Univerzita Komenského v Bratislave
Právnická fakulta

Učebnica

Vybrané kapitoly práva informačných technológií II

Jozef Andraško
Matej Horvat
Matúš Mesarčík

VYBRANÉ KAPITOLY PRÁVA INFORMAČNÝCH TECHNOLÓGIÍ II
Učebnica

Vypracovali: JUDr. Jozef Andraško, PhD.
doc. JUDr. Matej Horvat, PhD.
JUDr. Matúš Mesarčík, LL.M

Recenzenti: Mgr. Martin Daňko, PhD.
Mgr. Rastislav Munk, PhD.

Vybrané kapitoly práva informačných technológií I. Jozef Andraško – Matej Horvat – Matúš Mesarčík. 1. vyd. – Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2020, 101 strán.

ISBN: 978-80-7160-539-3
EAN: 9788071605393
- Právo informačných a komunikačných technológií
- Správne právo

Za odbornú a jazykovú stránku zodpovedajú autori. Rukopis neprešiel jazykovou úpravou.

Vydavateľ: © Univerzita Komenského v Bratislave, Právnická fakulta, 2020

ISBN: 978-80-7160-539-3

Táto učebnica bola vydaná v rámci riešenia rozvojového projektu MŠVVaŠ SR č. 002UK-2-1/2018 - Vzdelávanie pre informačnú spoločnosť.

JEDNOTLIVÉ ČASTI SPRACOVALI

JUDr. Jozef Andraško, PhD.	Úvodné poznámky, Kapitola 1 a 2 (okrem 2.5)
doc. JUDr. Matej Horvat, PhD.	Kapitola 3
JUDr. Matúš Mesarčík, LL.M	Kapitola 2.5

OBSAH

O AUTOROCH 7

ÚVOD 8

Úvodné poznámky..... 9

KAPITOLA 1 TEORETICKÝ ZÁKLAD – INFORMAČNÁ A KYBERNETICKÁ BEZPEČNOSŤ. 11

1.1 Informačná bezpečnosť – pojem 11

1.2 Základy informačnej bezpečnosti 13

1.3 Základné bezpečnostné požiadavky na ochranu informácií a systémov..... 16

1.4 Kybernetická bezpečnosť - pojem..... 18

1.4.1 Vzťah kybernetickej bezpečnosti s inými oblasťami bezpečnosti..... 24

1.4.2 Rozdiel medzi informačnou a kybernetickou bezpečnosťou..... 27

KAPITOLA 2 PRÁVNA ÚPRAVA INFORMAČNEJ A KYBERNETICKEJ BEZPEČNOSTI 28

2.1 Európska únia..... 28

2.1.1 Právne nezáväzné akty..... 28

2.1.2 Legislatívne akty..... 29

2.2 Smernica NIS..... 29

2.3 Akt o kybernetickej bezpečnosti..... 32

2.4 Nariadenie eIDAS 33

2.4.1 Bezpečnosť v zmysle článku 10 Nariadenia eIDAS..... 34

2.5 Všeobecné nariadenie o ochrane údajov 35

2.5.1 Úvodné poznámky..... 35

2.5.2 Všeobecná klauzula bezpečnosti v GDPR..... 35

2.5.3 Porušenie ochrany osobných údajov..... 37

2.5.4 Prax dozorných orgánov v Slovenskej republike a v EÚ 39

2.5.5 Špecifiká požiadaviek na bezpečnosť pri implementácií Policajnej smernice..... 40

2.6 Smernica PSD 2..... 43

2.7 Návrh nariadenia o súkromí a elektronických komunikáciách 44

2.7.1 Pôsobnosť návrhu nariadenia o súkromí a elektronických komunikáciách 45

2.8 Národná úroveň..... 47

2.8.1 Právne nezáväzné akty..... 47

Národná stratégia pre informačnú bezpečnosť SR 47

Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020..... 47

2.8.2 Legislatívne akty..... 50

2.8.2.1 Zákon o kybernetickej bezpečnosti..... 50

2.8.2.2 Zákon o ITVS 56
2.8.2.3 Zákon o e-Governmente 59
2.8.2.4 Zákon o dôveryhodných službách 59
2.8.2.5 Zákon o kritickej infraštruktúre 62
2.8.2.6 Zákon o elektronických komunikáciách 63
KAPITOLA 3 PRÁVNA ÚPRAVA ZODPOVEDNOSTI VO VEREJNOM PRÁVE S AKCENTOM NA POČÍTAČOVÚ KRIMINALITU A KYBERNETICKÚ BEZPEČNOSŤ 68
3.1 Úvodné poznámky o (právnej) zodpovednosti 68
3.2 Súkromnoprávna zodpovednosť a verejnoprávna zodpovednosť 73
3.2.1 Súkromnoprávna zodpovednosť 74
3.2.2 Verejnoprávna zodpovednosť 75
3.3 Súdne delikty a správne delikty 80
3.4 Trestnoprávna zodpovednosť 89
3.5 Správnoprávna zodpovednosť 94

O AUTOROCH

JUDr. Jozef Andraško, PhD., je absolventom Právnickej fakulty Univerzity Komenského v Bratislave. Témou jeho dizertačnej práce bolo Poskytovanie a využívanie elektronických služieb verejnej správy prostredníctvom informačných a komunikačných technológií. Od roku 2017 pôsobí ako odborný asistent na Ústave práva informačných technológií a práva duševného vlastníctva Právnickej fakulty Univerzity Komenského v Bratislave, kde vedie predmety ako Úvod do štúdia práva a právna informatika, Počítačové právo a IT Law. Absolvoval študijné pobyty na University of Iceland so zameraním na medzinárodné právo a na Tilburg University so zameraním na právo informačných a komunikačných technológií a právo duševného vlastníctva. V rámci výskumnej práce a publikačnej činnosti sa venuje najmä otázkam eGovernmentu, elektronickej identity, otvorených údajov, informačnej a kybernetickej bezpečnosti a umelej inteligencie. Kontakt: jozef.andrasko@flaw.uniba.sk

doc. JUDr. Matej Horvat, PhD., je absolventom Právnickej fakulty Univerzity Komenského v Bratislave, kde na Katedre správneho a environmentálneho práva obhájil dizertačnú prácu a v roku 2019 sa habilitoval na docenta v odbore 3.4.4 správne právo. V súčasnosti na tejto katedre pôsobí aj ako zástupca vedúceho katedry. Je aktívnym riešiteľom viacerých domácich aj zahraničných grantov (Vyšehradský grant, APVV, VEGA). Je autorom vedeckej monografie Administratívnoprávna zodpovednosť právnických osôb, komentára k zákonu o sťažnostiach a hlavným autorom komentára k Živnostenskému zákonu a navigátora Správny súdny poriadok v Automatizovanom systéme právnych informácií (ASPI). Spolupodieľal na tvorbe viacerých učebných textov. Vo svojej vedeckej práci sa venuje najmä správnemu trestaniu, všeobecnému správnemu konaniu a právu na prístup k informáciám. Výsledky jeho vedeckej práce boli prezentované na mnohých medzinárodných aj domácich vedeckých konferenciách. Kontakt: matej.horvat@flaw.uniba.sk

JUDr. Matúš Mesarčík, LL.M je absolventom Právnickej fakulty Univerzity Komenského v Bratislave v odbore právo (2016). V roku 2017 ukončil postgraduálne vzdelanie v odbore Právo a technológie na Tilburg University v Holandskom kráľovstve a získal titul LL.M. Je držiteľom Diplomu z anglického práva a práva Európskej únie (British Law Centre Diploma), ktorý udeľuje British Law Centre v spolupráci s University of Cambridge (Veľká Británia). V súčasnosti pôsobí ako interný doktorand v odbore správne právo na Katedre správneho a environmentálneho práva Právnickej fakulty, Univerzity Komenského v Bratislave s témou dizertačnej práce Dynamika pojmu osobný údaj vo svetle nových technológií. Takisto pôsobí v rámci Ústavu práva informačných technológií a práva duševného vlastníctva Právnickej fakulty Univerzity Komenského v Bratislave, kde okrem iných vedie semináre z predmetov Ochrana osobných údajov a Právo informačných technológií. Pravidelne publikuje v domácich a zahraničných vedeckých periodikách a zúčastňuje sa domácich a zahraničných konferencií. Poskytuje ad hoc konzultačné služby v oblasti ochrany osobných údajov. Kontakt: matus.mesarcik@flaw.uniba.sk

ÚVOD

Milí čitatelia,

do rúk sa Vám dostáva učebnica, ktorá je druhým dielom Vybraných kapitol práva informačných technológií. Táto časť sa na rozdiel od predchádzajúcej venuje vybraným otázkam bezpečnosti naprieč rôznymi právnymi predpismi. Každý z autorov má však osobitný štýl písania a techniku citovania. Z tohto dôvodu je možné nazerať na každú kapitolu ako samostatné dielo.

Z hľadiska právnych aspektov bezpečnosti sme sa snažili čitateľovi poskytnúť prierezový prehľad právnych predpisov, ktoré akýmkoľvek spôsobom reflektujú požiadavky bezpečnosti. V prvom rade je však potrebné začať vymedzením informačnej a kybernetickej bezpečnosti a poskytnúť teoretické základy riešenia danej problematiky z právneho a technického hľadiska. Nasleduje prierezová analýza otázok bezpečnosti v rôznych právnych predpisoch ako napr. nariadenie eIDAS, smernica NIS či GDPR. Záverečná kapitola je venovaná otázkam zodpovednosti vo verejnom práve s akcentom na počítačovú kriminalitu a kybernetickú bezpečnosť.

Dúfame, že predkladaná učebnica pomôže študentom, ale aj laickej verejnosti zorientovať sa v otázkach informačnej a kybernetickej bezpečnosti z právneho pohľadu.

Bratislava, 15.4.2020 *Autori*

Úvodné poznámky

Charakter ochrany informácií sa v posledných rokoch výrazne zmenil. Ešte pred niekoľkými desiatkami rokov, kedy sa informácie uchovávali väčšinou v písomnej forme a informačné systémy mali charakter papierových archívov, spoločnosť nemusela riešiť toľko otázok súvisiacich s ochranou a bezpečnosťou informácií. Zmena nastala najmä zavádzaním digitálnych informačných a komunikačných technológií (ďalej len „IKT")[1] do celej spoločnosti, vrátane verejnej správy. Pod tlakom informačnej "explózie" a prechodu od "papierovej" k elektronickej komunikácii a spracovaniu dokumentov v digitálnej podobe došlo k transformovaniu klasického uchovávania, prenosu a ochrany informácií a údajov. Od čias, kedy bola väčšina údajov uchovávaná v papierových kartotékach, kde ich bezpečnosť bola pod kontrolou, výrazne stúplo riziko zneužitia informácií. V súčasnej informačnej spoločnosti, kedy dochádza k prakticky nekontrolovateľnému pohybu veľkého množstva informácií z rozličných zdrojov je nevyhnutná primeraná ochrana a bezpečnosť informácií.

Samotná ochrana informácií a jednotlivých digitálnych IKT, v ktorých sa tieto informácie spracúvajú, ešte nemusí postačovať na zabezpečenie dostatočnej ochrany globálneho systému, **kybernetického priestoru**, ktorého prvkami sú tieto digitálne IKT.

Na digitálne IKT, informácie, ktoré sa v nich spracovávajú a činnosti, ktoré tieto IKT podporujú môžu mať negatívny vplyv/dopad rôzne udalosti, ktoré z hľadiska prevádzky IKT považujeme za bezpečnostné incidenty. Vzhľadom na charakter digitálnych IKT (prepojenosť prostredníctvom sietí) bezpečnostné incidenty nemusia mať len lokálny charakter a môžu negatívne ovplyvniť viacero subjektov. Ak dôjde k takému bezpečnostnému incidentu, je potrebné zabezpečiť, aby relevantné informácie boli zdieľané medzi zainteresovanými subjektmi a aby následné reakcie na bezpečnostný incident boli v prípade potreby koordinované.

Komplexnosť skúmanej problematiky je zvýraznená aj skutočnosťou, že informačná a kybernetická bezpečnosť majú prienik s viacerými oblasťami ako národná bezpečnosť, bezpečnosť Internetu, bezpečnosť sietí, ochrana kritickej infraštruktúry, kybernetická kriminalita, kybernetická obrana či kybernetický terorizmus. Skúmanie vzťahov medzi všetkými doménami je nad rámec tejto učebnice, avšak zodpovedanie otázky, čo je informačná a kybernetická bezpečnosť je viac ako žiaduca.

Autori si v rámci nasledujúcej kapitoly kladú za cieľ v prvom rade ozrejmiť pojmy **informačná a kybernetická bezpečnosť**, a to z pohľadu medzinárodných štandardov a odbornej literatúry.

[1] V širšom slova zmysle predstavujú IKT akýkoľvek nástroj, zariadenie alebo prostriedok, ktorý sa dá používať na spracovávanie informácie. V súčasnosti však IKT slúžia na spracovanie informácií, ktoré vznikli koncom minulého storočia spojením počítačov, telekomunikačných systémov a masovokomunikačných prostriedkov. IKT zaradzujeme do kritickej infraštruktúry spoločnosti, nakoľko sa využívajú aj na spracovanie dôležitých informácií, riadenie zložitých systémov a vykonávanie činností, od ktorých závisí riadny chod spoločnosti.

V druhej časti sa autori zamerajú na **právnu úpravu** informačnej a kybernetickej bezpečnosti z pohľadu **práva Európskej únie**, ako aj **právneho poriadku Slovenskej republiky.**

KAPITOLA 1 TEORETICKÝ ZÁKLAD – INFORMAČNÁ A KYBERNETICKÁ BEZPEČNOSŤ

Pojem informačná bezpečnosť je častokrát zamieňaný za pojem kybernetická bezpečnosť a naopak. Nejasnosť v terminológii spomínaných pojmov vychádza najmä zo skutočnosti, že predmetné pojmy sú upravené v mnohých dokumentoch, národného, ako aj medzinárodného charakteru, avšak tieto dokumenty nemajú právnu záväznosť. Nejednotnosť týchto pojmov, ktoré sú používané najmä v rôznych stratégiách, ktoré upravujú bezpečnosť v kybernetickom priestore spôsobila roztrieštenosť pohľadov na skúmané pojmy.

Pojmy informačná bezpečnosť a kybernetická bezpečnosť budeme analyzovať najmä prostredníctvom medzinárodných štandardov, ktoré túto problematiku riešia už viac než 20 rokov. Hoci štandardy nie sú právne záväzné, častokrát sa na ne legislatíva odvoláva a dávajú presnejšie formulované odpovede na otázky, ktoré súvisia informačnou a kybernetickou bezpečnosťou.

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.“*[2]

Z hľadiska orgánu, ktorý prijíma konkrétny štandard, možno štandardy rozdeliť na formálne a neformálne. Zatiaľ čo formálne štandardy boli schválené národnými[3], európskymi[4] alebo medzinárodnými štandardizačnými orgánmi[5], neformálne štandardy boli publikované organizáciami pre rozvoj štandardov, ktoré však nie sú uznané za štandardizačné orgány.[6]
Problematike informačnej bezpečnosti sa venuje viacero medzinárodných štandardov. V ďalších častiach sa zameriame na medzinárodné ISO štandardy, ako aj na diela autorov, ktorí sú považovaní za odborníkov v oblasti informačnej a kybernetickej bezpečnosti.

1.1 Informačná bezpečnosť – pojem

Informačná bezpečnosť nie je nový fenomén. Potreba uchovávať poznatky, chrániť dôverné informácie, overovať autentickosť správ existuje niekoľko tisíc rokov, ale „informačná bezpečnosť“ sa týkala pomerne úzkeho okruhu ľudí (vojakov, obchodníkov, diplomatov, politikov, sprisahancov). S objavením sa elektronických (telegraf, telefón, rádio) ale najmä neskôr digitálnych IKT však prudko

[2] ISO/IEC *Guide 2:2004 Standardization and related activities – General vocabulary*, s. 10.
[3] Zoznam národných štandardizačných orgánov dostupný na: https://standards.cen.eu/dyn/www/f?p=CENWEB:5.
[4] Medzi európske štandardizačné orgány možno zaradiť *European Committee for Standardization* (CEN), *European Committee for Electrotechnical Standardization* (CENEL) a *European Telecommunications Standards Institute* (ETSI).
[5] Medzi medzinárodné štandardizačné orgány možno zaradiť *International Organization for Standardization* (ISO), *International Electrotechnical Commission* (IEC) a *International Telegraph Union* (ITU).
[6] Napr. *American Society for Testing Materials International, Society of Automotive Engineers, Internet Engineering Task Force* a i.

vzrástol počet ľudí zainteresovaných na spracovaní a najmä využívaní informácie, a teda aj potreba zaistenia spoľahlivosti, dostupnosti, dôveryhodnosti informačných zdrojov.

Pojmu informačnej bezpečnosti predchádzali pojmy ako compusec – počítačová bezpečnosť, comsec – komunikačná bezpečnosť a množstvo iných. V osemdesiatych rokoch už bolo potrebné formalizovať požiadavky na zabezpečenie počítačov a IKT v podobe verejného štandardu a americká NSA (*National Security Agency*) vypracovala prvý štandard *Orange book* (a následne *Rainbow series*). Príklad USA nasledovali aj ďalšie informačne vyspelé krajiny, ktoré si vypracovali národné štandardy zabezpečenia informačných/počítačových systémov. Tieto štandardy boli nahradené najprv Harmonizovanými kritériami ITSEC a v polovici 90 rokov *Common Criteria* (norma ISO/IEC 15408). ISO spolu s IEC vytvorilo na štandardizáciu informatiky spoločný výbor JTC 1 a ten má podvýbor[7] ISO/IEC JTC 1/SC 27 *IT Security techniques*, ktorý zodpovedá za štandardy v oblasti informačnej a kybernetickej bezpečnosti. Podvýbor má 5 tematicky zameraných pracovných skupín, z ktorých sú pre potreby tejto kapitoly najdôležitejšie WG1 (*Information security management systems*) a WG4 (*Security controls and services*). WG1 takmer 20 rokov systematicky rieši manažment informačnej bezpečnosti a vydáva sériu medzinárodných štandardov ISO/IEC 270xx, pokrývajúcu všetky podstatné aspekty manažmentu informačnej bezpečnosti v organizácii.[8]

Prvým z tejto série je medzinárodný štandard **ISO/IEC 27000:2018 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary** (ďalej len „ISO/IEC 27000:2018") definuje **informačnú bezpečnosť** ako zachovanie dôvernosti, integrity a dostupnosti informácií. V zmysle predmetného štandardu sa za informácie považujú nielen informácie v digitálnej forme (údaje uložené na elektronických alebo optických médiách), ale aj v materiálnej forme (napr. papier).[9] Medzi informácie môžeme taktiež zaradiť informácie ako vedomosti zamestnanca. Informácie môžu byť prenášané rôznymi spôsobmi, kuriérom, elektronickou alebo verbálnou komunikáciou. Bez ohľadu na formu informácií a spôsob jej prenosu platí, že si vyžadujú dostatočnú ochranu.[10]

[7] Dostupné na: https://www.iso.org/committee/45306.html.
[8] ANDRAŠKO, J. a kol. *Zákon o kybernetickej bezpečnosti.* Komentár. Bratislava: Wolters Kluwer SR s.r.o. 2018, s. 14-35.
[9] Vo vzťahu k ochrane informácií má špecifické postavenie aj verejná správa, a to hneď z niekoľkých dôvodov. Dochádza v nej k spracúvaniu enormného množstva informácií, ktoré je porovnateľné so subjektmi súkromného sektora s celosvetovou pôsobnosťou. V porovnaní so súkromným sektorom, verejná správa v prípade nedostatočnej ochrany informácií spôsobuje škody iným subjektom, najmä štátu. Verejná správa nespracúva len svoje údaje, ale aj údaje iných subjektov, ktorých množstvo je veľmi veľké. Citlivé údaje sa uchovávajú v informačných systémoch verejnej správy, napr. Register obyvateľov SR, Matrika, Živnostenský register, Obchodný register, Kataster nehnuteľností, Register adries a i. Niektoré údaje sú v registroch verejnosti voľne prístupné, niektoré len cez kontaktné miesta, iné sú zas verejnosti neprístupné.
[10] ISO/IEC 27000:2016, s. 15.

Whitman a Mattord definujú informačnú bezpečnosť ako: *„ochranu informácií a ich kľúčových prvkov, vrátane systémov a hardvéru, ktoré používajú, uchovávajú a prenášajú túto informácie.“*[11] Kľúčovými prvkami sú v tomto prípade dôvernosť, integrita a dostupnosť informácie.[12]

Podľa Olejára sa pojem informačná bezpečnosť používa minimálne v troch významoch:[13]

1. je to ideálny stav systému alebo organizácie, ktorý sa dá charakterizovať tak, že všetko (IKT) funguje v súlade s požiadavkami (stanovenými napr. v bezpečnostnej politike) a v systéme/organizácii nedochádza k bezpečnostným incidentom;
2. označuje činnosť smerujúcu k dosiahnutiu ideálneho stavu;
3. medziodborová oblasť, ktorá skúma hrozby voči IKT a informácii a metódy eliminácie rizík, ktoré z nich vyplývajú.

