.

Aj v oblasti kybernetickej bezpečnosti môže dochádzať k protiprávnym konaniam zo strany subjektov vymedzených v ZoKB a následne je možné na základe tohto zákona vyvodiť voči takýmto subjektom administratívnoprávnu zodpovednosť.

---

[47] Zo zákona: *„Pokutu za správny delikt možno uložiť do dvoch rokov odo dňa zistenia porušenia povinnosti, najneskôr však do štyroch rokov odo dňa, keď k porušeniu povinnosti došlo.“* Pozri § 31 ods. 10 ZoKB.
[48] HORVAT, M. In ANDRAŠKO, J. a kol. *Vybrané kapitoly práva informačných technológií II.* Bratislava: Právnická fakulta UK, 2020. s. 100.
[49] HORVAT, M. In ANDRAŠKO, J. a kol. *Vybrané kapitoly práva informačných technológií II.* Bratislava: Právnická fakulta UK, 2020. s. 100.
[50] Pozri § 31 ods. 11 a 12 ZoKB.

ZoKB v § 30 vymedzuje skutkové podstaty konkrétnymi povinnosťami, ktorých porušenie je považované za protiprávne, sankcie a vecnú príslušnosť na prejednanie priestupkov v oblasti kybernetickej bezpečnosti. Skutkové podstaty správnych deliktov sú vymedzené v § 31 ZoKB a sú upravené formou odkazovej metódy. Odkazovacie normy určujú, porušenie ktorých povinností so sebou nesie spáchanie správneho deliktu v oblasti kybernetickej bezpečnosti. Pri oboch typoch deliktov tu vystupuje špeciálny subjekt, ktorý sa vyznačuje jeho osobitnou spôsobilosťou, ktorá je viazaná na podmienky uvedené v ZoKB. Konkrétne pôjde o subjekty, ktorými sú osoby, ktoré sa nachádzajú v pracovnoprávnom vzťahu alebo v obdobnom pracovnom vzťahu vrátane služobného pomeru k NBÚ alebo majú uzatvorenú dohodu o spolupráci s NBÚ, prevádzkovateľov základnej služby, poskytovateľov digitálnej služby, ústredné orgány štátnej správy a iné orgány štátnej správy (tak ako sú vymedzené na účely ZoKB).

Problematickým sa môže javiť v prípade priestupkov najmä tá skutočnosť, že špeciálny subjekt bude priestupkovo zodpovedný len vtedy, ak bude prevádzkovateľom v podobe fyzickej osoby a nie právnickej osoby (čo zrejme v praxi nenastane). Na tomto mieste tu môže dôjsť k situácii, že zodpovedať bude konkrétna fyzická osoba (pravdepodobne zamestnanec prevádzkovateľa), ktorá bola v mene prevádzkovateľa povinná zabezpečovať plnenie daných povinností. Zistenie páchateľa preto v praxi môže byť problematické, a to najmä v prípadoch, ak pôjde o zložitú organizačnú štruktúru toho-ktorého prevádzkovateľa.

Na záver je potrebné ešte uviesť, že za všetky uvedené delikty je možné uložiť pokuty v rozpätí určenom ZoKB, s tým, že pri priestupkoch je možné uložiť aj sankciu prepadnutia veci. Vecne príslušným orgánom na prejednanie priestupkov a správnych deliktov je NBÚ.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

Monografie a učebnice

ANDRAŠKO, J. a kol. *Zákon o kybernetickej bezpečnosti. Komentár.* Bratislava: Wolters Kluwer s.r.o., 2018. 548 s. ISBN 978-80-8168-905-5.

ANDRAŠKO, J. a kol. *Vybrané kapitoly práva informačných technológií II.* 1. vyd. Bratislava: Právnická fakulta UK, 2020. 101 s. ISBN 978-80-7160-539-3.

SREBALOVÁ, M. a kol. *Zákon o priestupkoch. Komentár.* 1. vyd. Bratislava: C. H. Beck, 2015. 484 s. ISBN 978-80-89603-30-5.
VRABKO, M. a kol. 2018. *Správne právo hmotné. Všeobecná časť*. 2. vyd. Bratislava: C.H. Beck, 338 s. ISBN 978-80-89603-68-8.

Právne predpisy

Zákon č. 372/1990 Zb. o priestupkoch a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
Zákon č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších predpisov.
Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Judikatúra

Rozsudok Najvyššieho súdu Slovenskej republiky sp. zn. 2Sžp/16/2011.

Internetové zdroje

ANDRAŠKO, J. Bezpečnosť informačných systémov verejnej správy vo svetle zákona o kybernetickej bezpečnosti a zákona o informačných technológiách vo verejnej správe. In: *Revue pro právo a technologie*. [Online]. 2019, č. 20, s. 3-40. [cit. 2020-10-29] Dostupné na internete: https://journals.muni.cz/revue/article/view/12536.
Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020 [Online]. 2015, 33 s. [cit. 2020-11-06] Dostupné na internete: https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Koncepcia-kybernetickej-bezpecnosti-SR-na-roky-2015-2020-A4.pdf.

Ostatné

ISO/IEC 27032:2012 Information technology - Security techniques - Guidelines for cybersecurity.
ISO/IEC Guide 2:2004 Standardization and related activities - General vocabulary.