Pojem	**Informačná bezpečnosť (*information security*)**
Organizácia	ISO/IEC JTC1/SC27 IT-Security Techniques
Číslo dokumentu	ISO/IEC 27000:2018
Názov dokumentu	Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
Vydané	2018
Definícia	Zachovanie dôvernosti, integrity a dostupnosti informácií.
Poznámka	V zmysle predmetného štandardu môže byť okrem dôvernosti, integrity a dostupnosti informácií zahrnutá aj autentickosť (authenticity), dosledovateľnosť (accountability), nepopretie pôvodu (non-repudiation) a spoľahlivosť (reliability).
Odkaz	https://www.iso.org/standard/73906.html

1.2 Základy informačnej bezpečnosti[14]

Vo všeobecnosti možno povedať, že **bezpečnosť** je založená na ochrane aktív pred rôznymi hrozbami pri určitej zraniteľnosti.[15] Každá organizácia[16] potrebuje pre svoje riadne fungovanie zabezpečiť ochranu svojich IKT, ako aj informácií, ktoré sa v nich spracúvajú, t. j. zabezpečiť primeranú úroveň informačnej bezpečnosti. Cieľom informačnej bezpečnosti organizácie

[11] WHITMAN, M.E. a MATTORD, H.J.: *Principles of Information security*. Boston: Course Technology, 2012, s. 9.
[12] Dôvernosť, integrita a dostupnosť informácie sú v odbornej literatúre označené ako CIA trojuholník. Skratka CIA vychádza zo začiatočných písmen anglických názvov týchto základných bezpečnostných požiadaviek (*Confidentiality, Integrity, Availability*).
[13] OLEJÁR, D. a kol.: *Manažment informačnej bezpečnosti a základy PKI*. Bratislava, 2015. s. 16. Dostupné: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html.
[14] Základy informačnej bezpečnosti vychádzajú z odbornej literatúry a jednotlivých medzinárodných ISO štandardov, ktoré sa zaoberajú informačnou bezpečnosťou.
[15] VON SOLMS, R., VAN NIEKERK, J.: *From information security to cyber security*. *In* Computers & Security, 2013, roč. 38, s. 100.
[16] V terminológii informačnej bezpečnosti je pojem organizácia definovaná ako skupina ľudí a zariadenie, so zodpovednosťou, právomocami a vzájomnými vzťahmi.

všeobecne je ochrana informácií, ako aj IKT, prostredníctvom, ktorých sa spracúvajú. Aby sme mohli definovať, čo je potrebné chrániť, zavedieme pojem **aktívum** *(asset)* organizácie. Tento pojem zahŕňa všetko, čo má pre danú organizáciu hodnotu, ktorú je nevyhnutné chrániť.[17]

Aktívami sú informácie, údaje, peniaze, majetok, dobré meno, ale aj know-how organizácie. Pri informáciách, čiže aktívach s nehmotným charakterom, budeme rozlišovať len uspokojivý a nežiaduci stav. Akákoľvek udalosť, skutočnosť, osoba, sila, ktorá môže spôsobiť, že sa aktíva organizácie dostanú do neželaného stavu, ktorý môže ohroziť bezpečnosť sa nazýva **hrozba** *(threat)*. Najčastejšími hrozbami, ktoré môžu narušiť aktíva sú prírodné vplyvy (zemetrasenie, búrka a i.), technické poruchy (výpadok siete, výpadok podpornej infraštruktúry a i.), chyby v programovom vybavení, neúmyselné ľudské chyby, cieľavedomá ľudská činnosť (sabotáž, prieniky hackerov do systému) a pod.[18]

Predpoklady, ktoré musí aktívum spĺňať, aby sa naň hrozba uplatnila, nazývame **zraniteľnosť** *(vulnerability)*. Každé aktívum je zraniteľné, nakoľko jeho hodnotu ohrozujú rôzne vplyvy. Pod zraniteľnosťou možno chápať chybu, nedostatok v podobe nedostatočne vyškoleného zamestnanca, ktorý svojou neodbornosťou a neskúsenosťou, sa môže dopúšťať chýb. Takýto nedostatok môže byť zneužitý hrozbou v takom rozsahu, že hodnota aktíva môže byť poškodená, alebo dokonca zničená.[19]

Hlavným cieľom informačnej bezpečnosti je ochrana aktív, najmä informácií a IKT, ktoré tieto informácie spracúvajú pred ujmou, ktorá môže vzniknúť z využitia zraniteľnosti (aktíva alebo organizácie) hrozbou.

Napriek tomu, že informatizácia spoločnosti má veľa pozitív, v súvislosti s ochranou informácií existujú aj negatíva. IKT sa čoraz častejšie stávajú terčom rôznych aktivít zo strany osôb, organizácií, ale aj štátov. Tieto aktivity majú za cieľ znefunkčniť, poškodiť, alebo ovládnuť IKT danej organizácie a získať nejakú výhodu, napríklad v podobe informácie. Úmyselný pokus o naplnenie

[17] OLEJÁR, D. a kol.: *Manažment informačnej bezpečnosti a základy PKI.* Bratislava, 2015. s. 7. Dostupné na: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html.
[18] OLEJÁR, D. a kol.: *Manažment informačnej bezpečnosti a základy PKI.* Bratislava, 2015. s. 7. Dostupné na: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html.
[19] POŽÁR, J.: *Informační bezpečnost.* Plzeň, Vydavatelství a nakladatelství Aleš Čeněk, 2005, s.38.

hrozby, ktorej nositeľom je človek (poškodenie údajov, prienik do systému) a výsledkom je škoda alebo strata aktív sa nazýva **útok** *(attack)*. Ten kto útok vykonáva sa označuje ako **útočník** *(attacker)*. Nie každý útok musí byť úspešný, a preto útočník musí mať dostačujúci **útočný potenciál** *(attack pottencial)*, ktorý pozostáva z motivácie, znalostí a príležitosti. Motivácia predstavuje vôľu útočníka zaútočiť na daný systém. K útoku sú potrebné znalosti o danom systéme a útočník musí mať k nemu dostatočný čas sa k nemu dostať.[20]

V prípade ak bude hrozba voči aktívu naplnená a spôsobí narušenie požadovaného stavu aktíva, dochádza k vzniku **bezpečnostného incidente** *(security incident)*. Bezpečnostný incident môže byť spôsobený aktivitou užívateľa (úmyselne, neúmyselne), alebo iným pôsobením (havária, chyba systému). Dôsledkom bezpečnostného incidentu je ujma na aktívach organizácie (nefunkčnosť aktíva, materiálne škody, finančné škody a i.). Takáto ujma sa nazýva **dopad** *(impact)*, ktorý sa dá vyjadriť kvantitatívne (finančne ako cena opravy alebo náhrady poškodeného počítača, obnova jeho programového vybavenia a údajov, a i.) alebo kvalitatívne.

Organizácia počas plnenia svojich úloh čelí mnohým bezpečnostným incidentom, či už tým vážnym, alebo menej vážnym. Nie všetky hrozby sú pre danú organizáciu opodstatnené, a preto je potrebné vytvoriť kritéria, na základe ktorých bude organizácia rozlišovať hrozby na relevantné a tie menej závažné. Takýmto kritériom je napr. dopad hrozby resp. bezpečnostného incidentu, pri ktorom došlo k naplneniu hrozby. Kritérium dopadu nie je dostačujúce, lebo existujú hrozby s katastrofickým dopadom, ktoré sa v priebehu existencie organizácie nikdy nenaplnili. Preto je potrebné si stanoviť druhé kritérium, ktorým je pravdepodobnosť naplnenia hrozby. Tieto oba kritéria sú spojené v **riziku** *(risk)*. Riziko ako miera ohrozenia konkrétneho aktíva predstavuje pravdepodobnosť, akou bude daná hodnota aktíva poškodená alebo zničená pôsobením konkrétnej hrozby.[21]

Riziká vyplývajúce z hrozieb voči aktívam organizácie nepredstavujú rovnaký bezpečnostný problém, a preto je potrebné vykonať **analýzu rizík**, ktorej výsledkom je stanovenie úrovne rizík. Následne sa riziká podľa závažnosti zoradia a rozhodne sa, ktorými rizikami sa bude organizácia zaoberať a ktorými nie. Hranica akceptovateľného rizika predstavuje pomyselnú čiaru v zozname rizík. Inými slovami, v prípade rizík, ktoré sa nachádzajú nad čiarou, musí organizácia prijať také riešenia, aby sa hodnoty daného rizika znížili. Takýmto riešením je **opatrenie** *(measures, countermeasures)*, ktoré plnia niekoľko úloh. Na jednej strane znižujú dopady bezpečnostných

[20] Pri ťažko merateľných dopadoch (napr. pri narušení reputácie) sa využíva kvalitatívne vyjadrenie dopadu bezpečnostného incidentu, a to označením nízky (ak nemá bezpečnostný incident vplyv na chod organizácie), alebo označením vysoký (organizácia nie je spôsobilá vykonávať svoje hlavné úlohy). Označenie dopadu bezpečnostného incidentu ako stredný predstavuje situáciu, kedy organizácia už pocítila dôsledky (dokáže plniť svoje primárne úlohy, ale nie v plnom rozsahu). Bližšie pozri OLEJÁR, D. a kol.: *Manažment informačnej bezpečnosti a základy PKI*. Bratislava, 2015, s. 8-9. Dostupné na: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html.

[21] POŽÁR, J.: *Informační bezpečnost*. Plzeň, Vydavatelství a nakladatelství Aleš Čeněk, 2005, s.37-38.

incidentov na aktíva, na strane druhej môžu odstraňovať zraniteľnosť aktív, čím v konečnom dôsledku znižujú pravdepodobnosť, že vôbec dôjde k bezpečnostnému incidentu. Takýmto opatrením môže byť napr. šifrovanie citlivej informácie, zálohovanie údajov a i.[22]

1.3 Základné bezpečnostné požiadavky na ochranu informácií a systémov

Aby organizácia plnila svoje úlohy, musí chrániť informácie, ktoré používa na plnenie týchto úloh. Tieto úlohy by asi ťažko mohla plniť v situáciách, kedy by sa nemohla spoľahnúť na pravdivosť informácií, alebo kedy sa citlivé údaje dostali k osobám, ktoré na to nemajú oprávnenie. Informačná bezpečnosť vychádza z niekoľkých základných bezpečnostných požiadaviek na ochranu informácií. Organizácie majú niekoľko základných požiadaviek na ochranu informácií. Konkrétne ide o nasledujúce bezpečnostné požiadavky:

a) dôvernosť
b) integrita
c) dostupnosť

Ad a) Bezpečnostná požiadavka na zaistenie **dôvernosti** informácie znamená, že informácia je chránená pred prezradením neoprávneným osobám. Príkladom informácií, ktoré si vyžadujú ochranu pred neoprávneným prístupom sú, napr. osobné údaje, informácie týkajúce sa bezpečnosti štátu a pod.[23]

Ad b) Bezpečnostná požiadavka na zaistenie **integrity** údajov znamená, že údaje[24] sú chránené pred náhodnou alebo úmyselnou modifikáciou, ktorá by mohla mať vplyv na platnosť údajov. Príkladom by mohla byť ochrana údajov v rámci transakcií, kde dochádza k platbe, kde by mohlo dôjsť k modifikácii sumy.[25]

Ad c) **Dostupnosť** informácie ako bezpečnostná požiadavka znamená, že informácie a služby, ktoré poskytujú osobám a organizáciám, musia byť dostupné používateľovi kedykoľvek, keď o to požiada. Napr. webová stránka, prostredníctvom ktorej sa osoby identifikujú a autentifikujú pre využívanie

[22] OLEJÁR, D. a kol.: *Manažment informačnej bezpečnosti a základy PKI.* Bratislava, 2015. s. 9-10. Dostupné na: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html.
[23] TODOROV, D.: *Mechanics of Users Identification and Authentication. Fundamentals of Identity Management.* USA: Auerbach Publications, 2007, s. 2.
[24] V tomto prípade je potrebné rozlišovať medzi informáciou a údajom. Ako uvádza Olejár, informácie sú obsahom údajov a údaje sú len forma zápisu informácií. To znamená, že tú istú informáciu (napr. desať) možno zapísať v rôznej forme (napr. X, ten a pod.). Bližšie pozri OLEJÁR, D. a kol.: *Manažment informačnej bezpečnosti a základy PKI.* Bratislava, 2015, s. 11. Dostupné na: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html.
[25] TODOROV, D.: *Mechanics of Users Identification and Authentication. Fundamentals of Identity Management.* USA: Auerbach Publications, 2007, s. 2.

elektronických služieb verejnej správy, musí byť dostupná kedykoľvek, ak o to daná osoba požiada. Nedostupnosť webovej stránky by narušila poskytovanie služieb.[26]

Popri vyššie uvedených bezpečnostných požiadavkách na ochranu informácií, existujú aj iné bezpečnostné požiadavky ako autentickosť, súkromnosť, anonymita, pseudonymita, nepopretie pôvodu, nepopretie doručenia, resp. v prípade ochrany systémov poznáme dosledovateľnosť.

Súkromnosť *(privacy)* predstavuje bezpečnostnú požiadavku, ktorá sa vzťahuje na osobné údaje. Je vyjadrením požiadavky, aby osoba určila, ktoré osobné údaje možno sprístupniť, komu a v akom rozsahu (napr. sprístupňovanie údajov zo zdravotnej dokumentácie vybranému okruhu osôb). Súkromnosť je slabšou bezpečnostnou požiadavkou ako dôvernosť. Pre zaistenie súkromnosti (napr. zdravotnej dokumentácie) stačí oddeliť osobné údaje o pacientovi od údajov, ktoré popisujú jeho zdravotný stav. Tým pádom by sa osoba mohla dostať k údajom o zdravotnom stave osoby, ale nedokáže určiť o koho osobné údaje ide.[27]

Autentickosť *(authenticity)* znamená, že údaje, ktoré boli poslané príjemcovi sa zhodujú s tými, ktoré poslal odosielateľ. Zaistenie autentickosti údajov sa zabezpečuje napríklad prostredníctvom digitálneho podpisu.[28]

Nepopretie pôvodu *(non repudiation of origin)* predstavuje bezpečnostnú požiadavku, na základe ktorej možno potvrdiť, že tvorca alebo odosielateľ dokument poslal a **nepopretie prijatia** *(non repudiation of receipt)* zasa, že príjemca dokument preukázateľne dostal.[29]

Významnou bezpečnostnou požiadavkou, najmä z pohľadu ochrany systémov je **dosledovateľnosť** *(accountability)*. Na základe tejto bezpečnostnej požiadavky možno určiť kto, kedy a v akom čase v systéme vykonal. Inými slovami vieme identifikovať používateľa (kto je skutočným používateľom, nakoľko ten kto bude vykonávať nekalú činnosť nevystupuje pod vlastným menom) a na základe aktivít vykonaných v systéme (napr. prihlasovanie sa do systému, modifikácia údajov atď.) možno priradiť ich pôvodcovi.[30]

Niektoré bezpečnostné požiadavky si odporujú, napríklad dostupnosť a dôvernosť, dostupnosť a súkromnosť. Polemickou je taktiež zaiste ďalšej bezpečnostnej požiadavky, **anonymity**, prostredníctvom ktorej by nebolo možné identifikovať subjekt. Na jednej strane si používateľ nepraje, aby jeho aktivity boli zaznamenané, no na strane druhej, anonymný prístup do vnútorného systému organizácie by bol privysokým rizikom. **Pseudonymita** predstavuje slabšiu

[26] Tamtiež, s. 2.
[27] OLEJÁR, D. a kol.: *Manažment informačnej bezpečnosti a základy PKI.* Bratislava, 2015. s. 11. Dostupné na: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html.
[28] Na to aby sme overili digitálny podpis potrebujeme overovací kľúč - verejný kľúč predpokladaného podpisovateľa a tvorcu zaslaného dokumentu. V prípade ak ho máme z dôveryhodného zdroja (napr. certifikát verejného kľúča vydaný dôveryhodnou certifikačnou autoritou), tak vieme bezpečne určiť kto je autorom daného dokumentu.
[29] OLEJÁR, D.a kol.: *Manažment informačnej bezpečnosti a základy PKI.* Bratislava, 2015. s. 12. Dostupné: : https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html.
[30] Tamtiež.

formu anonymity. V tomto prípade sa vyžaduje len čiastkové utajenie identity človeka, kedy je skutočná identita pred verejnosťou nahradená pseudonymom. To však neznamená, že skutočnú identitu pozná len konkrétny používateľ. Napríklad pri certifikátoch verejného kľúča, kedy si používateľ vytvorí pseudonym, skutočnú identitu držiteľa certifikátu pozná aj autorita, ktorá certifikát vydala.[31]

Bezpečnostné požiadavky majú význam najmä pri stanovení úrovne dopadu hrozby na aktívum danej organizácie. Ak chceme stanoviť dopad hrozby na aktívum, posudzujeme, aký dopad by malo narušenie dôvernosti, integrity a dostupnosti, prípadne iných bezpečnostných požiadaviek na aktívum resp. na organizáciu. Napríklad, ak je aktívom webová stránka Ministerstva vnútra Slovenskej republiky, tak už nie je potrebné aplikovať požiadavku na zachovanie dôvernosti ani súkromnosti informácie, nakoľko je obsah už verejne dostupný. V tomto prípade je potrebné aplikovať jednak bezpečnostnú požiadavku zaistenia integrity, nakoľko mohli byť modifikované údaje, ako aj bezpečnostnú požiadavku dostupnosti, pretože mohol byť znemožnený prístup na stránku.

Ak by sme chceli stanoviť úroveň ochrany jednotlivých aktív, bolo by nevyhnutné pre ne vykonať analýzu rizík. Niektoré informácie a s nimi súvisiace aktíva majú stanovenú úroveň ochrany samotným zákonom. V takýchto prípadoch máme na mysli najmä informácie, ktorých narušenie by poškodilo záujmy štátu. Ide o klasifikované *(classified)* informácie, ktoré sú v našom právnom poriadku označované ako utajované skutočnosti. Tieto informácie neobsiahli všetky dôležité informácie, a preto v odbornej literatúre zavádza pojem neklasifikovaných ale citlivých informácií *(nonclassified but sensitive)*.[32]

1.4 Kybernetická bezpečnosť - pojem

Pojem kybernetická bezpečnosť je v zmysle medzinárodného štandardu **ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity** (ďalej len „ISO/IEC 27032:2012“) definovaný ako zachovanie dôvernosti, integrity a dostupnosti informácií v kybernetickom priestore.[33] V porovnaní s informačnou bezpečnosťou, pôjde teda len o informácie, ktoré sú prenášané a uložené v kybernetickom priestore. Kybernetická bezpečnosť sa vzťahuje na opatrenia, ktoré by zainteresované strany[34] mali stanoviť pre vytvorenie a zachovanie bezpečnosti v kybernetickom priestore.[35]

---

[31] Tamtiež.
[32] Tamtiež, s.13.
[33] Predmetný medzinárodný štandard odkazuje na viacerých miestach na ISO štandardy, ktoré sa aplikujú v prípade informačnej bezpečnosti.
[34] Medzi zainteresované strany v kybernetickom priestore možno zaradiť užívateľov (jednotlivci, súkromné a verejné organizácie) a poskytovateľov (poskytovatelia Internetu a poskytovatelia aplikačných služieb).
[35] ISO/IEC 27032:2012, s. 17.

V zmysle vyššie uvedenej definície by sme mohli povedať, že kybernetická bezpečnosť je informačná bezpečnosť kybernetického priestoru. Je viac ako potrebné ozrejmiť pojem **kybernetický priestor** *(cyberspace)*, ktorý je spätý s pojmom kybernetická bezpečnosť.

Neexistuje 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 IKT, ktorý však neexistuje v materiálnej forme.[36]

V zmysle medzinárodného štandardu ISO/IEC 27032:2012 predstavuje kybernetický priestor komplexné prostredie, ktoré vzniklo interakciou ľudí, softvéru a služieb na Internete prostredníctvom zariadení a sietí, technológií k nemu pripojených, ktoré neexistuje v žiadnej fyzickej podobe.[37]

Autori odbornej literatúry chápu kybernetický priestor ako geograficky neobmedzený, nefyzický priestor, v ktorom sa nezávisle od času, diaľky a miesta vykonávajú transakcie medzi ľuďmi, medzi počítačmi a medzi počítačmi a ľuďmi. Charakteristickým znakom kybernetického priestoru je nemožnosť určiť presné miesto a čas, kedy došlo k danej aktivite alebo kde došlo k presunu informácií.[38]

Hoci ISO/IEC 27032:2012 a niektorí autori odbornej literatúry chápu kybernetický priestor ako prostredie, ktoré neexistuje vo fyzickej podobe, nemožno ho chápať izolovane od jeho technologických komponentov, z ktorých je tvorený. Avšak, okrem technologickej úrovne má kybernetický priestor aj sociálno-technickú úroveň, v rámci ktorej sa vykonávajú rôzne kybernetické aktivity.[39]

Pojem kybernetický priestor *(cyberspace)* sa prvýkrát objavil v poviedke Williama Gibsona „Neuromancer" v roku 1984. Avšak je potrebné podotknúť, že slovo kybernetický, ktoré má pôvod v gréckom pojme *kyber* – riadiť, vychádza z pojmu kybernetika, ktorej zakladateľom bol Norbert Wiener. V jeho knihe „*Cybernetics: or Control and Communications in the Animal and the Machine*" (MIT

[36] Bližšie pozri: ANDRAŠKO, J. a kol.: Zákon o kybernetickej bezpečnosti. Komentár. Bratislava: Wolters Kluwer SR s.r.o. 2018, s. 96.
[37] Tamtiež, s. 12.
[38] HAMELINK, C. J: *The ethics of cyberspace*. Sage, 2001, s. 9.
[39] VAN DEN BERG, J. a kol.: *On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education*. NATO STO/IST-122 symposium, Tallinn, 13-14 október 2014, s. 12-2.

Press, 1948) používa pojem kybernetika v súvislosti s riadením komplexných systémov v ríši zvierat a v mechanických sieťach konkrétne v samoregulovaných systémoch.[40]

Pojem kybernetická bezpečnosť je definovaný v zákone č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. V zmysle § 3 písm. g) zákona o KB je kybernetická bezpečnosť[41] definovaná ako: *„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."* Predmetná definícia vychádza z pojmu bezpečnosť sietí a informačných systémov v zmysle čl. 4 ods. 2 smernice Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii.[42]

V nasledujúcich tabuľkách uvádzame definície pojmu kybernetická bezpečnosť, upravenú rôznymi organizáciami a v právnom poriadku Slovenskej republiky.

Pojem	**Kybernetická bezpečnosť *(cybersecurity)***
Organizácia	ISO/IEC JTC1/SC27 IT-Security Techniques
Číslo dokumentu	ISO/IEC 27032:2012
Názov dokumentu	Information technology—Security techniques—Guidelines for cybersecurity
Vydané	2012
Definícia	Zachovanie dôvernosti, integrity a dostupnosti informácií v kybernetickom priestore.
Poznámka	V štandarde ISO/IEC 27032:2012 sa ako synonymum kybernetickej bezpečnosti uvádza pojme bezpečnosť kybernetického priestoru. V zmysle predmetného štandardu môže byť okrem dôvernosti, integrity a dostupnosti informácií v kybernetickom priestore zahrnutá aj autentickosť *(authenticity)*, dosledovateľnosť *(accountability)*,

[40] V súčasnosti sa predpona kybernetický používa v mnohých oblastiach: kybernetický zločin *(cybercrime)*, kybernetická šikana *(cyberbullying)*, kybernetická vojna *(cyberwarfare)* a pod.

[41] Bližšie k pojmu kybernetická bezpečnosť v zmysle zákona o kybernetickej bezpečnosti pozri ANDRAŠKO, J. a kol. *Zákon o kybernetickej bezpečnosti*. Komentár. Bratislava: Wolters Kluwer SR s.r.o. 2018, s. 100-103.

[42] V zmysle predmetnej smernice sa bezpečnosť sietí a informačných systémov chápe ako: *„schopnosť sietí a informačných systémov 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."* Predmetná smernica chápe bezpečnosť sietí a informačných systémov ako vlastnosť sietí a informačných systémov, zatiaľ čo v zákone č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov je chápaná kybernetická bezpečnosť ako stav.

	nepopierateľnosť *(non-repudiation)* a spoľahlivosť *(reliability)*. Pojem kybernetická bezpečnosť vychádza z pojmu informačná bezpečnosť, ktorý je definovaný v štandarde ISO/IEC 27000:2016. Kybernetický priestor predstavuje komplexné prostredie, ktoré vzniklo interakciou ľudí, softvéru a služieb na Internete prostredníctvom zariadení a sietí, technológií k nemu pripojených, ktoré neexistuje v žiadnej fyzickej podobe.
Odkaz	https://www.iso.org/standard/44375.html

Pojem	**Kybernetická bezpečnosť *(cybersecurity)***
Organizácia	ITU-T
Číslo dokumentu	X.1205
Názov dokumentu	SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Telecommunication security Overview of cybersecurity
Vydané	2008
Definícia	Súbor nástrojov, politík, bezpečnostných konceptov, bezpečnostných záruk, smerníc, prístupov k riadeniu rizík, akcií, školení, osvedčených postupov, záruk a technológií, ktoré môžu byť použité na ochranu kybernetického priestoru a organizácie a aktív používateľov.
Poznámka	Predmetný dokument upravuje pojem kybernetické prostredie *(cyber environment)*, ktoré zahŕňa používateľov, siete, zariadenia, všetok softvér, postupy, prenášané alebo uchovávané informácie, aplikácie, služby a systémy, ktoré môžu byť spojené priamo alebo nepriamo so sieťami.
Odkaz	https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items

Pojem	**Kybernetická bezpečnosť *(cybersecurity)***
Organizácia	NIST National Institute of Standards and Technology
Číslo dokumentu	Special Publication 800-39
Názov dokumentu	Managing Information Security Risk Organization, Mission, and Information System View

Vydané	2011
Definícia	Schopnosť chrániť alebo brániť využitie kybernetického priestoru pred kybernetickými útokmi.
Poznámka	Kybernetický priestor je v zmysle predmetného dokumentu definovaný ako globálna doména v rámci informačného prostredia pozostávajúca z nezávislých sietí alebo infraštruktúr informačných systémov vrátane Internetu, telekomunikačných sietí, počítačových systémov a vstavaných procesorov a riadiacich systémov.
Odkaz	http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

Pojem	**Kybernetická bezpečnosť**
Právny predpis	Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
Účinný	1. Apríl 2018
Definícia	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.
Poznámka	V zákone č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov možno nájsť aj legálnu definíciu pojmu kybernetický priestor. Kybernetický priestor je v zmysle § 3 písm. b) predmetného zákona definovaný ako: *„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.“* Predmetná definícia má viacero nedostatkov, nakoľko medzi prvky, ktoré patria do kybernetického priestoru zaradzuje len aktivované prvky, čím vylučuje prvky, ktoré nie sú aktivované. Ako príklad neaktivovaných prvkov možno uviesť siete, počítače a zariadenia, ktoré sa nemusia dočasne používať, avšak stále sú súčasťou technologickej infraštruktúry, ktorú je potrebné chrániť. V prípade ak by sme pripustili, že kybernetická bezpečnosť sa vzťahuje len na aktívne prvky kybernetického priestoru, potom by pasívne

	komponenty prestali byť prvkami kybernetického priestoru. Takéto úvahy sú namieste najmä z dôvodu, že nová právna úprava týkajúca sa ochrany informačných technológií verejnej správy sa netýka len ISVS, ale aj infraštruktúry, ktorá zabezpečujúce implementáciu a prevádzkovanie ISVS.[43]
Odkaz	https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/20190101

V zmysle štandardu ISO/IEC 27032:2012 sa za aktíva považujú najmä:

- informácie
- softvér (počítačový program)
- fyzický majetok (počítač)
- služby
- osoby, ich kvalifikácia, zručnosti, skúsenosti
- nehmotné aktívna ako povesť a imidž.[44]

Aktíva v kybernetickom priestore sú v zmysle štandardu ISO/IEC 27032:2012 delené na **osobné**[45] a **organizačné**[46]. Pre oba druhy aktív platí, že môžu byť **fyzické**, ktoré existujú v skutočnom svete alebo **virtuálne**, ktoré existujú len v kybernetickom priestore, a nemožno ich vidieť, alebo dotknúť sa ich v reálnom svete. [47]

Hrozby, ktoré existujú v kybernetickom priestore sú rozsiahle a možno ich deliť na hrozby pre osobné aktíva[48] a hrozby pre organizačné aktíva[49]. Je potrebné podotknúť, že tieto hrozby majú pôvod v kybernetickom prostredí.

[43] Problematickým aspektom pojmu kybernetický priestor v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov je aj zaradenie ľudí medzi prvky kybernetického priestoru. Bližšie pozri ANDRAŠKO, J. a kol.: *Zákon o kybernetickej bezpečnosti*. Komentár. Bratislava: Wolters Kluwer SR s.r.o. 2018, s. 95.
[44] ISO/IEC 27032:2012, s. 21.
[45] Medzi osobné virtuálne aktíva možno zaradiť napríklad online identitu konkrétneho používateľa, virtuálnu menu a pod. Medzi fyzické osobné aktíva možno zaradiť hardvér, softvér, ako aj osobné digitálne zariadenia, ktoré slúžia osobe na komunikáciu v kybernetickom priestore.
[46] Medzi materiálne organizačné aktíva možno zaradiť infraštruktúru, do ktorej patrí prepojenie sietí, serverov, aplikácií, ktoré patria poskytovateľom služieb. Táto infraštruktúra poskytuje používateľom možnosť pripojiť sa do kybernetického priestoru a využívať služby poskytované v tomto priestore. Medzi virtuálne organizačné aktíva patrí napr. obchodná značka, URL organizácie, informácie o jej webovom sídle alebo jej duševné vlastníctvo.
[47] ISO/IEC 27032:2012, s. 16.
[48] Medzi hrozby pre osobné aktíva možno zaradiť krádež osobných údajov, online identity, neoprávnený prístup k finančným údajom osoby a pod.
[49] Medzi hrozby pre organizačné aktíva možno zaradiť krádež informácií (o zamestnancoch, klientoch, dodávateľoch a pod.), ako aj informácií, ktoré uchováva vláda a štát (informácie z oblasti národnej bezpečnosti, spravodajskej služby, armády, informácie o jednotlivcoch a pod.). Ďalšiu hrozbu predstavuje napadnutie infraštruktúry a informácií, ktoré zabezpečujú poskytovanie a využívanie služieb e-Governmentu.

Podobne ako v prípade informačnej bezpečnosti, aj v prípade kybernetickej bezpečnosti môže pri využití **zraniteľnosti** konkrétneho aktíva dôjsť k poškodeniu alebo zničeniu hodnoty aktíva.[50]

1.4.1 Vzťah kybernetickej bezpečnosti s inými oblasťami bezpečnosti

Kybernetická bezpečnosť sa v zmysle štandardu ISO/IEC 27032:2012 opiera o informačnú bezpečnosť *(information security)*, bezpečnosť aplikácií *(application security)*, bezpečnosť siete *(network security)* a bezpečnosť Internetu *(Internet security)* ako o základné stavebné kamene. Kybernetická bezpečnosť je jednou z činností potrebných pre ochranu kritickej informačnej infraštruktúry *(critical information infrastructure protection)*. Primeraná ochrana služieb kritickej infraštruktúry súčasne prispieva k základným potrebám bezpečnosti (bezpečnosť, spoľahlivosť a dostupnosť kritickej infraštruktúry) za účelom dosiahnutia cieľov kybernetickej bezpečnosti.[51]

Kybernetická bezpečnosť nie je synonymom informačnej bezpečnosti, bezpečnosti aplikácií, bezpečnosti siete, bezpečnosti Internetu či ochrany kritickej informačnej infraštruktúry. Tieto bezpečnostné domény majú svoje vlastné ciele a rozsah zamerania.

V zmysle predmetného medzinárodného štandardu sú vyššie uvedené oblasti bezpečnosti chápané ako:

Informačná bezpečnosť

- týka sa ochrany dôvernosti, integrity a dostupnosti informácií vo všeobecnosti, tak aby slúžila potrebám užívateľov príslušných informácií.

Bezpečnosť aplikácií[52]

- bezpečnosť aplikácií predstavuje proces smerujúci k zavádzaniu opatrení a ich meranie pre aplikácie organizácie tak, aby bolo možné riadiť rizika spojené s ich používaním. Opatrenia a merania môžu byť zavedené pre aplikáciu samotnú (jej procesy, komponenty, softvér

[50] Zraniteľnosťou môže byť už samotné pripojenie počítača na Internet.
[51] ISO/IEC 27032:2012, s. 17.
[52] Aplikácia *(application)* predstavuje IT riešenie, vrátane aplikačného softvéru, aplikačných údajov a postupov, navrhnuté k tomu, aby pomáhali užívateľom v organizácii plniť určité úlohy alebo zvládať určité druhy IT problémov pomocou automatizácie procesov činností organizácie alebo pomocou funkcie. ISO/IEC 27032:2012, s. 10.

a výsledky), pre jej údaje (konfiguračné údaje, užívateľské údaje, organizačné údaje) a pre celú technológiu, procesy a aktérov zapojených do životného cyklu aplikácie.

Bezpečnosť siete

- sa zaoberá návrhom, zavedením a prevádzkovaním sietí na dosiahnutie cieľov informačnej bezpečnosti v sieťach v rámci organizácií, medzi organizáciami a medzi organizáciami a užívateľmi.[53]

Bezpečnosť Internetu

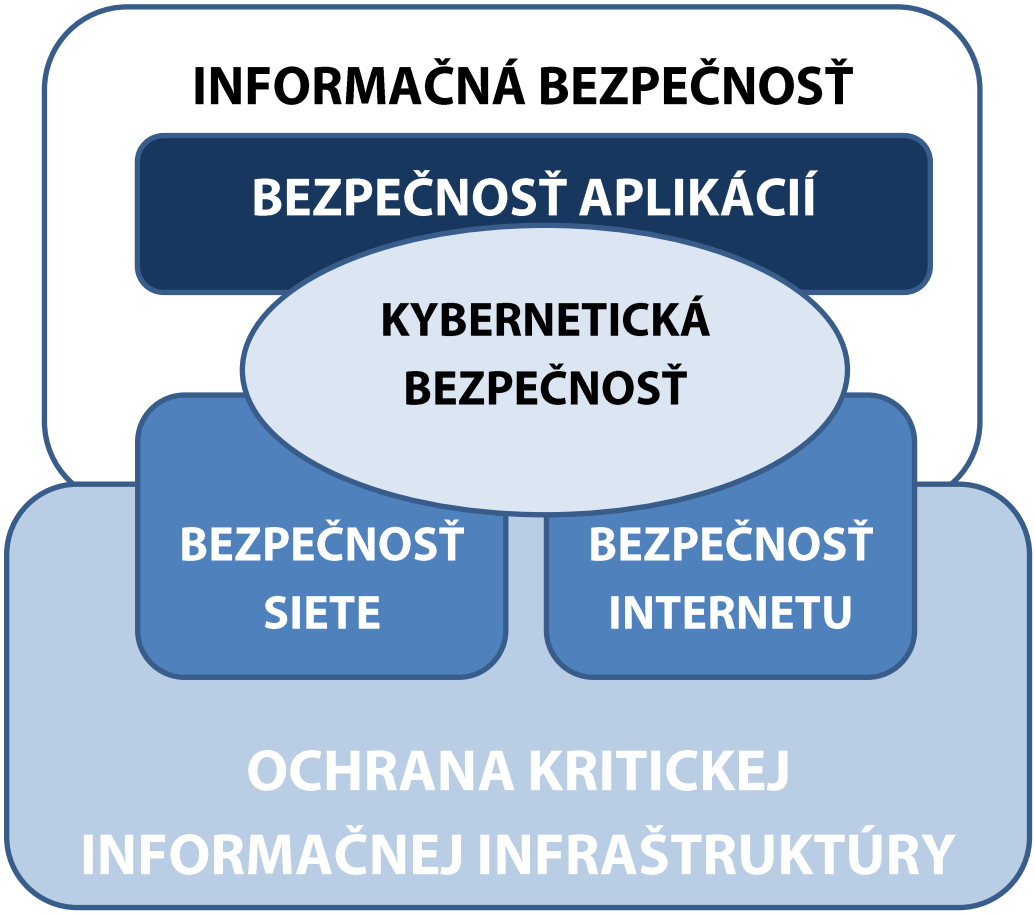
- sa týka ochrany služieb súvisiacich s Internetom a súvisiacich systémov a sietí IKT ako rozšírenia bezpečnosti siete v organizáciách a domácnostiach za účelom dosiahnutia ich bezpečnosti. Bezpečnosť Internetu taktiež zabezpečuje dostupnosť a spoľahlivosť služieb Internetu.

Ochrana kritickej informačnej infraštruktúry

- sa zaoberá ochranou systémov, ktoré sú poskytované alebo prevádzkované poskytovateľmi kritickej infraštruktúry, ako sú energetické, telekomunikačné a vodárenské spoločnosti. Ochrana kritickej informačnej infraštruktúry zabezpečuje, aby tieto systémy a siete boli chránené a odolné voči rizikám informačnej bezpečnosti, bezpečnosti siete, bezpečnosti Internetu, ako aj rizikám kybernetickej bezpečnosti.[54]

Nižšie uvedený obrázok znázorňuje vzťah kybernetickej bezpečnosti s inými bezpečnostnými doménami. Vzťah medzi týmito oblasťami a kybernetickou bezpečnosťou je komplexný. Niektoré služby kritickej infraštruktúry (napr. dodávka vody a preprava) nemusia ovplyvňovať kybernetickú bezpečnosť priamo alebo významným spôsobom. Avšak nedostatok kybernetickej bezpečnosti môže mať negatívny vplyv na dostupnosť systémov kritickej informačnej infraštruktúry, ktoré sú poskytované poskytovateľmi kritickej infraštruktúry.[55]

[53] Tamtiež, s. 18.
[54] Tamtiež.
[55] Tamtiež, s. 12.



Zdroj: ISO/IEC 27032:2012

Riešenie problémov kybernetickej bezpečnosti si vyžaduje značnú komunikáciu a koordináciu medzi rôznymi súkromnými a verejnými subjektmi z rôznych krajín a organizácií. Incidenty kybernetickej bezpečnosti často prekračujú národné, geografické a organizačné hranice. Rýchlosť toku informácií a zmien z rozvíjajúceho sa incidentu dáva často obmedzený čas k tomu, aby reagujúci jednotlivci a organizácie mohli konať. Preto je viac ako potrebné vytvoriť systém pre zdieľanie informácií a koordináciu, ktorý by bol nastavený spôsobom, aby pomáhal pripravovať reakciu na udalosti a incidenty kybernetickej bezpečnosti. Takýto systém pre zdieľanie informácií a koordináciu by mal byť bezpečný, efektívny, spoľahlivý a účelný.[56]

Pre účely vytvorenia systému zdieľania informácií a koordinácie v prípade incidentov kybernetickej bezpečnosti, štandard ISO/IEC 27032:2012 zavádza dve skupiny organizácií, konkrétne organizácia, ktorá poskytuje informáciu a organizácia, ktorá prijíma informáciu.[57]

[56] Tamtiež, s. 38.
[57] Tamtiež.

1.4.2 Rozdiel medzi informačnou a kybernetickou bezpečnosťou

V prvom rade si je potrebné uvedomiť, že v prípade skúmaných pojmov nejde o synonymá. Informačnú a kybernetickú bezpečnosť nemožno vnímať ako totožné pojmy a nie je ani vhodné ich rozlišovať na základe toho, ktorý pojem je širší alebo užší.

V zmysle vyššie skúmaných medzinárodných štandardov a odbornej literatúry je zrejmé, že cieľom informačnej bezpečnosti je ochrana informácií a IKT, ktoré tieto informácie spracúvajú. V prípade kybernetickej bezpečnosti je okrem iného taktiež cieľom ochrana informácií, ale len tých z prostredia kybernetického priestoru. V tejto súvislosti si je potrebné uvedomiť, že z pohľadu ochrany informácie ako aktíva, sú v prípade informačnej bezpečnosti chránené nie len informácie v elektronickej podobe, ale aj vo fyzickej podobe.

V druhom rade je potrebné podotknúť, že kybernetická bezpečnosť má z pohľadu štandardov za cieľ zabezpečiť zdieľanie a koordináciu medzi jednotlivými bezpečnostnými doménami. Možno povedať, že kybernetická bezpečnosť spravuje bezpečnostné problémy, ktoré nerieši žiadna z bezpečnostných domén alebo môže byť identifikovaná viacerými doménami. V druhom prípade je potrebné zdieľať a koordinovať informácií pre efektívne a komplexné riešenie bezpečnostného problému.[58] V niektorých prípadoch je pojem kybernetickej bezpečností spájaný s ochranou kritickej informačnej infraštruktúry, čo však nie je pravdou. Súvislosť medzi kybernetickou bezpečnosťou a ochranou kritickej informačnej infraštruktúry častokrát viac ako zrejmá, nakoľko napr. infraštruktúra telekomunikačných sietí zabezpečuje prístup do kybernetického priestoru.

Správne zadefinovanie pojmu kybernetický priestor, resp. vymedzenie jeho pôsobnosti je z teoretického hľadiska dôležité, nakoľko kybernetickú bezpečnosť môžeme chápať ako informačnú bezpečnosť kybernetického priestoru. Avšak v súčasnosti sa v právnom poriadku Slovenskej republiky nerozlišuje medzi informačnou bezpečnosťou a kybernetickou bezpečnosťou. Z právneho hľadiska, ako aj praktického hľadiska je rozlišovanie medzi informačnou bezpečnosťou a kybernetickou bezpečnosťou nepodstatné. Dôležitejšie je, aby právna úprava zabezpečila dostatočnú ochranu informačných systémov a informácií, ktoré sa v nich spracúvajú, tak aby sa dalo spoľahnúť na ich dôvernosť, dostupnosť a integritu. Taktiež je potrebné, aby sa zabezpečila nielen ochrana informácií v materiálnej podobe, ale aj informácií, ktoré sú spracúvané v elektronickej alebo digitálnej forme.

[58] V niektorých prípadoch je pojem kybernetickej bezpečností spájaný s ochranou kritickej informačnej infraštruktúry, čo však nie je pravdou. Súvislosť medzi kybernetickou bezpečnosťou a ochranou kritickej informačnej infraštruktúry je častokrát viac ako zrejmá, nakoľko napr. infraštruktúra telekomunikačných sietí zabezpečuje prístup do kybernetického priestoru.

KAPITOLA 2 PRÁVNA ÚPRAVA INFORMAČNEJ A KYBERNETICKEJ BEZPEČNOSTI

Právna úprava informačnej a kybernetickej bezpečnosti je do značnej miery roztrieštená či už z pohľadu práva Európskej únie, alebo právneho poriadku Slovenskej republiky. Okrem všeobecne záväzných právnych aktov je skúmaná problematika obsahom aj rôznych stratégií, ktoré boli prijaté na národnej úrovni a úrovni Európskej únie. Je však potrebné podotknúť, že právo nie je jediným regulačným nástrojom informačnej a kybernetickej bezpečnosti, nakoľko je problematika informačnej a kybernetickej bezpečnosti predmetom aj technických noriem.

V tejto časti učebnice dôjde k zhrnutiu základných právnych aktov, ktoré boli prijaté na úrovni práva Európskej únie a právneho poriadku Slovenskej republiky. V prvom rade sa zameriame na právne akty nezáväzného charakteru a nasledovne rozoberiem právne záväzné akty. V rámci legislatívnych aktov poskytneme základný pohľad na daný právny akt a poukážem na aspekty informačnej a kybernetickej bezpečnosti.

2.1 Európska únia

Európska únia doposiaľ neprijala legislatívny akt, ktorý by komplexne harmonizoval problematiku informačnej a kybernetickej bezpečnosti v členských štátoch Európskej únie. Aktivity Európskej únie v oblasti informačnej a kybernetickej bezpečnosti smerujúce najmä k ochrane jednotného digitálneho trhu a dosiahnutiu vysokej úrovne kybernetickej bezpečnosti v Európskej únii. V aktoch Európskej únie sa používa skôr pojem kybernetická bezpečnosť, než pojem informačná bezpečnosť.

2.1.1 Právne nezáväzné akty

Stratégia kybernetickej bezpečnosti Európskej únie

Prvá stratégia Európskej únie v oblasti kybernetickej bezpečnosti bola prijatá v roku 2013 a stanovila strategické ciele a konkrétne opatrenia na dosiahnutie odolnosti, zníženie počítačovej kriminality, rozvoj politiky a kapacít kybernetickej obrany, rozvoj priemyselných a technologických zdrojov a vytvorenie koherentnej medzinárodnej politiky kybernetického priestoru pre Európsku úniu.

Stratégia kybernetickej bezpečnosti Európskej únie[59] bola 7. februára 2013 predložená Vysokou predstaviteľkou Európskej únie pre zahraničné veci a bezpečnostnú politiku. Súčasne bol s týmto politickým dokumentom predložený návrh smernice Európskeho parlamentu a Rady o

[59] KOMISIA: Stratégia kybernetickej bezpečnosti Európskej únie. Brusel: 2013, s. 3.

opatreniach k zaisteniu vysokej spoločnej úrovne bezpečnostných sietí a informácií v Únii. Podľa Stratégie možno pod **kybernetickou bezpečnosťou** rozumieť nasledovné:
„Kybernetická bezpečnosť obyčajne odkazuje na ochranné opatrenia a plány, ktoré môžu byť použité k ochrane kybernetickej domény, a to ako v civilnej, tak aj vo vojenskej oblasti, pred hrozbami, ktoré sú s nimi spojené alebo ktoré by mohli poškodiť jej vzájomne prepojené siete a informačnú infraštruktúru. Kybernetická bezpečnosť usiluje o zachovanie dostupnosti a integrity sietí a infraštruktúry a dôvernosť informácií v nich obsiahnutých."[60]

2.1.2 Legislatívne akty

Medzi legislatívne akty, ktoré reflektujú požiadavky informačnej a kybernetickej bezpečnosti zaraďujeme:

- Smernicu NIS;
- Akt o kybernetickej bezpečnosti;
- Nariadenie eIDAS;
- Všeobecné nariadenie na ochranu údajov;
- Smernicu PSD2; a
- Smernicu o ochrane súkromia v elektronických komunikáciách.

2.2 Smernica NIS

Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (ďalej len „smernica NIS")[61] predstavuje prvý legislatívny akt prijatý európskym zákonodarcom, ktorého hlavným cieľom je posilniť kybernetickú bezpečnosť v celej Európskej únii.

Smernica NIS je prvým základným krokom s cieľom podporiť manažment rizík, tým že stanovuje bezpečnostné požiadavky ako právne povinnosti pre kľúčové hospodárske subjekty, ktorými sú prevádzkovatelia základných služieb a poskytovatelia digitálnych služieb.

V zmysle recitálu 3 smernice NIS zohrávajú siete a informačné systémy, a predovšetkým Internet zásadnú úlohu pri uľahčovaní cezhraničného pohybu tovaru, služieb a osôb. Z dôvodu tohto nadnárodného charakteru môžu mať zásadné narušenia týchto systémov, či už úmyselné, alebo nie a bez ohľadu na to, kde k nim dôjde, dôsledky pre jednotlivé členské štáty aj Európsku úniu ako celok. **Bezpečnosť sietí a informačných systémov je preto základným predpokladom hladkého fungovania vnútorného trhu.**

Za sieť a informačný systém je v zmysle smernice možno považovať:

a) **elektronickú komunikačnú sieť** v zmysle článku 2 písm. a) smernice 2002/21/ES;

[60] Tamtiež.
[61] Z anglického názvu *Directive on security of network and information systems.*

b) každé **zariadenie alebo skupina vzájomne prepojených alebo súvisiacich zariadení**, z ktorých jedno alebo viaceré vykonávajú na základe programu automatické spracúvanie digitálnych údajov, alebo

c) **digitálne údaje**, ktoré sa ukladajú, spracúvajú, získavajú alebo prenášajú prostredníctvom prvkov uvedených v písmenách a) a b) na účely ich prevádzkovania, používania, ochrany a udržiavania;[62]

Smernica NIS stanovuje **opatrenia** na dosiahnutie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v rámci Európskej únie s cieľom zlepšiť fungovanie vnútorného trhu. Na tento účel sa:

- stanovujú pre všetky členské štáty povinnosti prijať **národnú stratégiu** v oblasti bezpečnosti sietí a informačných systémov,
- vytvára **skupina pre spoluprácu** s cieľom podporiť a uľahčiť strategickú spoluprácu a výmenu informácií medzi členskými štátmi a rozvíjať vzájomnú dôveru medzi nimi,
- vytvára **sieť jednotiek pre riešenie počítačových bezpečnostných incidentov** (computer security incident response teams network – ďalej len „sieť jednotiek **CSIRT**") s cieľom prispievať k rozvoju dôvery medzi členskými štátmi a podporovať rýchlu a účinnú operačnú spoluprácu,
- **stanovujú bezpečnostné a oznamovacie požiadavky** pre prevádzkovateľov základných služieb a pre poskytovateľov digitálnych služieb,
- stanovujú povinnosti členských štátov **určiť príslušné vnútroštátne orgány, národné jednotné kontaktné miesta a jednotky CSIRT** s úlohami súvisiacimi s bezpečnosťou sietí a informačných systémov

Smernica NIS neupravuje pojem kybernetická bezpečnosť alebo informačná bezpečnosť, ale definuje pojem **bezpečnosť sietí a informačných systémov.** V zmysle čl. 4 ods. 1 smernice NIS predstavuje bezpečnosť sietí a informačných systémov: *„schopnosť sietí a informačných systémov odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje **dostupnosť**, **autentickosť, integritu** alebo **dôvernosť** uchovávaných, prenášaných alebo spracúvaných **údajov alebo súvisiacich služieb** poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov."*

V smernici NIS sú definované dva druhy hospodárskych subjektov, a to konkrétne **prevádzkovatelia základných služieb** (ďalej len „**PZS**") a **poskytovatelia digitálnych služieb** (ďalej len „**PDS**"). PZS sú verejné alebo súkromné subjekty, ktoré spĺňajú kritéria v zmysle čl. 5 ods. 2 smernice NIS a typ takéhoto subjektu sa uvádza v prílohe II smernice NIS. Ide o subjekty z odvetvia

[62] Čl. 4 ods. 1 smernice NIS.

energetiky, dopravy, bankovníctva, infraštruktúry finančných trhov, zdravotníctva, dodávky a distribúcie pitnej vody a digitálnej infraštruktúry. Smernica NIS ukladá členským štátom regulovať PZS podľa zásady minimálnej harmonizácie, čo znamená, že je možné, aby si členské štáty túto úpravu rozšírili i na ďalšie, smernicou neuvedené odvetvia.

Kritériami na identifikáciu PZS v zmysle čl. 5 ods. 2 smernice NIS sú:

a) subjekt poskytuje službu, ktorá má zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností;
b) poskytovanie tejto služby je závislé od sietí a informačných systémov a
c) incident by mal závažný rušivý vplyv na poskytovanie uvedenej služby.

V súvislosti s **určením závažného rušivého vplyvu** zohľadňujú členské štáty v zmysle čl. 6 smernice NIS aspoň tieto medziodvetvové faktory:

a) počet používateľov využívajúcich službu, ktorú poskytuje daný subjekt;
b) závislosť ostatných odvetví uvedených v prílohe II od služby, ktorú poskytuje daný subjekt;
c) vplyvu, ktorý by mohli mať incidenty z hľadiska rozsahu a trvania na hospodárske a spoločenské činnosti alebo verejnú bezpečnosť;
d) trhový podiel daného subjektu;
e) geografické rozšírenie z hľadiska oblasti, ktorú by incident mohol postihnúť;
f) význam subjektu z hľadiska zachovania dostatočnej úrovne služby, berúc do úvahy dostupnosť alternatívnych spôsobov poskytovania danej služby.

Podľa potreby môžu členské štáty zohľadniť pri určení či by mal incident závažný rušivý vplyv aj faktory špecifické pre jednotlivé odvetvia.[63]

Smernica NIS v súvislosti s PDS uplatňuje maximálnu harmonizáciu, čo znamená, že na rozdiel od úpravy PZS u PDS nesmú členské štáty prijať prísnejšie pravidlá, ako tie ktoré vyplývajú zo smernice NIS. PDS je každá právnická osoba, ktorá poskytuje niektorú z týchto digitálnych služieb:

a) online trhovisko (čl. 4 ods. 17, recitál 15)
b) internetový vyhľadávač (čl. 4 ods. 18, recitál 16)
c) služby cloud computingu (čl. 4 ods. 19, recitál 17)

Bezpečnostné a oznamovacie požiadavky sa nevzťahujú len na incidenty z kybernetického priestoru, nakoľko akýkoľvek incident, ktorý môže ohroziť bezpečnosť sietí a informačných systémov, ktoré slúžia na poskytovanie základných služieb môžu byť oznámené. Medzi takéto incidenty možno zaradiť výpadky prúdu, nebezpečenstvá pre životné prostredie, zlyhanie hardvéru, počítačové útoky, škodlivý softvér a vírusy.

[63] Čl. 6 ods. 2 smernice NIS.

Smernica NIS nešpecifikuje lehotu na oznámenie incidentov ale len ukladá povinnosť prevádzkovateľom základných služieb, aby bez zbytočného odkladu oznamovali príslušnému orgánu alebo jednotke CSIRT incidenty, ktoré majú závažný vplyv na kontinuitu základných služieb, ktoré poskytujú.[64]

Požiadavky pre oznámenie incidentov v zmysle smernice NIS a pravidlá pre oznámenie porušenia ochrany osobných údajov v zmysle všeobecného nariadenia o ochrane údajov sa môžu prekrývať, čo môže mať za následok oznamovanie rovnakých incidentov rôznym orgánom.

Smernica NIS v čl. 19 podporuje využívanie európskych alebo medzinárodne uznávaných noriem a špecifikácií, ktoré sú relevantné pre bezpečnosť sietí a informačných systémov. Takýmito normami by mohli byť medzinárodné štandardy ISO z oblasti hodnotenia rizík, napr. ISO 27001 Information technology -- Security techniques -- Information security management systems – Requirements a ISO 22301 Societal security -- Business continuity management systems --- Requirements.

2.3 Akt o kybernetickej bezpečnosti

Na úrovní práva EÚ bolo prijaté **nariadenie európskeho parlamentu a rady o Agentúre EÚ pre kybernetickú bezpečnosť (ENISA), o zrušení nariadenia (EÚ) č. 526/2013 a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií** (ďalej len „akt o kybernetickej bezpečnosti“).[65]

Akt o kybernetickej bezpečnosti, ktorý okrem iného vytvára systém certifikácie v oblasti kybernetickej bezpečnosti, ktorý by mal zabezpečiť dostatočnú úroveň kybernetickej bezpečnosti IKT produktov, postupov a služieb v Európskej únii.[66] Certifikácia IKT v oblasti kybernetickej bezpečnosti sa stáva veľmi dôležitou otázkou, a to najmä vo vzťahu k zvýšenému používaniu technológií, ktoré požadujú vysokú úroveň kybernetickej bezpečnosti (autonómne vozidlá, systémy elektronickej kontroly zdravia alebo priemyselnej automatizácie). Certifikát osvedčí, že výrobky a služby IKT, ktoré boli certifikované v súlade s takýmto systémom, spĺňajú stanovené požiadavky na kybernetickú bezpečnosť. Výsledný certifikát bude uznávaný vo všetkých členských štátoch, čo uľahčí podnikom cezhraničné obchodovanie a zákazníkom pochopiť bezpečnostné prvky produktu alebo služby.

Avšak je potrebné podotknúť, že využitie certifikácie kybernetickej bezpečnosti je dobrovoľné, pokiaľ sa to nestanovuje inak v právnych predpisoch Európskej únie alebo vnútroštátnych právnych predpisoch, ktorými sa stanovujú bezpečnostné požiadavky týkajúce sa

[64] Tamtiež, čl. 14 ods. 3.
[65] Dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:52017PC0477R(01)&from=SK
[66] Bližšie k certifikácii pozri: VOSTOUPAL, Jakub. Certifikace kyberbezpečnostních technologií. *Revue pro právo a technologie*. [Online]. 2019, č. 20, s. 147-268. Dostupné z: https://journals.muni.cz/revue/article/view/12570.

produktov a služieb IKT. Postupy certifikácie kybernetickej bezpečnosti produktov a služieb IKT, na ktoré sa vzťahuje európsky systém certifikácie kybernetickej bezpečnosti, by mali stratiť účinky od dátumu, ktorý stanoví Komisia vo vykonávacom akte. Okrem toho by členské štáty nemali zavádzať nové vnútroštátne systémy certifikácie kybernetickej bezpečnosti v prípade produktov a služieb IKT, pre ktoré už existuje európsky systém certifikácie kybernetickej bezpečnosti.[67]

2.4 Nariadenie eIDAS[68]

Hlavným cieľom **nariadenia EP a Rady 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** (ďalej len „nariadenie eIDAS") je, aby elektronický podpis, elektronická pečať, elektronická časová pečiatka použité občanmi členských štátov Európskej únie mali rovnaké právne účinky v iných členských štátoch Európskej únie a taktiež aby mohli občania Európskej únie využívať národné prostriedky elektronickej identifikácie (napr. elektronický občiansky preukaz) v iných členských štátoch Európskej únie minimálne pri vstupe do online služieb poskytovaných subjektmi verejného sektora.

V súvislosti s vyššie uvedenými cieľmi je spojených mnoho otázok, ktoré sa týkajú informačnej a kybernetickej bezpečnosti. V prvom rade možno hovoriť o identifikácii a autentifikácii osôb, ktoré sa budú chcieť autentifikovať do online služieb poskytovaných subjektom verejného sektora iných členských štátov Európskej únie. Pre jednotlivé online služby bude potrebné v zmysle nariadenia eIDAS stanoviť úrovne záruky, ako aj pre samotné prostriedky elektronickej identifikácie. V súvislosti so stanovením konkrétnej úrovne záruky, vychádzal európsky zákonodarca z projektu STORK *(Secure idenTity acrOss boRders linKed)* a medzinárodného štandardu ISO/IEC 29115:2013 *Entity authentication assurance framework*. [69]

V druhom rade sa problematika informačnej a kybernetickej bezpečnosti týka samotného procesu cezhraničnej autentifikácie, kde je potrebné zabezpečiť dostatočnú ochranu informácií, ktoré sú spracované v rámci jednotlivých uzlov, ktoré budú medzi sebou komunikovať.[70]

---

[67] Bod 57 recitálu Aktu o kybernetickej bezpečnosti.

[68] Viac o nariadení eIDAS pozri ANDRAŠKO. J. a kol. *Vybrané kapitoly práva informačných technológií 1*. 1. vyd. Bratislava: Právnická fakulta UK, 2019, s. 117 a nasl. Dostupné na: https://www.flaw.uniba.sk/fileadmin/praf/Veda/Publikacne_vystupy/2019/Monografia_DVSEI_2019.pdf.

[69] Výsledky spomínaného projektu a ISO štandardu sú predmetom Vykonávacieho nariadenia Komisie (EÚ) 2015/1502 z 8. septembra 2015, ktorým sa stanovujú minimálne technické špecifikácie a postupy pre úrovne záruky prostriedkov elektronickej identifikácie do značnej miery vychádza.

[70] Uzly musia spĺňať požiadavky medzinárodného štandardu ISO/IEC 27001. Bližšie pozri Vykonávacie nariadenie Komisie (EÚ) 2015/1501 z 8. septembra 2015 o rámci interoperability.

2.4.1 Bezpečnosť v zmysle článku 10 Nariadenia eIDAS

Jedným z cieľov nariadenia eIDAS je zabezpečiť, aby bola možná bezpečná elektronická identifikácia a autentifikácia[71] pri prístupe k cezhraničným službám online, ktoré ponúkajú členské štáty.[72]

Kľúčom k dôveryhodnému cezhraničnému vzájomnému uznávaniu prostriedkov elektronickej identifikácie je **bezpečnosť** schém elektronickej identifikácie.[73]

Narušenie bezpečnosti schémy elektronickej identifikácie je upravená v článku 10 nariadenia eIDAS. Predmetné ustanovenie nariadenia eIDAS upravuje situáciu, kedy oznámená schéma elektronickej identifikácie bola narušená alebo čiastočne skompromitovaná spôsobom, ktorý ovplyvní spoľahlivosť cezhraničnej autentifikácie danej schémy. V takýchto prípadoch je dotknutý členský štát povinný danú cezhraničnú autentifikáciu alebo dotknuté skompromitované časti bezodkladne pozastaviť alebo zrušiť a informuje o tom ostatné členské štáty a Komisiu.

V prípade ak dôjde k náprave narušenia alebo skompromitovania schémy elektronickej identifikácie dotknutý členský štát cezhraničnú autentifikáciu opätovne zavedie a bez zbytočného odkladu o tom informuje ostatné členské štáty a Komisiu. V opačnom prípade, a teda ak sa narušenie alebo skompromitovanie neodstráni v lehote troch mesiacov od pozastavenia alebo zrušenia, dotknutý členský štát informuje ostatné členské štáty a Komisiu o stiahnutí schémy elektronickej identifikácie. Komisia bez zbytočného odkladu uverejní zodpovedajúce zmeny v zozname schém elektronickej identifikácie v Úradnom vestníku Európskej únie.[74]

V podmienkach Slovenskej republiky možno hovoriť o narušení alebo skompromitovaní schémy elektronickej identifikácie v prípade, ak by bol narušený alebo skompromitovaný modul IAM (Identity Access Management), taktiež známy ako autentifikačný modul, ktorý plní dôležitú úlohu pri cezhraničnej autentifikácii osôb.

Bezpečná schéma elektronickej identifikácie, ktorá zabezpečuje spoľahlivú cezhraničnú autentifikáciu osôb do značnej miery súvisí a závisí od dostatočnej ochrany osobných údajov. V prvom rade, ak dôjde k úspešnej cezhraničnej autentifikácie sú osobám iných členských štátov zapísané osobné údaje do modulu IAM. Akékoľvek narušenie dôvernosti, integrity a dostupnosti údajov v procese cezhraničnej autentifikácie bude mať za následok porušenie ochrany osobných údajov.

---

[71] V zmysle bodu 7 preambuly vykonávacieho nariadenia Komisie (EÚ) 2015/1502 z 8. septembra 2015, ktorým sa stanovujú minimálne technické špecifikácie a postupy pre úrovne zabezpečenia prostriedkov elektronickej identifikácie podľa článku 8 ods. 3 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu by sa na zvýšenie bezpečnosti procesu autentifikácie mal používať väčší počet faktorov autentifikácie, a najmä z rôznych kategórií faktorov. Ako príklady sa uvádzajú spoločné tajomstvá, fyzické zariadenia a fyzické vlastnosti.

[72] Bod 12 preambuly nariadenia eIDAS.

[73] Tamtiež, bod 19.

[74] Čl. 10, ods. 2-3 nariadenia eIDAS.

2.5 Všeobecné nariadenie o ochrane údajov

2.5.1 Úvodné poznámky

Európska únia (EÚ) prijatím nového právneho rámca pre ochranu osobných údajov spresňuje a kreuje nové požiadavky pri spracúvaní osobných údajov. Ako už bolo uvedené v predchádzajúcom diele učebnice, na úrovní EÚ boli prijate primárne dva právne akty a to:

- Nariadenie Európskeho parlamentu a Rady (EÚ) 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 – ďalej len „**GDPR“**); a
- Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV (ďalej len „**Policajná smernica**“), pričom implementáciu Policajnej smernice reflektuje tretia časť zákona č. 18/2018 Z. z. o ochrane osobných údajov (ďalej len „**ZOOÚ**“).

V rámci tejto kapitoly s ohľadom na obsahové zameranie predkladanej časti učebnice sa zameriame na konkrétne aspekty bezpečnosti v súvislosti so spracúvaním osobných údajov. Primárne sa budeme venovať GDPR, avšak poukážeme aj na určité odchýlky implementácie Policajnej smernice.

2.5.2 Všeobecná klauzula bezpečnosti v GDPR

GDPR upravuje otázky bezpečnosti v rámci zásady integrity a dôvernosti a nadväzujúcich inštitútov. Zásada integrity a bezpečnosti v zmysle článku 5 ods. 1 písm. f) ustanovuje, že osobné údaje musia byť *„spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení.“* Na túto zásadu následne nadväzuje článok 32 GDPR (bezpečnosť spracúvania osobných údajov a nahlasovanie porušení ochrany osobných údajov (články 33 a 34 GDPR).

V kontexte bezpečnosti podľa GDPR je potrebné na úvod uviesť dve poznámky. V prvom rade, GDPR predstavuje technologicky neutrálny predpis.[75] V súvislosti s bezpečnosťou to znamená, že nepredpisuje na zabezpečenie spracovateľských operácií konkrétne technológie (napr. špecifický software alebo hardware). Voľba vhodných technológií je na prevádzkovateľovi. V druhom rade, bezpečnosť spracúvania osobných údajov je v zmysle tohto nariadenia závislá od posúdenia

[75] Článok 15 GDPR: *„S cieľom zabrániť vzniku závažného rizika obchádzania právnych predpisov by mala byť ochrana fyzických osôb technologicky neutrálna a nemala by závisieť od použitých technologických riešení.“*

subjektívneho rizika. Subjektívne riziko ďalej rozvádza recitál 39 GDPR. Pre ilustráciu *„riziko pre práva a slobody fyzických osôb s rôznym stupňom pravdepodobnosti a závažnosti môžu vyplývať zo spracúvania osobných údajov, ktoré by mohlo viesť k ujme na zdraví, majetkovej alebo nemajetkovej ujme, a to najmä ak spracúvanie môže viesť k diskriminácii, krádeži totožnosti alebo podvodu, finančnej strate, poškodeniu dobrého mena, strate dôvernosti osobných údajov chránených profesijným tajomstvom, neoprávnenej reverznej pseudonymizácii alebo akémukoľvek inému závažnému hospodárskemu alebo sociálnemu znevýhodneniu; ak by dotknuté osoby mohli byť pozbavené svojich práv a slobôd alebo im bolo bránené v kontrole nad svojimi osobnými údajmi.“*[76] Ako je zjavné z vyššie uvedeného, GDPR preferuje tzv. prístup založený na analýze rizika (*risk-based approach*) a z toho dôvodu nie je riešením spoľahnutie sa na informačnú bezpečnosť v zmysle ISO noriem série 27k. Tie totiž nezohľadňujú práve spomenuté subjektívne riziká pre práva, slobody a záujmy dotknutých osôb, ako to vyžaduje GDPR. Súlad s ISO normami síce môže byť nápomocný, avšak reguluje skôr technické zabezpečenie informácie.

Jediný článok, ktorý výslovne upravuje bezpečnosť spracúvania osobných údajov je článok 32 GDPR: *„Prevádzkovateľ a sprostredkovateľ prijmú so zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb, primerané technické a organizačné opatrenia s cieľom zaistiť úroveň bezpečnosti primeranú tomuto riziku.“* GDPR ďalej demonštratívne uvádza výpočet organizačných či technických opatrení. Konkrétne hovorí o (i) pseudonymizácií a šifrovaní osobných údajov; (ii) schopnosti zabezpečiť trvalú dôvernosť, integritu, dostupnosť a odolnosť systémov spracúvania a služieb; (iii) schopnosti včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu a (iv) procese pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania. Prirodzene, každý prevádzkovateľ či sprostredkovateľ si vyberá *primerané* organizačné a technické opatrenia kvôli bezpečnosti. Iné opatrenia sú vhodné pre sociálnu sieť s dvoma miliardami užívateľov a pre malého podnikateľa s päťdesiatimi zákazníkmi. Organizačné opatrenia smerujú skôr ku implementácií opatrení z organizačného hľadiska a týkajú sa výkonu konkrétnych pracovných úloh či nastavení mantinelov pri práci s osobnými údajmi. Technické opatrenia majú už z dikcie svojho názvu technický charakter a týkajú sa použitia konkrétneho softwaru alebo hardwaru či technického nastavenia procesov súvisiacich so spracúvaním osobných údajov. Nižšie uvádzame praktické príklady organizačných a technických opatrení v prehľadnej tabuľke.

Organizačné opatrenia	Technické opatrenia
Poučenia poverených osôb	Postupy bezpečného obstarávania softwarov

[76] Viď ďalšie riziká podľa recitálu 75 GDPR.

Oddelenie právomocí	Sieťove firewally
Pravidlá a kontrola vstupu	Monitorovanie bezpečnosti siete
Vzdelávanie	Manažment identitít
Určenie postupov likvidácie údajov	Šifrovanie alebo pseudonimizácia
Pravidlá manipulácie s nosičmi	Logovanie
Pravidlá pre používanie prenosných zariadení	Ochrana proti malware
Politika čistého stola	Migrované sieťové úložiská dát
Organizácia tímu a riadenie bezpečnostných incidentov	Záložné kópie dát
Pravidlá na výber sprostredkovateľov	
Politika manažmentu práv dotknutých osôb	

Tabuľka č. 1: Príklady organizačných a technických opatrení v zmysle článku 32 GDPR

Pri poskytovaní elektronických služieb verejnej správy by mala byť bezpečnosť dát jednou z priorít orgánov verejnej moci a s tým súvisí aj požiadavky úrovne bezpečnostných opatrení. Aj samotný zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov upravuje požiadavky bezpečnosti informačných technológií verejnej správy v § 18, pričom odkazuje na osobitný predpis v podobe právnej úpravy kybernetickej bezpečnosti[77] a súvisiacich podzákonných právnych aktov.

2.5.3 Porušenie ochrany osobných údajov

Druhou zložkou bezpečnosti v rámci GDPR je problematika nahlasovania porušení ochrany osobných údajov. Porušenie ochrany osobných údajov je definované v článku 4 bode 12 GDPR ako *„porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim.“* Vzhľadom na atribúty informácie v zmysle teórie informačnej bezpečnosti možno porušenia ochrany osobných údajov rozdeliť na:

- Porušenie dôvernosti (*confidentiality breach*) napr. únik osobných údajov;
- Porušenie integrity (*integrity breach*) napr. kompromitovanie kamerového záznamu; a
- Porušenie dostupnosti (*availiability breach*) napr. hacknutie systému a odopretie prístupu k osobným údajom povereným osobám.[78]

Samotné nahlasovanie (reportovanie) porušení ochrany osobných údajov môžeme deliť podľa entity, ktorej sa tieto incidenty nahlasujú. Článok 33 GDPR upravuje nahlasovanie porušení ochrany osobných údajov dozornému orgánu a článok 34 GDPR upravuje nahlasovanie porušení ochrany osobných údajov dotknutej osobe.

Proces nahlasovania vyhodnocovania porušení ochrany osobných údajov možno zadeliť do viacerých etáp alebo fáz. V prvom rade, ak všeobecne dôjde ku bezpečnostnému incidentu

[77] Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.
[78] K tomu pozri aj Article 29 Working Party Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01.

v najširšom slova zmysle, je potrebné zistiť, či tento incident možno kvalifikovať ako porušenie ochrany osobných údajov. Za týmto účelom je dobrou praxou, ak je v organizácií zriadený tím na riešenie bezpečnostných incidentov, ktorý zahŕňa bezpečnostného analytika, právnika a prípadne zodpovednú osobu doplnenú o podporu informatikov. V druhom rade by malo nasledovať hodnotenie rizika, ktoré rozoberáme nižšie. Treťou etapou je samotné splnenie povinnosti porušenie nahlásiť. Na záver je potrebné porušenie ochrany osobných údajov zadokumentovať. Asi najdôležitejšiu časť analýzy tvorí posúdenie, či predmetné porušenie vedie k (vysokým) rizikám pre práva a slobody dotknutých osôb.

Ak je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb, prevádzkovateľ je povinný do 72 hodín od momentu zistenia (*„po tom, čo sa o tom prevádzkovateľ dozvedel“*) incident nahlásiť **dozornému orgánu**. Nie je tak potrebné nahlasovať incidenty, ktoré nepredstavujú riziká pre práva a slobody fyzických osôb. Ilustrovať to možno na príklade, keď sa zamestnancovi stratí laptop s databázou klientov, ale predmetná databáza je šifrovaná a kľúč k nej má iba zamestnanec a jeho zamestnávateľ. Vzhľadom na to, že kľúč nebol kompromitovaný, je riziko pre práva a slobody dotknutých osôb žiadne resp. minimálne. V prípade, ak sa porušenie ochrany osobných údajov stane na strane sprostredkovateľa, je o tom povinný informovať prevádzkovateľa bez zbytočného odkladu.[79] Pri komplexnejších situáciách je možné dozorný orgán informovať postupne s vysvetlením, prečo tak prevádzkovateľ robí. Úrad na ochranu osobných údajov Slovenskej republiky má na svojom webe zverejnený formulár, prostredníctvom ktorého je možné porušenia ochrany osobných údajov nahlasovať.[80] Následne je prevádzkovateľ povinný predmetný incident zdokumentovať.

O porušeniach ochrany osobných údajov je potrebné informovať **dotknuté osoby** za predpokladu, že toto porušenie pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb. V takom prípade je prevádzkovateľ povinný túto informáciu poskytnúť dotknutým osobám bezodkladne.[81] Kritéria na posúdenie vysokého rizika vymedzila Pracovná skupina čl. 29 vo svojom usmernení.[82] Konkrétne ide o

- typ porušenia;
- povaha, citlivosť a kvantita údajov;
- možnosť identifikácie jednotlivcov;
- závažnosť dopadu pre jednotlivcov;
- či ide o dáta detí a zraniteľné osoby;
- rola prevádzkovateľa;

[79] Viď článok 33 ods. 2 GDPR.
[80] https://dataprotection.gov.sk/uoou/sk/dp/dp-breach (dostupné 15.11.2019).
[81] Článok 34 ods. 1 GDPR.
[82] Article 29 Working Party Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01.

- počet zasiahnutých osôb prípadne ďalšie faktory.[83]

V prípade, ak prevádzkovateľ vysoké riziko pri porušení ochrany osobných údajov vyhodnotí, nemusí automaticky dotknuté osoby informovať. GDPR totiž ustanovuje tri výnimky, keď prevádzkovateľ takéto incidenty nemusí notifikovať dotknutým osobám. Prvou výnimkou sú prípady, ak prevádzkovateľ prijal primerané technické a organizačné ochranné opatrenia a tieto opatrenia uplatnil na osobné údaje, ktorých sa porušenie ochrany osobných údajov týka, a to najmä tie opatrenia, na základe ktorých sú osobné údaje nečitateľné pre všetky osoby, ktoré nie sú oprávnené mať k nim prístup, ako je napríklad šifrovanie.[84] Druhým prípadom je situácia, ak prevádzkovateľ prijal následné opatrenia, ktorými sa zabezpečí, že vysoké riziko pre práva a slobody dotknutých osôb pravdepodobne už nebude mať dôsledky.[85] Poslednou výnimkou je prípad, ak by si informovanie vyžadovalo neprimerané úsilie. V takom prípade však dôjde namiesto toho k informovaniu verejnosti alebo sa prijme podobné opatrenie, čím sa zaručí, že dotknuté osoby budú informované rovnako efektívnym spôsobom (napr. oznámením na webstránke alebo v aplikácií po prihlásení užívateľa).[86] Ak prevádzkovateľ túto povinnosť nesplní, dozorný orgán si môže notifikačnú povinnosť vynútiť.[87] Aj v tomto prípade je prevádzkovateľ povinný predmetný incident zdokumentovať.

2.5.4 Prax dozorných orgánov v Slovenskej republike a v EÚ

Porušenia článku 32 GDPR bývajú jedným z najčastejších porušení GDPR za rok a pol aplikácie daného nariadenia. Vyplýva to z verejne dostupnej databázy rozhodnutí dozorných orgánov v EÚ.[88] Nižšie uvádzame najvyššie uložené pokuty v EÚ a na Slovensku za porušenie článku 32 GDPR so stručnou charakteristikou skutkovej podstaty prípadu.

Krajina / Pokuta	Charakteristika
Spojené kráľovstvo / 204,600,000 €	Britský dozorný orgán *plánuje* uložiť leteckej spoločnosti British Airways pokutu za nedostatočné bezpečnostné opatrenia a únik údajov o 500 000 zákazníkoch prostredníctvom kybernetického útoku na web spoločnosti. Vyšetrovanie ukázalo nedostatočné logovanie, ochranu informácií o kreditných kartách či údajoch o cestách.[89]
Spojené kráľovstvo / 110,390,200 €	Britský dozorný orgán *plánuje* uložiť sieti hotelových zariadení Marriott International pokutu za nedostatočné bezpečnostné

[83] Tamže.
[84] Článok 34 ods. 3 a) GDPR.
[85] Článok 34 ods. 3 b) GDPR.
[86] Článok 34 ods. 3 c) GDPR.
[87] Viď článok 34 ods. 4 GDPR.
[88] https://www.enforcementtracker.com/ (dostupné 14.2.2020).
[89] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/ (dostupné 12.12.2019).

	opatrenia a únik údajov týkajúci sa 339 miliónov zákazníkov.[90]
Taliansko / 27,800,000 €	Jeden z najväčších telekomunikačných operátorov v Talianksu (TIM) dostal pokutu v uvedenej výške za viacero porušení GDPR pri marketingovej komunikácií vrátane článku 32 GDPR.[91]
Nemecko / 9,550,000 €	Pokutu taktiež dostal nemecký telekomunikačný operátor (1&1 Telecom). Detaily nie sú verejne dostupné.[92]
Bulharsko / 2,600,000 €	Bulharská Národná daňová agentúra dostala uvedenú pokutu za porušenie článku 32 GDPR pri úniku údajov o 6 miliónoch daňových rezidentoch.[93]
Slovensko / 50,000 €	Najvyššiu pokutu od účinnosti GDPR dostala Sociálna poisťovňa za porušenie článku 32 GDPR v dôsledku straty žiadostí o sociálne poistenie, ktoré boli zaslané poisťovňou do zahraničia klasickým doručením (nie do vlastných rúk) a následne stratené.[94]
Slovensko / 40,000 €	Druhá najvyššia pokuta bola uložená telekomunikačnému operátorovi Slovak Telekom za nedostatočné bezpečnostné opatrenia. Detaily prípadu nie sú verejne dostupné.[95]

Tabuľka č. 2: Pokuty za porušenie článku 32 v EÚ a na Slovensku

2.5.5 Špecifiká požiadaviek na bezpečnosť pri implementácií Policajnej smernice

Pri legislatívou vymedzenom rozsahu subjektov je potrebné posúdiť aj bezpečnostné požiadavky kladené na tieto orgány. V prvom rade je však potrebné zvýrazniť, kedy sa tieto požiadavky aplikujú.

Pôsobnosť 3. časti ZOOÚ, ktorý predstavuje implementáciu Policajnej smernice spúšťajú dve podmienky, ktoré musia byť kumulatívne splnené. V prvom prípade musí ísť o spracúvanie osobných údajov na tzv. trestnoprávne účely, ktoré legislatíva definuje ako *„účely predchádzania a odhaľovania trestnej činnosti, zisťovania páchateľov trestných činov, stíhania trestných činov alebo na účely výkonu rozhodnutí v trestnom konaní vrátane ochrany pred ohrozením verejného poriadku a predchádzania*

[90] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/ (dostupné 12.12.2019).
[91] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9256486 (dostupné 12.12.2019).
[92] https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2019/30_BfDIverh%C3%A4ngtGeldbu%C3%9Fe1u1.html (dostupné 12.12.2019).
[93] https://www.cpdp.bg/index.php?p=news_view&aid=1519 (dostupné 12.12.2019).
[94] https://www.etrend.sk/ekonomika/socialna-poistovna-porusila-gdpr-pokutu-50-tisic-eur-nechce-zaplatit.html (dostupné 12.12.2019).
[95] https://www.etrend.sk/ekonomika/gdpr-zacina-hryzt-telekomunikacny-operator-dostal-pokutu-40-tisic-eur.html (dostupné 12.12.2019).

takémuto ohrozeniu."[96] Druhou podmienkou je personálna pôsobnosť, nakoľko implementácia Policajnej smernice sa týka iba tzv. príslušných orgánov a to konkrétne ak ide o spracúvanie osobných údajov Policajným zborom, Vojenskou políciou, Zborom väzenskej a justičnej stráže, Finančnou správou, prokuratúrou a súdmi.[97]

Za splnenia požiadaviek uvedených vyššie je potrebné dodržiavať aj špecifické bezpečnostné opatrenia, nakoľko ide o spracúvanie údajov v pomerne veľkom rozsahu pri vyšetrovaní a odhaľovaní trestných činoch a za veľmi špecifickým účelom.

§ 69 ZOOÚ ustanovuje povinnosť tzv. vedenia logov. Log je definovaný ako záznam o priebehu činnosti používateľa v automatizovanom informačnom systéme.[98] Ilustrovať to možno na príklade vyšetrovateľa, ktorý si prezerá záznamy o protiprávnej činnosti osoby podozrivej zo spáchania trestného činu v databáze. V zmysle tejto požiadavky je tak nutné, aby tento systém zaznamenával virtuálny „pohyb" vyšetrovateľa v tejto databáze. *„Príslušný orgán pri získavaní, zmene, prehliadaní, poskytovaní vrátane prenosu, kombinovaní a vymazaní osobných údajov v systéme automatizovaného spracúvania uchováva logy. Z logov o prehliadaní a poskytovaní musí byť možné určiť dôvod, dátum a čas prehliadania alebo poskytovania a identifikačné údaje osoby, ktorá tieto osobné údaje prehliadala alebo ich poskytovala, ako aj totožnosť príjemcov."*[99] Tieto operácie sa vykonávajú za účelom dodržiavania zákonnosti a bezpečnosti práce s takýmito systémami. Príslušné orgány majú povinnosť logy sprístupniť na požiadanie Úradu na ochranu osobných údajov SR.[100]

§ 71 ZOOÚ upravuje špecifické bezpečnostné opatrenia pri automatizovanom spracúvaní osobných údajov. Konkrétne by malo ísť o opatrenia na:

- kontrolu prístupu k zariadeniam, aby sa zabránilo neoprávnenému prístupu k zariadeniam na spracúvanie osobných údajov, ktoré sa používajú na spracúvanie,
- kontrolu nosičov osobných údajov, aby sa zabránilo neoprávnenému čítaniu nosičov osobných údajov, kopírovaniu nosičov osobných údajov, pozmeňovaniu nosičov osobných údajov alebo odstráneniu nosičov osobných údajov;
- kontrolu uchovávania osobných údajov, aby sa zabránilo neoprávnenému vkladaniu osobných údajov do informačného systému a neoprávnenému prehliadaniu osobných údajov v informačnom systéme, pozmeňovaniu osobných údajov v informačnom systéme alebo vymazaniu osobných údajov z informačného systému;

[96] § 3 ods. 3 ZOOÚ.
[97] Tamže.
[98] § 5 i) ZOOÚ.
[99] § 69 ods. 1 ZOOÚ.
[100] § 69 ods. 3 ZOOÚ.

- kontrolu užívateľa informačného systému, aby sa zabránilo použitiu systémov automatizovaného spracúvania neoprávnenými osobami pomocou zariadenia na prenos osobných údajov;
- kontrolu prístupu k osobným údajom, aby sa zabezpečilo, že osoby oprávnené používať systém automatizovaného spracúvania budú mať prístup iba k tým osobným údajom, na ktoré sa vzťahuje ich oprávnenie na prístup;
- kontrolu prenosu údajov, aby sa zabezpečila možnosť overiť a zistiť subjekty, ktorým sa preniesli osobné údaje alebo poskytli osobné údaje, alebo overiť a zistiť subjekty, ktorým sa môžu preniesť osobné údaje, alebo poskytnúť osobné údaje prostredníctvom zariadenia na prenos osobných údajov;
- kontrolu vkladania údajov do informačného systému, aby sa zabezpečilo, že bude možné overiť a zistiť, aké osobné údaje sa vložili do systému automatizovaného spracúvania, a kedy a kto ich tam vložil;
- kontrolu prepravy osobných údajov, aby sa zabránilo neoprávnenému čítaniu osobných údajov, kopírovaniu osobných údajov, pozmeňovaniu osobných údajov alebo vymazaniu osobných údajov počas ich prenosu alebo počas prepravy nosiča osobných údajov;
- obnovu osobných údajov, aby sa zabezpečilo, že sa inštalované systémy obnovia, ak dôjde k ich prerušeniu;
- zabezpečenie spoľahlivosti informačného systému, aby sa zabezpečilo, že funkcie tohto systému fungujú a hlási sa výskyt chýb v jeho funkciách;
- zabezpečenie integrity informačného systému, aby sa uchovávané osobné údaje nemohli poškodiť, ak nastane porucha tohto systému.

Špecifické pravidlá sa týkajú príslušných orgánov aj pri nahlasovaní porušení ochrany osobných údajov. Oznámenie sa v zmysle § 72 ZOOÚ vykoná *„orgánu členského štátu príslušnému na plnenie úloh na účely trestného konania, ak porušenie ochrany osobných údajov zahŕňa osobné údaje, ktorých prenos vykonal orgán členského štátu príslušný na plnenie úloh na účely trestného konania alebo ktoré boli prenesené takému orgánu.“* Oznamovacia povinnosť platí rovnako ako pri porušeniach podľa GDPR voči Úradu na ochranu osobných údajov SR. Príslušný orgán má však možnosť oznámenia odložiť, obmedziť alebo od neho úplne upustiť ak by vzhľadom na oznámenie porušenia:

- by mohlo dôjsť k ovplyvňovaniu alebo mareniu úradného postupu alebo súdneho postupu alebo šetrenia;
- by mohlo dôjsť k ohrozeniu plnenia úloh na účely trestného konania;
- je to potrebné na zabezpečenie ochrany verejného poriadku alebo bezpečnosti štátu; alebo

- je to potrebné na ochranu práv iných osôb.[101]

Súhrnne tak možno konštatovať, že právna úprava bezpečnosti pri implementácií Policajnej smernice je striktnejšia a špecifickejšia ako pri GDPR. Takýto prístup je však absolútne relevantný a odôvodnený špecifickými úlohami a účelmi vykonávanými príslušnými orgánmi.

2.6 Smernica PSD 2

Smernica Európskeho parlamentu a Rady (EÚ) 2015/2366 z 25. novembra 2015 o platobných službách na vnútornom trhu, ktorou sa menia smernice 2002/65/ES, 2009/110/ES a 2013/36/EÚ a nariadenie (EÚ) č. 1093/2010 a ktorou sa zrušuje smernica 2007/64/ES (ďalej len „smernica PSD 2") bola prijatá v súlade so stratégiou Európa 2020 a digitálnou agendou s cieľom prispieť k vytvoreniu harmonizovaného trhu elektronických platieb v rámci celej Európskej únie. Ako sa uvádza v samotnej smernici PSD 2, konkrétne v bode 3 preambuly, smernica 2007/64/ES bola prijatá ešte v decembri 2007 (na základe návrhu Komisie z roku 2005), pričom retailový platobný trh od tej doby prešiel značnými technickými inováciami a rýchlym nárastom počtu elektronických a mobilných platieb, a taktiež došlo k príchodu nových druhov platobných služieb na trh, čo predstavuje výzvy pre súčasný právny rámec. Aj preto je ďalší vývoj platobného trhu, resp. platobných služieb z regulačného hľadiska spojený s významnými výzvami. V bode 4 preambuly smernice PSD 2 uvádza, že významné oblasti platobného trhu, predovšetkým platby kartou, internetové a mobilné platby zostávajú v jednotlivých členských štátoch Európskej únie roztrieštené. Preto je harmonizácia v tejto oblasti dôležitá, objem využívaných elektronických služieb, ako aj využívanie mobilných platieb má stúpajúcu tendenciu. Rozširujú sa okruhy platobných služieb o nové typy, čo má za následok zvyšovanie úrovne digitalizácie v oblasti poskytovania platobných služieb. Ako bolo uvedené vyššie, smernica PSD 2 bola prijatá s cieľom prispieť **k vytvoreniu harmonizované trhu** platobných služieb, vďaka čomu používatelia platobných služieb (najmä spotrebitelia a maloobchodníci, ako aj ďalší účastníci) budú môcť v plnej miere využívať ďalšie prínosy vnútorného trhu.

Primárnymi cieľmi smernice PSD 2 sú:

- posilnenie transparentnosti a možnosti rýchlejšieho prijímania inovácií v oblasti platobných služieb a tým prispieť k účinnému a efektívnemu trhu s platbami,
- zavedenie nových prvkov s cieľom uľahčiť používanie elektronických, najmä nízkonákladových internetových a mobilných platieb (napr. bod 29 preambuly),

[101] § 72 ods. 2 ZOOÚ

- zabezpečenie nediskriminačných podmienok pre poskytovateľov platobných služieb, vrátane možnosti vstupu nových hráčov na trh platobných služieb a tým prispieť k vytvoreniu zdravého konkurenčného prostredia v tejto oblasti (napr. body 6 a 50 preambuly).
- **zavedenie nových bezpečnostných opatrení za účelom zmierňovania rizík v oblasti bezpečnosti platieb, ako aj posilnenie práv spotrebiteľov a nárast ich informovanosti s cieľom prispieť k zvýšeniu ochrany spotrebiteľov (napr. bod 54, 91, 92, 95 preambuly),**

Smernica PSD 2 osobitne upravuje v čl. 96 problematiku **nahlasovania bezpečnostných incidentov**, kedy poskytovatelia platobných služieb bez zbytočného odkladu informujú príslušný orgán v domovskom členskom štáte Európskej únie poskytovateľa platobných služieb o závažnom prevádzkovom alebo bezpečnostnom incidente. V čl. 97 predmetnej smernice je taktiež osobitne upravená **autentifikáciu zákazníkov** do platobných služieb, kde sa v zmysle smernice vyžaduje silná autentifikácie.

2.7 Návrh nariadenia o súkromí a elektronických komunikáciách

V rámci **Stratégie pre jednotný digitálny trh v Európe** bolo oznámené preskúmanie **smernice Európskeho parlamentu a Rady2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií** (ďalej len „smernica o súkromí a elektronických komunikáciách"), s cieľom zabezpečiť prísne pravidlá ochrany súkromia pre používateľov elektronických komunikačných služieb a rovnaké podmienky pre všetkých účastníkov trhu.

Smernicou o súkromí a elektronických komunikáciách sa zabezpečuje ochrana základných práv a slobôd, najmä rešpektovanie súkromného života, dôvernosť komunikácií a ochrana osobných údajov v sektore elektronických komunikácií. Tiež sa ňou zaručuje voľný pohyb údajov z elektronických komunikácií, ako aj elektronických komunikačných zariadení a služieb v EÚ.[102]

Hoci zásady a hlavné ustanovenia smernice o súkromí a elektronických komunikáciách zostávajú vo všeobecnosti uspokojivé, daná smernica nedrží v plnej miere krok s technologickým vývojom a realitou na trhu, čo má za následok nejednotnú alebo nedostatočne efektívnu ochranu súkromia a dôvernosti vo vzťahu k elektronickým komunikáciám.[103]

Od poslednej revízie smernice o súkromí a elektronických komunikáciách v roku 2009 však došlo k významnému technologickému a hospodárskemu vývoju. Spotrebitelia a podniky čoraz

[102] Návrh nariadenia Európskeho parlamentu a Rady o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách a o zrušení smernice 2002/58/ES (smernica o súkromí a elektronických komunikáciách), str. 2.
[103] Recitál 6 preambuly návrhu nariadenia o súkromí a elektronických komunikáciách.

častejšie namiesto tradičných komunikačných služieb využívajú nové internetové služby umožňujúce interpersonálnu komunikáciu, ako sú internetová telefónia, rýchle správy a e-mailové služby založené na webe. Na tieto internetové komunikačné (over-the-top) služby (ďalej len „OTT") sa vo všeobecnosti nevzťahuje aktuálny rámec elektronických komunikácií EÚ a ani smernica o súkromí a elektronických komunikáciách. Predmetná smernica teda nedrží krok s technologických vývojom, v dôsledku čoho nie sú komunikácie uskutočňované prostredníctvom nových služieb chránené. Ďalší vývoj predstavujú nové metódy sledovania správania koncových používateľov na internete, ktorých sa netýka predmetná smernica. Smernica o súkromí a elektronických komunikáciách by mala byť preto zrušená a nahradená **návrhom nariadenia Európskeho parlamentu a Rady o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách a o zrušení smernice 2002/58/ES (smernica o súkromí a elektronických komunikáciách)** (ďalej len „návrh nariadenia o súkromí a elektronických komunikáciách").[104]

V návrhu nariadenia o súkromí a elektronických komunikáciách sa skúma smernica o súkromí a elektronických komunikáciách z hľadiska dodržiavania cieľov Stratégie pre jednotný digitálny trh v Európe a zabezpečovania súladu so všeobecným nariadením o ochrane údajov.[105]

2.7.1 Pôsobnosť návrhu nariadenia o súkromí a elektronických komunikáciách

Návrh nariadenia o súkromí a elektronických komunikáciách upravuje vecnú a územnú pôsobnosť. **Vecná pôsobnosť** je upravená v článku 2 predmetného návrhu. V zmysle predmetného článku sa nariadenie uplatňuje na spracovávanie údajov z elektronických komunikácií uskutočňované v spojitosti s poskytovaním a využívaním elektronických komunikačných služieb a na informácie súvisiace s koncovými zariadeniami koncových používateľov.

V zmysle recitálu 8 predmetného návrhu by sa mal návrh predmetného nariadenia uplatňovať na:

- poskytovateľov elektronických komunikačných služieb,
- poskytovateľov verejne dostupných zoznamov,
- poskytovateľov softvéru umožňujúceho elektronické komunikácie vrátane vyhľadávania a prezentácie informácií na internete.
- fyzické a právnické osoby, ktoré používajú elektronické komunikačné služby na odosielanie priamych marketingových obchodných komunikácií alebo získavanie informácií súvisiacich s koncovými zariadeniami koncových používateľov alebo uložených v týchto zariadeniach.

[104] Návrh nariadenia o súkromí a elektronických komunikáciách, s. 2 a recitál 6 preambuly.
[105] Tamtiež.

Negatívne vymedzenie vecnej pôsobnosti je upravené v článku 2 ods. 2 návrhu nariadenia o súkromí a elektronických komunikáciách. V zmysle tohto ustanovenia sa predmetný návrh neuplatňuje na:

a) činnosti, ktoré nepatria do pôsobnosti práva EÚ,

b) činnosti členských štátov, ktoré patria do rozsahu pôsobnosti kapitoly 2 hlavy V Zmluvy o Európskej únii,

c) elektronické komunikačné služby, ktoré nie sú verejne dostupné,

d) činnosti príslušných orgánov na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo výkonu trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a jeho predchádzania.

Územná pôsobnosť je upravená v článku 3 ods. 1 písm. a) – c) návrhu nariadenia o súkromí a elektronických komunikáciách. V zmysle predmetných ustanovení sa návrh nariadenia sa uplatňuje na:

a) poskytovanie elektronických komunikačných služieb koncovým používateľom v EÚ, bez ohľadu na to, či sa od koncového používateľa vyžaduje platba,

b) využívanie takýchto služieb,

c) ochranu informácií súvisiacich s koncovými zariadeniami koncových používateľov, ktoré sa nachádzajú v EÚ.

V súvislosti s územnou pôsobnosťou sa v recitáli 9 predmetného návrhu dodáva, že nariadenie by sa malo uplatňovať na údaje z elektronických komunikácií spracúvané v súvislosti s poskytovaním a používaním elektronických komunikačných služieb v EÚ, a to bez ohľadu na to, či sa spracovanie vykonáva v EÚ. Taktiež platí, že predmetný návrh nariadenia by sa mal uplatňovať aj na údaje z elektronických komunikácií v súvislosti s poskytovaním elektronických komunikačných služieb z krajín mimo EÚ koncovým používateľom v EÚ.

V prípade ak poskytovateľ elektronických komunikačných služieb nie je usadený v EÚ, písomne určí svojho **zástupcu** v EÚ. Tento zástupca musí byť usadený v jednom z členských štátov EÚ, v ktorom sa nachádzajú koncoví používatelia takýchto elektronických komunikačných služieb.[106] Zástupca má právomoc odpovedať na otázky a poskytovať informácie najmä dozorným orgánom a koncovým používateľom v súvislosti so všetkými záležitosťami týkajúcimi sa spracovávania údajov z elektronických komunikácií, a to popri poskytovateľovi, ktorého zastupuje, alebo namiesto neho.[107]

[106] Tamtiež, čl. 3 ods. 2 – 5.
[107] Tamtiež,ods. 4.

2.8 Národná úroveň

Ochrana informácií, IKT ktoré tieto informácie spracúvajú a ochrana kybernetického priestoru je v právnom poriadku Slovenskej republiky upravená viacerými právnymi predpismi. V tejto časti učebnice budeme venovať pozornosť právne nezáväzným aktom a legislatívnym aktom, ktoré čiastkovo upravujú otázky informačnej a kybernetickej bezpečnosti.

2.8.1 Právne nezáväzné akty

Národná stratégia pre informačnú bezpečnosť SR

Hlavným dokumentom, ktorý sa zaoberá oblasťou **informačnej bezpečnosti**, je **Národná stratégia pre informačnú bezpečnosť SR**, ktorú 27. augusta 2008 schválila bez pripomienok Vláda Slovenskej republiky.[108] Na národnú stratégiu nadväzuje **Akčný plán informačnej bezpečnosti**[109].

Podľa **Národnej stratégie pre informačnú bezpečnosť SR** je informačná bezpečnosť definovaná ako:

„(1) Ochrana informácie a informačno-komunikačných technológií a systémov pred neoprávneným prístupom, použitím, zverejnením, poškodením, modifikáciou alebo zničením, aby sa zaistila dôvernosť, integrita a dostupnosť informácie,

(2) schopnosť systému na danej úrovni spoľahlivosti odolávať náhodným udalostiam aj zámerným akciám, ktoré kompromitujú dostupnosť, autentickosť, integritu a dôvernosť uložených alebo prenášaných údajov a služby poskytované alebo sprístupňované daným systémom,

(3) interdisciplinárna oblasť zaoberajúca sa ochranou informačno-komunikačných technológií."[110]

V zmysle vyššie uvedenej definície informačnej bezpečnosti sa v Slovenskej republike rozlišuje jednak medzi ochranou utajovaných skutočností, ktorú má vo svojej kompetencii Národný bezpečnostný úrad a medzi ochranou všetkých ostatných údajov (tzv. neutajovaných), ktoré spravuje Ministerstvo financií Slovenskej republiky.

Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020

Problematika kybernetickej bezpečnosti je na národnej úrovni predmetom **Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020**.[111] K vypracovaniu tohto dokumentu sa vláda Slovenskej republiky zaviazala do konca roka 2014 v Správe o bezpečnosti Slovenskej republiky za rok 2013. Koncepcia vychádza z uvedenia a opisu základných pojmov,

---

[108] Vláda Slovenskej republiky materiál (č. mat. ÚV-18175/2008) schválila 27. augusta 2008 uznesením č.570/2008. Dostupné na: http://www.informatizacia.sk/narodna-strategia-pre-ib/6783s.

[109] Vláda Slovenskej republiky materiál (č. mat. ÚV-30315/2009) schválila 19. januára 2010 uznesením č.46/2010. Dostupné na: http://www.informatizacia.sk/narodna-strategia-pre-ib/6783s.

[110] VLÁDA SLOVENSKEJ REPUBLIKY: *Národná stratégia pre informačnú bezpečnosť SR. Príloha č. 5: Definície pojmov.* Bratislava, 2008, s. 2.

[111] Schválená vládou Slovenskej republiky dňa 17.06.2015. Dostupné na: http://www.rokovanie.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=24702.

základných princípov, charakteristiky aktuálneho stavu strategického, legislatívneho a inštitucionálneho rámca v oblasti kybernetickej bezpečnosti v Slovenskej republike, ako aj zo strategického a metodického rámca formovaného dokumentmi NATO a Európskej únie a z nich následne formuluje princípy, ciele a návrhy riešení.

V zmysle prílohy predmetnej koncepcie, ktorá vymedzuje vybrané pojmy, ako aj význam kľúčových pojmov, je kybernetická bezpečnosť vymedzená ako: *„súhrn právnych, organizačných a technických prostriedkov na zaistenie ochrany kybernetického priestoru."*[112]

Predmetný dokument poukazuje na značné nedostatky v oblasti kybernetickej bezpečnosti, a to najmä v absentujúcej právnej úprave, ktorá by regulovala ochranu národného kybernetického priestoru. Práve chýbajúcu legislatívu v tejto oblasti považuje koncepcia za najzávažnejší problém a na viacerých miestach poukazuje na nutnosť prijatia komplexnej právnej úpravy v tejto oblasti. Ďalej predmetný dokument poukazuje na nedostatočnú inštitucionálnu základňu v oblasti kybernetickej bezpečnosti, nedostatočne rozvinutú spoluprácu medzi verejným sektorom a súkromným sektorom, akademickou sférou a občianskou spoločnosťou.

Strategickým cieľom kybernetickej bezpečnosti Slovenskej republiky je: *„otvorený, bezpečný a chránený národný kybernetický priestor, t.j. vybudovanie dôvery v spoľahlivosť a bezpečnosť najmä kritickej informačnej a komunikačnej infraštruktúry, ako aj istoty, že táto bude plniť svoje funkcie a slúžiť národným záujmom aj v prípade kybernetického útoku."*[113]

Koncepcia sa zaoberá taktiež otázkou **inštitucionálneho rámca kybernetickej bezpečnosti**. Na národnej úrovni by mala patriť problematika kybernetickej bezpečnosti do pôsobnosti príslušného ústredného orgánu štátnej správy, ktorého kompetencie a pôsobnosť všeobecne vymedzí kompetenčný zákon a konkrétne stanoví osobitný právny predpis (zákon o kybernetickej bezpečnosti). Koncepcia odporúča, aby túto pôsobnosť zákonodarca zveril **Národnému bezpečnostnému úradu.**[114]

V rámci otázky inštitucionálneho rámca sa navrhuje zriadiť:

- **Ústredný orgán štátnej správy pre kybernetickú bezpečnosť** - rozšírená pôsobnosť existujúceho odvetvovo nezávislého ústredného orgánu štátnej správy o ďalší úsek štátnej správy.
- **Národná jednotka pre riešenie incidentov (národný CERT/CSIRT)** - osobitné pracovisko s vecnou pôsobnosťou v oblasti kybernetickej bezpečnosti na národnej úrovni v riadiacej

[112] ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY: *Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020.* Bratislava 2015. Príloha č. 1. s. 2.
[113] Tamtiež, s. 9.
[114] V závere koncepcia sumarizuje hlavné dôvody prijatia takéhoto koncepčného materiálu pre oblasť kybernetickej bezpečnosti. Týmito dôvodmi sú najmä ochrana národného kybernetického priestoru, plnenia záväzkov Slovenskej republiky ako členskej krajiny Európskej únie a NATO a iných medzinárodných záväzkov, skúsenosti z ostatných členských krajín, optimalizácia spolupráce medzi orgánmi verejnej moci navzájom, ako aj medzi verejnou mocou a súkromnou a akademickou sférou, ako aj odstránenie duplicít.

pôsobnosti Ústredného štátneho orgánu pre kybernetickú bezpečnosť[115] (plní tiež úlohy „tímu reakcie na núdzové počítačové situácie" v zmysle smernice NIS).

- **Vecne príslušná autorita pre kybernetickú bezpečnosť** - organizačný útvar existujúcich ústredných štátnych orgánov. V rámci svojej vecnej pôsobnosti zaisťuje kybernetickú bezpečnosť.
- **Jednotka pre riešenie incidentov (vládny CERT/CSIRT, CERT/CSIRT XY)** - osobitné pracovisko ústredného štátneho orgánu - vecne príslušnej autority pre kybernetickú bezpečnosť.[116]
- **Formálna platforma pre spoluprácu na národnej úrovni** - umožní účasť reprezentantov podnikateľskej a akademickej sféry na príprave a vytváraní vládnych rozhodnutí formou predkladania odporúčaní, alebo názorov na rozvoj a nepretržité zlepšovanie systému zabezpečenia kybernetickej bezpečnosti v Slovenskej republike.[117]

Na Koncepciu nadväzuje **Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020[118].** Jedným z cieľov stanovených v koncepcii bolo aj predloženie **návrhu zákona o kybernetickej bezpečnosti,** ktorý by ucelene pokryl oblasť kybernetickej bezpečnosti.

Kybernetickej bezpečnosti sa ďalej venuje dokument **Príprava Slovenskej republiky na plnenie úloh v oblasti kybernetickej obrany**, vyplývajúcich z cieľov spôsobilostí Slovenskej republiky. Tento dokument vymedzuje národné spôsobilosti Slovenskej republiky v oblasti kybernetickej obrany, ktoré bude nevyhnutné vybudovať a rozvíjať do konca roka 2017. V zmysle tohto dokumentu Národný bezpečnostný úrad bude plniť úlohy, ktoré súvisia so zabezpečením a koordinovaním vybudovania spôsobilostí Slovenskej republiky v oblasti kybernetickej obrany.[119]

---

[115] V texte Koncepcie sa na viacerých miestach používa pojem „Ústredný štátny orgán". Z legislatívneho hľadiska, ako aj z hľadiska pojmov, ktoré používa správne právo, by bolo vhodnejšie používať pojem „Ústredný orgán štátnej správy". Bližšie pozri: VRABKO, M. a kol.: Správne právo hmotné. Všeobecná časť. 1. vydanie. Bratislava: C. H. Beck, 2012, s. 127.

[116] Nepredpokladá sa fyzické zriadenie odvetvových jednotiek v každom odvetví správy. Je však potrebné zabezpečiť realizáciu týchto funkcionalít v rámci jednotlivých odvetví správy. Vládny CERT/CSIRT je jednotka pre riešenie incidentov v pôsobnosti Ministerstva financií SR pre informačné systémy verejnej správy a pre vybrané informačné systémy kritickej infraštruktúry.

[117] Túto platformu má predstavovať Komisia pre kybernetickú bezpečnosť ako stály odborný poradný orgán riaditeľa Národného bezpečnostného úradu pre uplatňovanie štátnej politiky v oblasti kybernetickej bezpečnosti v Slovenskej republike. Vláda Slovenskej republiky vzala na vedomie Návrh Štatútu Komisie pre kybernetickú bezpečnosť. Dostupné na: http://www.rokovanie.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=25017.

[118] Dostupné na: http://www.rokovania.sk/File.aspx/ViewDocumentHtml/Mater-Dokum-197723?prefixFile=m_.

[119] Ďalšími strategickými, resp. koncepčnými dokumentmi, ktorých obsah sa čiastočne venuje problematike ochrany kybernetického priestoru resp. kybernetickej bezpečnosti sú:
- Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany, schválená uznesením vlády SR č. 120/2007.
- Národná politika pre elektronické komunikácie na roky 2009 - 2013, schválená uznesením vlády SR č. 360/2009.
- Správy o plnení úloh Akčného plánu na roky 2009 až 2013 k dokumentu Národná stratégia pre informačnú bezpečnosť v SR, materiály vláda SR vzala každoročne na vedomie od roku 2010 do roku 2014.
- Biela kniha o obrane Slovenskej republiky, schválená uznesením vlády SR č. 326/2013.
- Správa o bezpečnosti Slovenskej republiky za rok 2012, schválená uznesením vlády SR č. 325/2013.
- Operačný program Integrovaná infraštruktúra 2014 - 2020, schválený uznesením vlády SR č. 171/2014.

2.8.2 Legislatívne akty

2.8.2.1 Zákon o kybernetickej bezpečnosti

Od 1. apríla 2018 je účinný **zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti** a o zmene a doplnení niektorých zákonov (ďalej len „zákon o kybernetickej bezpečnosti). Predmetný zákon je reakciou na povinnosť transponovať smernicu NIS".

Pôsobnosť zákona o kybernetickej bezpečnosti

Zákon o kybernetickej bezpečnosti 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.

V rámci tejto kapitoly sa budeme venovať len vybraným inštitútom, ktoré upravuje predmetný zákon. Menovite upriamime našu pozornosť na pôsobnosť orgánov verejnej moci, postavenie a povinnosti PZS a PDS, jednotný informačný systém kybernetickej bezpečnosti a jednotky CSIRT.

Pôsobnosť orgánov verejnej moci

Ústredným orgánom štátnej správy v oblasti kybernetickej bezpečnosti je od. 1. januára 2016 **Národný bezpečnostný úrad** (ďalej len „NBÚ")[120]. NBÚ je aj národným kontaktným miestom v zmysle smernice NIS. Postavenie NBÚ ako ústredného orgánu štátnej správy pre kybernetickú bezpečnosť bolo definované už v Koncepcii kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020.[121]

- Správa o bezpečnosti Slovenskej republiky za rok 2013, schválená uznesením vlády SR č. 276/2014.

[120] § 34 zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy. NBÚ sa stal ústredným orgánom štátnej správy pre kybernetickú bezpečnosť zákonom č. 339/2015 Z. z. ktorým sa mení a dopĺňa zákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov.

[121] Dostupné na: http://www.nbusr.sk/wp-content/uploads/kyberneticka-bezpecnost/Koncepcia-kybernetickej-bezpecnosti-SR-na-roky-2015-2020-A4.pdf.

NBÚ plní v oblasti kybernetickej bezpečnosti v zmysle § 5 zákona o kybernetickej bezpečnosti 24 úloh. Medzi tieto úlohy patrí napr. správa a prevádzkovanie jednotného informačného systému kybernetickej bezpečnosti, akreditácia jednotiek CSIRT, vypracovanie národnej stratégie kybernetickej bezpečnosti a pod.. NBÚ taktiež zaradzuje základné služby a digitálne služby do zoznamov a PZS a PDS do registrov. V zmysle § 6 zákona o kybernetickej bezpečnosti má NBÚ postavenie národnej jednotky CSIRT. Táto jednotka je zaradená do zoznamu akreditovaných jednotiek CSIRT zo zákona a nepodlieha akreditácii.

V zákone o kybernetickej bezpečnosti sú špecificky upravené úlohy **ústredných orgánov**[122], ktoré v rozsahu svojej pôsobnosti pre príslušný sektor alebo podsektor v zmysle prílohy č. 1 predmetného zákona zodpovedajú za zabezpečenie kybernetickej bezpečnosti, a to tým, že napr. plnia úlohy jednotky CSIRT, určujú v spolupráci s NBÚ špecifické sektorové identifikačné kritéria, identifikujú základnú službu a prevádzkovateľa základných služieb a i.[123]

Postavenie a povinnosti PZS a PDS

V zmysle zákona o kybernetickej bezpečnosti existuje niekoľko spôsobov ako dôjde k zaradeniu základnej služby alebo digitálnej služby do príslušného zoznamu alebo zaradeniu PZS resp. PDS do príslušného registra.

V prípade základných služieb a ich prevádzkovateľov platí, že ak entita zistí, že došlo k prekročeniu identifikačných kritérií prevádzkovanej služby a takáto entita patrí do niektorého zo sektorov podľa prílohy č. 1, je povinná urobiť oznámenie do 30 dní odo dňa, keď sa o prekročení identifikačných kritérií dozvedela. Takéto oznámenie obsahuje konkrétne informácie a je adresované NBÚ. Právny základ pre zaradenie základnej služby do zoznamu základných služieb a PZS do registra PZS závisí od jednotlivých druhov základných služieb.

Slovenský zákonodarca definuje tri druhy základných služieb. V zmysle § 3 písm. k) zákona o kybernetickej bezpečnosti je základnou službou služba, ktorá je zaradená v zozname základných služieb a:

a) závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1,

b) je informačným systémom verejnej správy[124], alebo

[122] Medzi ústredné orgány patria 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.

[123] Zákon o kybernetickej bezpečnosti taktiež definuje aj okruh iných orgánov štátnej správy. Pozri § 4 písm. c).

[124] § 2 ods. 1 písm. b) zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov.

c) je prvkom kritickej infraštruktúry[125].

V prípade ak ide o zaradenie **základnej služby typu A** platí, že NBÚ zaradí túto službu zo zoznamu základných služieb a jej prevádzkovateľa do registra PZS:

a) na základe oznámenia prevádzkovateľom tejto služby,

b) na základe podnetu ústredného orgánu, ak došlo k prekročeniu identifikačných kritérií prevádzkovanej služby podľa § 18,

c) z vlastnej iniciatívy, ak sa NBÚ dozvedel o prekročení identifikačných kritérií prevádzkovanej služby podľa § 18 a nedošlo k postupu podľa písmena a) alebo písmena b).[126]

V prípade **základných služieb typu B** (služba ako informačný systém verejnej správy) platí, že NBÚ v spolupráci s príslušným ústredným orgánom zaradí základnú službu do zoznamu základných služieb a jej prevádzkovateľa do registra PZS.[127]

V súvislosti so **základnými službami typu C** platí, že NBÚ zaradí takúto základnú službu do zoznamu základných služieb a jej prevádzkovateľa do registra PZS zo zákona.[128]

Zaradenie základnej služby do zoznamu základných služieb a jej prevádzkovateľa do registra PZS oznámi NBÚ prevádzkovateľovi tejto služby prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.[129]

Aby došlo k zaradeniu základnej služby do zoznamu základných služieb a jej prevádzkovateľa do registra PZS, musí príslušná základná služba, ktorú poskytuje entita prekročiť **identifikačné kritériá prevádzkovanej služby**. V zmysle § 18 zákona o kybernetickej bezpečnosti sa identifikačné kritéria prevádzkovanej služby delia na:

a) dopadové kritéria

b) špecifické sektorové kritériá

Dopadové kritériá vychádzajú z čl. 6 smernice NIS, ktorý upravuje faktory pre určenie závažnosti rušivého vplyvu. Podrobnosti o dopadových a špecifických sektorových kritériách pre základnú službu je upravené vo vyhláške.[130] Na tomto mieste je potrebné podotknúť, že európsky zákonodarca určuje identifikačné kritéria PZS a nie pre základné služby. Zatiaľ čo slovenský zákonodarca upravuje identifikačné kritéria prevádzkovanej služby a ak entita tieto kritéria prekročí následne možno hovoriť o tom, že má postavenie PZS.

PZS je v zmysle § 19 ods. 1 zákona o kybernetickej bezpečnosti povinný do šiestich mesiacov odo dňa oznámenia o zaradení do registra PZS prijať a dodržiavať všeobecné bezpečnostné

[125] § 2 písm. a) zákona č. 45/2011 Z. z. o kritickej infraštruktúre.
[126] § 17 ods. 2 zákona o kybernetickej bezpečnosti.
[127] Tamtiež, § 17 ods. 3.
[128] Tamtiež, § 17 ods. 4.
[129] Tamtiež, § 17 ods. 5.
[130] Vyhláška Národného bezpečnostného úradu č. 164/2018 Z. z. ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby).

opatrenia najmenej v rozsahu bezpečnostných opatrení podľa § 20 a sektorové bezpečnostné opatrenia, ak sú prijaté. PZS je okrem iného povinný hlásiť závažný kybernetický bezpečnostný incident a riešiť kybernetický bezpečnostný incident. V súvislosti s povinnosťou riešiť kybernetický bezpečnostný incident sa podľa môjho názoru majú na mysli len incidenty, ktoré súvisia s základnou službou, ktorú prevádzkovateľ poskytuje.

V prípade PDS platí, že poskytovateľ je povinný do 30 dní odo dňa začatia poskytovania digitálnej služby oznámiť úradu názov a sídlo, kontaktné údaje, poskytovanú službu, názov, sídlo a kontaktné údaje zástupcu podľa § 23.

NBÚ zaradí službu do zoznamu digitálnych služieb a jej poskytovateľa do registra PDS na základe oznámenia alebo aj na základe vlastného zistenia. Zaradenie služby do zoznamu digitálnych služieb a jej poskytovateľa do registra PDS oznámi NBÚ poskytovateľovi tejto služby.[131]

V prípade ak PDS poskytuje digitálnu službu v Slovenskej republike, nemá sídlo v Európskej únii a neustanovil si svojho zástupcu v inom členskom štáte Európskej únie, je povinný si ustanoviť svojho zástupcu v Slovenskej republike.[132]

Hlásenie bezpečnostných kybernetických incidentov

PZS je v zmysle § 19 ods. 6 písm. b) zákona o kybernetickej bezpečnosti povinný bezodkladne hlásiť **závažný kybernetický bezpečnostný incident**. Rovnakú povinnosť musí PZS splniť aj v zmysle § 24 ods.1 predmetného zákona. PZS identifikuje závažný kybernetický bezpečnostný incident na základe presiahnutia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov. V zmysle zákona o kybernetickej bezpečnosti sa závažné kybernetické bezpečnostné incidenty členia na kategórie prvého, druhého a tretieho stupňa. Stanovenie konkrétneho stupňa závisí od nasledujúcich faktorov:

a) počtu používateľov základnej služby alebo digitálnej služby zasiahnutých kybernetickým bezpečnostným incidentom,
b) dĺžky trvania kybernetického bezpečnostného incidentu,
c) geografického rozšírenia kybernetického bezpečnostného incidentu,
d) stupňa narušenia fungovania základnej služby alebo digitálnej služby,
e) rozsahu vplyvu kybernetického bezpečnostného incidentu na hospodárske alebo spoločenské činnosti štátu.

[131] § 21 zákona o kybernetickej bezpečnosti.
[132] Tamtiež, § 23 ods. 2.

Presná špecifikácia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov je predmetom vyhlášky.[133] PZS a PDS majú povinnosť hlásiť kybernetické bezpečnostné incidenty prostredníctvom JISKB.[134]

V porovnaní s PZS, sú PDS v zmysle § 22 ods. 3 písm. a) zákona o kybernetickej bezpečnosti hlásiť každý kybernetický bezpečnostný incident, a to za predpokladu, že PDS disponuje informáciami na základe ktorých je spôsobilý identifikovať, či má tento kybernetický bezpečnostný incident podstatný vplyv podľa osobitného predpisu[135], a to bezodkladne po jeho zistení.

Na tomto mieste je potrebné podotknúť, že v zmysle smernice NIS má PZS, ako aj PDS povinnosť hlásiť **incidenty, ktoré majú závažný vplyv** na kontinuitu základných služieb, resp. závažný rušivý vplyv na poskytovanie digitálnych služieb. S cieľom určiť závažnosť vplyvu incidentu sa zohľadňujú konkrétne parametre osobitne pre základné služby a digitálne služby.

Parametre pre určenie závažnosti vplyvu incidentu na kontinuitu základných služieb, ktoré PZS poskytujú sú najmä: počet používateľov postihnutých narušením základnej služby; dĺžka trvania incidentu a geografické rozšírenie z hľadiska oblasti, ktorú incident postihol.[136]

Pre určenie závažnosti vplyvu na poskytované digitálne služby sú najmä tieto parametre: počet používateľov postihnutých incidentom, najmä používateľov využívajúcich danú službu na účely poskytovania vlastných služieb; dĺžka trvania incidentu; geografické rozšírenie z hľadiska oblasti, ktorú incident postihol; stupeň narušenia fungovania služby; rozsah vplyvu na hospodárske a spoločenské činnosti.[137]

V zákone o kybernetickej bezpečnosti boli parametre pre určenie závažnosti vplyvu incidentu na kontinuitu základných služieb a pre určenie závažnosti vplyvu na poskytované digitálne služby v zmysle smernice NIS spojené do jedného, a to pre účely stanovenia stupňa závažného kybernetického bezpečnostného incidentu.

Jednotný informačný systém kybernetickej bezpečnosti

Jednotný informačný systém kybernetickej bezpečnosti (ďalej len „JISKB“) predstavuje základný komunikačný kanál medzi NBÚ a ostatnými entitami v oblasti kybernetickej bezpečnosti.

[133]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.
[134] § 24 ods. 4 a § 25 ods. 1 zákona o kybernetickej bezpečnosti.
[135] 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).
[136] Čl. 14 ods. 4 smernice NIS.
[137] Tamtiež, čl. 16 ods. 4.

Jeho správcom a prevádzkovateľom má byť v zmysle zákona o kybernetickej bezpečnosti NBÚ. NBÚ sprístupní JISKB do 18 mesiacov od účinnosti predmetného zákona.[138]

JISKB obsahuje komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálny systém včasného varovania. V súvislosti s prístupom k JISKB má tento informačný systém verejnú časť a neverejnú časť. Verejná časť obsahuje príslušné registre PZS, PDS, ústredných orgánov, kybernetických bezpečnostných incidentov a zoznamy základných služieb, digitálnych služieb a akreditovaných jednotiek CSIRT.[139] Do neverejnej časti JISKB majú prístup v elektronickej forme, v reálnom čase a v rozsahu určenom NBÚ alebo osobitným predpisom na základe vecnej pôsobnosti ústredný orgán, jednotka CSIRT (zaradená v zozname akreditovaných jednotiek CSIRT), PZS, PDS, Národná banka Slovenska, Úrad na ochranu osobných údajov Slovenskej republiky a iný orgán verejnej moci rozhodnutím NBÚ.[140]

Z dikcie zákona o kybernetickej bezpečnosti vyplýva, že JISKB je primárnym komunikačným kanálom. Avšak, je potrebné myslieť aj na situácie, kedy by JISKB nemohol plniť svoj účel, napr. z dôvodu incidentu, ktorý by ochromil alebo znefunkčnil jeho prevádzku. Pre tieto prípady by sa mal aplikovať § 24 ods. 6 zákona o kybernetickej bezpečnosti. V zmysle predmetného ustanovenia platí, že NBÚ môže uzatvoriť písomnú zmluvu o spôsobe a forme hlásenia kybernetických bezpečnostných incidentov s PZS. Podobným spôsobom môže NBÚ uzavrieť zmluvu aj s PDS.[141]

Jednotky CSIRT

V zákone o kybernetickej bezpečnosti sa vytvorili tri kategórie jednotiek CSIRT. Prú kategóriu tvorí **národná jednotka CSIRT**. Postavenie národnej jednotky CSIRT má NBÚ a musí spĺňať všetky podmienky pre akreditáciu jednotiek CSIRT v zmysle § 14 zákona o kybernetickej bezpečnosti. Národná jednotka CSIRT (SK CERT)[142] plní úlohy jednotiek CSIRT pre všetky sektory a podsektory v zmysle prílohy č.1 a pre digitálne služby okrem tých sektorov a podsektorov, pre ktoré plní úlohy jednotky CSIRT ústredný orgán.[143] Národná jednotka CSIRT je akreditovaná zo zákona.

Druhou kategóriou je **vládna jednotka CSIRT**. Predmetná jednotka je v pôsobnosti Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu pre podsektor informačné systémy verejnej správy a musí spĺňať podmienky akreditácie podľa § 14 a plniť úlohy podľa § 15 zákona o kybernetickej bezpečnosti. Vládna jednotka CSIRT sa zaraďuje do zoznamu akreditovaných jednotiek CSIRT. Podobne ako národná jednotka CSIRT aj táto jednotka je akreditovaná zo zákona.[144]

---

[138] Tamtiež, § 34 ods. 1.
[139] Tamtiež § 8 ods. 2. Bližšie pozri: http://www.nbusr.sk/kyberneticka-bezpecnost/jednotny-informacny-system-kybernetickej-bezpecnosti/index.html.
[140] Tamtiež, § 8 ods. 5.
[141] Tamtiež, § 25 ods. 3.
[142] Dostupné na: http://www.nbusr.sk/kyberneticka-bezpecnost/sk-csirt/index.html.
[143] § 6 ods. zákona o kybernetickej bezpečnosti.
[144] Tamtiež, § 11.

V súvislosti so zriadením vládnej jednotky CSIRT je potrebné podotknúť, že existujúca jednotka CSIRT, ktorá je v rozpočtovej organizácii DataCentrum zriadenej Ministerstvom financií Slovenskej republiky je od 1. apríla 2018 v správe Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu.[145]

Tretiu kategóriu tvoria **akreditované jednotky CSIRT**. V zmysle zákona o kybernetickej bezpečnosti platí, že každý ústredný orgán na účely plnenia úloh jednotky CSIRT v rozsahu svojej pôsobnosti pre sektor alebo podsektor podľa prílohy č. 1 zriaďuje a prevádzkuje akreditovanú jednotku CSIRT. Zákon o kybernetickej bezpečnosti taktiež upravuje možnosť využitia akreditovanej jednotky CSIRT, ktorú zriaďuje a prevádzkuje iný ústredný orgán, ak sa tak dohodnú. V takýchto prípadoch pôjde o situácie, keď ústredný orgán nebude mať kapacity (personálne, technické a pod.) pre zriadenie jednotky CSIRT.[146]

V prípade ak ústredný orgán nevie zriadiť a prevádzkovať akreditovanú jednotku CSIRT a nevie využiť na tento účel ani akreditovanú jednotku CSIRT iného ústredného orgánu, tak NBÚ ako národná jednotka CSIRT bude plniť túto úlohu.[147]

2.8.2.2 Zákon o ITVS

Právna úprava informačných systémov verejnej správy (ďalej „ISVS“) a otázka ich bezpečnosti prešla v poslednom období výraznými zmenami. V prvom rade, zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ISVS“) bol zrušený zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ITVS“), ktorý nadobudol účinnosť 5. mája 2019.

Problematika bezpečnosti ISVS je v súčasnosti stále upravená vo výnose Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy. Predmetný výnos obsahuje bezpečnostné štandardy.[148]

Bezpečnosť ISVS je taktiež predmetom zákona o kybernetickej bezpečnosti, nakoľko za určitých okolností môže byť konkrétny ISVS zaradený medzi základné služby a jeho správca do registra prevádzkovateľov základných služieb. V takejto situácii je správca v pôsobnosti ktorého je konkrétny ISVS povinný plniť povinnosti v zmysle zákona o kybernetickej bezpečnosti.

V nasledujúcej časti kapitoly dôjde k ozrejmeniu pojmu informačná technológia verejnej správy, ktorý v sebe zahŕňa aj pojem informačný systém verejnej správy. Taktiež upriamime

[145] Tamtiež, § 34 ods. 10.
[146] Tamtiež, § 9 ods. 2.
[147] Tamtiež, § 6 ods. 2.
[148] Výnos Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy v znení neskorších predpisov zostáva platný a účinný do nadobudnutia účinnosti vykonávacieho právneho predpisu podľa § 31 zákona o ITVS, najneskôr však do 1. mája 2020.

pozornosť na ustanovenia zákona o ITVS, ktoré upravujú problematiku bezpečnosti informačných technológií verejnej správy. Následne poukážeme na zákon o KB a jeho vzťah k zákonu o ITVS, a to najmä z pohľadu bezpečnostných opatrení resp. iných povinností, ktoré musia konkrétne subjekty plniť, aby zabezpečili dostatočnú úroveň bezpečnosti informačných technológií verejnej správy, resp. ISVS.

Bezpečnosť ISVS v zákone o ITVS

Zákon o ITVS v porovnaní so zrušeným zákonom o ISVS definuje pojem informačné technológie verejnej správy (ďalej len „ITVS") a rozširuje svoju pôsobnosť aj na bezpečnosť týchto technológií. V zmysle § 2 ods. 2 zákona ITVS sú ITVS definované ako: *„informačná technológia v pôsobnosti správcu podporujúca služby verejnej správy, služby vo verejnom záujme alebo verejné služby*." Informačné technológie sú v zmysle § 2 ods. 1 zákona o ITVS chápané ako: *„prostriedok alebo postup, ktorý slúži na spracúvanie údajov alebo informácií v elektronickej podobe*." Zákon o ITVS uvádza príklady informačných technológií, konkrétne informačný systém, infraštruktúru, informačnú činnosť a elektronické služby. Definícia pojmu informačný systém verejnej správy zostala zachovaná v znení už zrušeného zákona o ISVS ako: *„informačný systém v pôsobnosti správcu podporujúci služby verejnej správy, služby vo verejnom záujme alebo verejné služby."* V prípade pojmu informačný systém došlo k zmene, nakoľko informačný systém predstavuje v zmysle § 2 ods. 2 zákona o ITVS: *„funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických prostriedkov a programových prostriedkov*."[149] V porovnaní s definíciou pojmu informačný systém v zmysle zrušeného zákona o ISVS nemusia byť technické prostriedky a programové prostriedky súčasťou informačného systému a taktiež tieto prostriedky nemôžu poskytovať iný informačný systém.

Bezpečnosť ITVS je v zákone o ITVS upravená v § 18 až § 23. Predmetný zákon upravuje bezpečnosť ITVS v oblasti:

- plánovania a organizácie (§ 19),
- obstarávania a implementácie (§ 20),
- prevádzky, servisu a podpory (§ 21),
- monitoringu a hodnotenia (§ 22),

V § 18 zákona o ITVS sú základné ustanovenia týkajúce sa situácie kedy je správca aj PZS v zmysle zákona o KB. V § 23 predmetného zákona sú upravené osobitné opatrenia na úseku bezpečnosti ITVS (napr. bezpečnostný projekt).

[149] V zmysle § 2 ods. 1 písm. a) zákona o ISVS bol informačný systém definovaný ako: *„funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických prostriedkov a programových prostriedkov, ktoré sú súčasťou informačného systému alebo ktoré informačnému systému poskytuje iný informačný systém."*

Správcom ITVS je v zmysle § 2 ods. 5 zákona o ITVS ten orgán riadenia[150], ktorého za správcu ITVS ustanoví zákon alebo je ustanovený na základe zákona o ITVS. Povinnosť správcu zabezpečiť riadenie bezpečnosti je zakotvená v § 14 ods. 1 písm. i) zákona o ITVS. V súvislosti s bezpečnostnými opatreniami je správca povinný:

- identifikovať potrebné bezpečnostné opatrenia (§ 19 ods. 1 písm. e) zákona o ITVS),
- určiť prostriedky na zabezpečenie implementácie a riadneho fungovania bezpečnostných opatrení (§ 19 ods. 1 písm. h) zákona o ITVS),
- realizovať bezpečnostné opatrenia (§ 19 ods. 3 písm. c) zákona o ITVS).

Povinnosti správcov ITVS v oblasti bezpečnosti ITVS budú detailne upravené vo vykonávacom právnom predpise, ktorý nahradí výnos Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy. Obsah bezpečnostných opatrení v novej vyhláške by mal reflektovať už existujúce bezpečnostné opatrenia, ktoré sú správcovia povinní realizovať.

Z pohľadu správcu ITVS bude dôležité, aké bezpečnostné opatrenia musí prijať a realizovať a taktiež, ktorý právny predpis má aplikovať pri prijímaní konkrétnych bezpečnostných opatrení. V zmysle § 18 ods. 1 zákona o ITVS je správca, ktorý je zároveň aj PZS povinný prijať a realizovať bezpečnostné opatrenia vo vzťahu k ISVS v jeho správe v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov v zmysle § 20 zákona o kybernetickej bezpečnosti. Avšak môže dôjsť k situácii, kedy správca v pozícii PZS nebude realizovať bezpečnostné opatrenia v zmysle zákona o kybernetickej bezpečnosti ale v zmysle zákona o ITVS. V zmysle § 18 ods. 2 zákona o ITVS platí, že zákon o ITVS ustanovuje: *„obsah bezpečnostných opatrení vo vzťahu k informačným systémom verejnej správy a spôsob a rozsah ich prijímania a realizácie v súlade s osobitným predpisom."* Týmto osobitným predpisom je zákon o kybernetickej bezpečnosti, konkrétne jeho § 2 ods. 2 písm. e), v zmysle ktorého sa zákon o kybernetickej bezpečnosti nevzťahuje na: *„požiadavky na zabezpečenie sietí a informačných systémov v sektore podľa osobitného predpisu, ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov ako podľa tohto zákona."* Predmetným osobitným predpisom je už zrušený zákon o ISVS.[151] Na základe vyššie uvedeného možno konštatovať, že v prípade ak zákon o ITVS stanoví pre správcu, ktorý je zároveň aj PZS, striktnejšie bezpečnostné opatrenia, bude musieť správca prijať a realizovať bezpečnostné opatrenia v zmysle zákona o ITVS. V praxi to bude pre správcu, ktorý je aj PZS znamenať, že bude musieť porovnávať bezpečnostné opatrenia v zmysle zákona o kybernetickej bezpečnosti a zákona o ITVS.

[150] Taxatívny zoznam orgánov riadenia je uvedený v § 5 ods. 2 zákona o ITVS.
[151] V zmysle § 33 ods. 1 zákona o ITVS: *„informačné systémy verejnej správy podľa doterajších predpisov sú informačnými systémami verejnej správy podľa tohto zákona."*

2.8.2.3 Zákon o e-Governmente

Problematika informačnej a kybernetickej bezpečnosti je čiastočne upravená aj v **zákone č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov** (ďalej len „zákon o e-Governmente"), najmä čo sa týka otázok súvisiacich s **elektronickou identitou**, **identifikáciou a autentifikáciou** osôb v kybernetickom priestore.[152]

Prijatím zákona o e-Governmente sa vytvorila všeobecná právna úprava spôsobu pre výkon pôsobnosti orgánov verejnej moci v elektronickej podobe (ďalej len „výkon verejnej moci elektronicky").[153] Vytvorením takéhoto právneho rámca malo dôjsť k realizácii elektronických služieb orgánov verejnej moci, a teda aj orgánov verejnej správy, pričom sa postupovalo jednotným spôsobom, tak aby nebolo potrebné zasahovať do každého osobitného právneho predpisu, ktorý tento výkon upravuje v konkrétnych prípadoch. Základným cieľom zákona o e-Governmente je zakotvenie elektronickej úradnej komunikácie ako kľúčovej formy komunikácie medzi osobami a orgánmi verejnej moci, ako aj medzi orgánmi verejnej moci navzájom.[154]

2.8.2.4 Zákon o dôveryhodných službách[155]

Reakciou na prijatie nariadenia eIDAS bolo v podmienkach Slovenskej republiky prijatie **zákona č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov** (ďalej len „zákon o dôveryhodných službách"),

---

[152] Bližšie pozri ANDRAŠKO, J. a kol.: *Digitálna verejná správa a elektronická identifikácia.* Bratislava : Právnická fakulta UK. 2019, 98 s. Dostupné na:
https://www.flaw.uniba.sk/fileadmin/praf/Veda/Publikacne_vystupy/2019/Monografia_DVSEI_2019.pdf

[153] V zmysle § 1 Zákona o e-Governmente tento zákon upravuje:
a) niektoré informačné systémy pre výkon pôsobnosti orgánov verejnej moci v elektronickej podobe (ďalej len „výkon verejnej moci elektronicky"),
b) elektronické podanie, elektronický úradný dokument a niektoré podmienky a spôsob výkonu verejnej moci elektronicky a elektronickej komunikácie,
c) elektronické schránky a elektronické doručovanie,
d) identifikáciu osôb a autentifikáciu osôb,
e)autorizáciu,
f) zaručenú konverziu,
g) spôsob vykonania úhrady orgánu verejnej moci,
h) referenčné registre.

[154] Orgány verejnej moci sú vo všeobecnosti povinné vykonávať verejnú moc elektronicky od 1. novembra 2013, s výnimkami upravenými v § 17 ods. 1 písm. a) až c) Zákona o e-Governmente. Všeobecná povinnosť vykonávať verejnú moc elektronicky bola odložená po dobu 3 rokov od účinnosti Zákona o e-Governmente v prípadoch, kedy sú na strane orgánu verejnej moci technické dôvody, pre ktoré nemôže verejnú moc vykonávať elektronicky a zároveň mu žiaden osobitný právny predpis výkon verejnej moci neukladá ako povinnosť. Odklad tejto všeobecnej povinnosti vypršal 1. novembra 2016.

[155] Slovenský zákonodarca používa pojem dôveryhodné služby, ktorý vychádza z nesprávneho prekladu nariadenia eIDAS. V súvislosti so slovenským prekladom nariadenia eIDAS je potrebné uviesť, že slovenská verzia nariadenia eIDAS používa pojem dôveryhodné služby. Zastávam názor, že pojem *trust services* v anglickej verzii predmetného nariadenia by mal byť preložený ako služby dôvery, resp. služby vytvárajúce dôveru, nakoľko hlavnou úlohou služieb poskytovaných v zmysle nariadenia eIDAS je zabezpečenie dôvery, a tá je obsahom a podstatou týchto služieb.

ktorý zrušil zákon č. 215/2002 Z. z o elektronickom podpise a doplnení niektorých zákonov, ako aj všetky súvisiace vyhlášky NBÚ.[156]

Tento zákon zaujal vo vzťahu k nariadeniu eIDAS minimalistický prístup, a preto je v zákone upravené iba to, čo predmetné nariadenie výslovne ponecháva na vnútroštátnu právnu úpravu. Ide teda o implementačný, resp. vykonávací právny predpis k nariadeniu eIDAS. Taktiež je potrebné dodať, že zákon o dôveryhodných službách nerieši všetky oblasti nariadenia eIDAS, ale iba tie, ktoré sú aplikovateľné od 1. júla 2016, tzn. problematiku služieb dôvery. Problematika vzájomného uznávania prostriedkov elektronickej identifikácie nie je upravená zákonom o dôveryhodných službách.

Zákon o dôveryhodných službách upravuje podmienky poskytovania služieb dôvery, povinnosti poskytovateľov služieb dôvery, pôsobnosť NBÚ v oblasti služieb dôvery, ako aj sankcie za porušenie povinností podľa nariadenia eIDAS a tohto zákona.[157]

Prijatím nariadenia eIDAS bolo potrebné zosúladiť terminológiu, ktorá sa týka elektronického podpisu, elektronickej pečate a časovej pečiatky. V zmysle § 17 ods. 2 zákona o dôveryhodných službách dochádza k nasledujúcim zmenám. Ak sa vo všeobecne záväzných právnych predpisoch používa pojem:

a) zaručený elektronický podpis, rozumie sa tým **kvalifikovaný elektronický podpis**,

b) zaručená elektronická pečať, rozumie sa tým **kvalifikovaná elektronická pečať**,

c) časová pečiatka, rozumie sa tým **kvalifikovaná elektronická časová pečiatka**.

V zmysle zákona o dôveryhodných službách môže kvalifikovaný elektronický podpis, kvalifikovaný certifikát pre elektronický podpis vydaný kvalifikovaným poskytovateľom dôveryhodných služieb, ktorému NBÚ udelil kvalifikovaný štatút, obsahovať **osobitný atribút**,[158] ktorým je rodné číslo podpisovateľa, za podmienky, že sa využívajú v styku s orgánmi verejnej moci. Táto podmienka je v súlade s právnou úpravu nariadenia eIDAS, ktoré povoľuje existenciu nepovinných dodatočných osobitných atribútov, ale tie nesmú mať vplyv na interoperabilitu a uznávanie kvalifikovaných elektronických podpisov.[159] Z uvedeného dôvodu sa môže kvalifikovaný elektronický podpis, kvalifikovaný certifikát pre elektronický podpis obsahujúci rodné číslo používať len v styku s orgánmi verejnej moci.

V prípade, ak podpisovateľovi nebolo pridelené rodné číslo, môže kvalifikovaný elektronický podpis, kvalifikovaný certifikát pre elektronický podpis obsahovať číslo pasu alebo číslo identifikačnej karty. Tieto údaje môžu z hľadiska automatizovaného spracovania predstavovať

[156] § 19 ods. 1 zákona o dôveryhodných službách.
[157] Tamtiež, § 1.
[158] V zmysle smernice, ktorú vydala ENISA by nemali nepovinné atribúty obmedzovať povinnú interoperabilitu. Príkladmi takýchto atribútov sú napr. organizačná jednotka, názov štátu alebo provincie, sídlo, titul. Bližšie pozri: ENISA: Guidelines for TSPs based on standards. Technical guidelines on trust services. 2017, s. 39.
[159] Čl. 28 ods. 3 nariadenia eIDAS.

problém, nakoľko každý z týchto údajov (číslo cestovného pasu alebo číslo identifikačnej karty) má iný formát.[160]

Použitie rodného čísla, resp. čísla cestovného pasu alebo čísla identifikačnej karty v prípade cudzincov v kvalifikovanom elektronickom podpise, kvalifikovanom certifikáte pre elektronický podpis, by malo vyriešiť problém pri určovaní identity osoby, ktorá vykonáva autorizáciu pre vnútroštátne účely.

Kvalifikovaná elektronická pečať, kvalifikovaný certifikát pre elektronickú pečať, ktorý bol vydaný kvalifikovaným poskytovateľom dôveryhodných služieb, ktorému NBÚ udelil kvalifikovaný štatút a sú používané v styku s orgánmi verejnej moci, môžu obsahovať identifikačné číslo pôvodcu pečate.[161] Identifikačné číslo pôvodcu pečate predstavuje v zmysle nariadenia eIDAS nepovinný dodatočný osobitný atribút, ktorý nemôže ovplyvňovať interoperabilitu a uznávanie kvalifikovaných elektronických pečatí, a preto sa môže využívať len na vnútroštátne účely.[162]

Zákon o dôveryhodných službách upravuje aj problematiku **mandátnych certifikátov**, ktoré predstavujú osobitný druh kvalifikovaných certifikátov pre elektronický podpis a slúžia len na vnútroštátne použitie. Základným účelom tohto certifikátu je určenie postavenia osoby, držiteľa mandátneho certifikátu, ktorá vykonáva autorizáciu, ak ide o osobu, ktorá je oprávnená konať v zastúpení, ale taktiež osobu, ktorá vykonáva určitú činnosť alebo zastáva konkrétnu funkciu v zmysle osobitných právnych predpisov.

V zmysle § 8 ods. 1 zákona o dôveryhodných službách predstavuje mandátny certifikát kvalifikovaný certifikát pre elektronický podpis, ktorý sa vydáva mandatárom, ktorými sú:

a) fyzická osoba oprávnená zo zákona alebo na základe zákona konať za inú osobu alebo orgán verejnej moci alebo v ich mene,

b) fyzická osoba, ktorá vykonáva činnosť podľa osobitného predpisu (napr. notár, súdny exekútor alebo advokát)[163] alebo vykonáva funkciu (napr. sudca, prokurátor) podľa osobitného predpisu.[164]

Mandátny certifikát dokazuje, že osoba vykonávajúca autorizáciu koná za alebo v mene orgánu verejnej moci alebo inej osoby, sama je orgánom verejnej moci (notár, súdny exekútor) alebo zastáva funkciu v orgáne verejnej moci (sudca, prokurátor).

---

[160] § 2 ods. 1 zákona o dôveryhodných službách.
[161] Tamtiež, § 2 ods. 2.
[162] Čl. 38 ods. 3 nariadenia eIDAS.
[163] Napríklad zákon Slovenskej národnej rady č. 323/1992 Zb. o notároch a notárskej činnosti (Notársky poriadok) v znení neskorších predpisov, zákon Národnej rady Slovenskej republiky č. 233/1995 Z. z. o súdnych exekútoroch a exekučnej činnosti (Exekučný poriadok) a o zmene a doplnení ďalších zákonov v znení neskorších predpisov, zákon č. 586/2003 Z. z. o advokácii a o zmene a doplnení zákona č. 455/1991 Zb. o živnostenskom podnikaní (živnostenský zákon) v znení neskorších predpisov v znení neskorších predpisov, zákon č. 382/2004 Z. z. o znalcoch, tlmočníkoch a prekladateľoch a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
[164] Napríklad zákon č. 385/2000 Z. z. o sudcoch a prísediacich a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 153/2001 Z. z. o prokuratúre v znení neskorších predpisov.

2.8.2.5 Zákon o kritickej infraštruktúre

Problematika ochrany kritickej infraštruktúry je upravená **zákonom č. 45/2011 Z. z. o kritickej infraštruktúre** (ďalej len „zákon o kritickej infraštruktúre"). Kritická infraštruktúra predstavuje systém, ktorý sa skladá z jednotlivých sektorov a prvkov kritickej infraštruktúry. Medzi sektory kritickej infraštruktúry možno zaradiť dopravu, elektronické komunikácie, energetiku, informačné a komunikačné technológie, poštu, priemysel, vodu a atmosféru a zdravotníctvo.[165]

Za prvok kritickej infraštruktúry sa v zmysle § 2 písm. a) zákona o kritickej infraštruktúre považuje najmä inžinierska stavba, služba vo verejnom záujme a **informačný systém** v sektore kritickej infraštruktúry, ktorých narušenie alebo zničenie by malo 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.

Právnické osoby, fyzické osoby podnikatelia alebo fyzické osoby, ktoré sú vlastníkmi prvku kritickej infraštruktúry alebo ho prevádzkujú sú považovaní za prevádzkovateľov.[166]

Ochranou prvku kritickej infraštruktúry sa rozumie zabezpečenie funkčnosti, integrity a kontinuity činnosti prvku s cieľom predísť, odvrátiť alebo zmierniť hrozbu jeho narušenia alebo zničenia.[167]

V zmysle tohto zákona majú prevádzkovatelia povinnosť ochraňovať prvok kritickej infraštruktúry pred narušením alebo zničením. Na tento účel je prevádzkovateľ okrem iného povinný zaviesť bezpečnostný plán, ktorý obsahuje popis možných spôsobov hrozby narušenia alebo zničenia prvku, zraniteľné miesta prvku a bezpečnostné opatrenia na jeho ochranu. Medzi **bezpečnostné opatrenia** možno zaradiť mechanické zábranné prostriedky, technické zabezpečovacie prostriedky, bezpečnostné prvky informačných systémov, fyzická ochrana, organizačné opatrenia, kontrolné opatrenia a ich vzájomná kombinácia.[168]

Ústredný orgán na úseku kritickej infraštruktúry v sektore vo svojej pôsobnosti vypracúva analýzu rizík sektora a jej aktualizáciu, ktorú predkladá Ministerstvu vnútra Slovenskej republiky. Analýza rizík sektora predstavuje dokument, ktorý obsahuje posúdenie hrozby narušenia alebo zničenia sektora, jeho zraniteľné miesta, ako aj predpokladané dôsledky narušenia alebo zničenia sektora.[169]

[165] Príloha č. 3 zákona o kritickej infraštruktúre.
[166] Tamtiež § 2 písm. l).
[167] Tamtiež § 2 písm. i).
[168] Tamtiež § 9 a § 10.
[169] Tamtiež § 6 a § 2 písm. j).

2.8.2.6 Zákon o elektronických komunikáciách

Významným právnym predpisom z oblasti informačnej a kybernetickej bezpečnosti je **zákon č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov** (ďalej len „zákon o elektronických komunikáciách").

Dôležitosť informačnej a kybernetickej bezpečnosti v tejto oblasti vyplýva najmä zo skutočnosti, že hlavnou úlohou elektronických komunikácií je zabezpečiť výmenu alebo prenos informácií najmä vo forme obrazu, zvuku alebo textu (ďalej len „signál") po elektronických komunikačných sieťach.[170]

Predmetný zákon okrem podmienok na poskytovanie elektronických komunikačných sietí (ďalej len „sieť") a elektronických komunikačných služieb (ďalej len „služba") upravuje aj problematiku ich ochrany a ochrany súkromia a spracúvania osobných údajov v oblasti elektronických komunikácií.

Zákon o elektronických komunikáciách definuje elektronickú komunikačnú sieť ako: *„funkčne prepojenú sústava prenosových systémov, a ak je to potrebné, prepájacích alebo smerovacích zariadení, vrátane sieťových prvkov, ktoré nie sú aktívne, ktoré umožňujú prenos signálov po vedení, rádiovými, optickými alebo inými elektromagnetickými prostriedkami, vrátane družicových sietí, pevných sietí s prepájaním okruhov a s prepájaním paketov, internetu a mobilných pozemských sietí, sietí na rozvod elektrickej energie v rozsahu, v ktorom sa používajú na prenos signálov, sietí pre rozhlasové a televízne vysielanie a káblových distribučných systémov bez ohľadu na druh prenášaných informácií."*[171] Verejnou sieťou je sieť, ktorá sa úplne alebo prevažne používa na poskytovanie verejných elektronických komunikačných služieb, ktoré podporujú prenos signálov medzi koncovými bodmi siete.[172]

Za **elektronickú komunikačnú službu** možno považovať službu obvykle poskytovaná za odplatu, ktorá spočíva úplne alebo prevažne v prenose signálov v sieťach, vrátane telekomunikačných služieb a prenosových služieb v sieťach používaných na rozhlasové a televízne vysielanie. **Verejná služba** je verejne dostupná služba, o ktorej používanie sa môže uchádzať každý záujemca.[173]

Zákon o elektronických komunikáciách obsahuje osobitné ustanovenia o **bezpečnosti a integrite verejných sietí a služieb**, kde sa podnikom, ktoré poskytujú verejné siete alebo verejné služby ukladá povinnosť, aby prijali 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

[170] § 1 ods. 3 zákona o elektronických komunikáciách.
[171] Tamtiež § 2 ods. 1.
[172] Tamtiež § 2 ods. 2.
[173] Tamtiež § 3 ods.1 a 2.

predchádzať bezpečnostným incidentom a minimalizovať vplyv bezpečnostných incidentov na užívateľov a vzájomne prepojené siete.[174]

V prípade ak dôjde k narušeniu bezpečnosti alebo integrity, ktoré by mali významný vplyv na prevádzku sietí alebo služieb, je podnik povinný o tejto skutočnosti bezodkladne informovať Úrad pre reguláciu elektronických komunikácií a poštových služieb.

V súvislosti s **ochranou súkromia a ochranou osobných údajov** platí, že podnik, ktorý poskytuje verejnú sieť alebo službu, je povinný zabezpečiť technicky a organizačne dôvernosť správ[175] a s nimi spojených prevádzkových údajov, ktoré sa prenášajú prostredníctvom jeho verejnej siete a verejných služieb. Je zakázané najmä nahrávanie, odpočúvanie, ukladanie správ alebo iné druhy zachytenia alebo sledovania správ a s nimi spojených údajov inými osobami ako sú užívatelia alebo bez súhlasu dotknutých užívateľov. Avšak, technické ukladanie údajov, ktoré sú nevyhnutné na prenos správ, bez toho aby bola dotknutá zásada dôvernosti je dovolené.[176]

Podnik je povinný informovať účastníka o tom, aké osobné údaje sa získavajú a spracúvajú, na základe akého právneho dôvodu, na aký účel a ako dlho sa budú spracúvať. Táto informácia sa poskytuje najneskôr pri uzavretí zmluvy o poskytovaní verejných služieb.[177]

ZOZNAM POUŽITEJ LITERATÚRY

1) ANDRAŠKO, J., GÁBRIŠ, T., HOCHMANN, J., OLEJÁR, D. Zákon o kybernetickej bezpečnosti. Bratislava : Wolters Kluwer, 2018,

2) ANDRAŠKO. J. a kol. Vybrané kapitoly práva informačných technológií 1. 1. vyd. Bratislava: Právnická fakulta UK, 2019, 142 s. Dostupné na: https://www.flaw.uniba.sk/fileadmin/praf/Veda/Publikacne_vystupy/2019/Monografia_DVSEI_2019.pdf.

3) HAMELINK, Cees J.: *The ethics of cyberspace*. Sage, 2001, 224 s.

4) OLEJÁR, Daniel a kol.: *Informačná bezpečnosť*. Bratislava, 2013. 246 s.

5) OLEJÁR, Daniel a kol.: *Manažment informačnej bezpečnosti a základy PKI*. Bratislava, 2015, 175 s.

6) POŽÁR, Jozef: *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005, 309 s.

7) TODOROV, Dobromir: *Mechanics of Users Identification and Authentication. Fundamentals of Identity Management*. USA: Auerbach Publications, 2007, 756 s.

[174] Tamtiež § 64 ods. 1.
[175] Správa predstavuje informáciu, ktorá sa vymieňa alebo prenáša medzi konečným počtom subjektov prostredníctvom verejnej služby.
[176] § 55 ods. 2 a 3 zákona o elektronických komunikáciách.
[177] Tamtiež § 55 ods. 4.

8) VAN DEN BERG, Jan a kol.: *On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education*. NATO STO/IST-122 symposium, Tallinn, 13-14 október 2014, 10 s.

9) VON SOLMS, Rossouw a VAN NIEKERK, Johan: *From information security to cyber security. In* Computers & Security, 2013, roč. 38, s. 97-102

10) VRABKO, Marián a kol.: *Správne právo hmotné. Všeobecná časť*. 1. vydanie. Bratislava: C. H. Beck, 2012, 480 s.

11) VOSTOUPAL, Jakub. Certifikace kyberbezpečnostních technologií. *Revue pro právo a technologie*. [Online]. 2019, č. 20, s. 147-268. Dostupné z: https://journals.muni.cz/revue/article/view/12570

12) Zborník príspevkov z konferencie SASIB Informačná bezpečnosť 2015, ktorá sa konala dňa 18. 3. 2015 v Kongresovom centre Technopol v Bratislave

13) WHITMAN, Michael E. a MATTORD, Herbert J.: *Principles of Information security*. Boston: Course Technology, 2012, 617 s. ISBN-13: 978-1-111-13821-9

14) Nariadenie EP a Rady 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

15) Nariadenie Európskeho parlamentu a Rady (EÚ) 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

16) Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii

17) Smernica Európskeho parlamentu a Rady (EÚ) 2015/2366 z 25. novembra 2015 o platobných službách na vnútornom trhu, ktorou sa menia smernice 2002/65/ES, 2009/110/ES a 2013/36/EÚ a nariadenie (EÚ) č. 1093/2010 a ktorou sa zrušuje smernica 2007/64/ES

18) Nariadenie európskeho parlamentu a rady o Agentúre EÚ pre kybernetickú bezpečnosť (ENISA), o zrušení nariadenia (EÚ) č. 526/2013 a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií

19) Nariadenie Európskeho parlamentu a Rady (EÚ) 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

20) Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV

21) Zákon č. 18/2018 Z. z. o ochrane osobných údajov v znení neskorších predpisov.

22) KOMISIA: Stratégia kybernetickej bezpečnosti Európskej únie. Brusel: 2013

23) Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
24) 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),
25) Výnos č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy
26) Zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov
27) Zákon č. 45/2011 Z. z. o kritickej infraštruktúre
28) Zákon č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov
29) MINISTERSTVO FINANCIÍ SLOVENSKEJ REPUBLIKY: Národná koncepcia informatizácie verejnej správy. Bratislava, 2008
30) MINISTERSTVO FINANCIÍ SLOVENSKEJ REPUBLIKY: Národná stratégia pre informačnú bezpečnosť SR, Bratislava, 2008
31) ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY: Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020. Bratislava, 2015
32) ÚRAD PODPREDSEDU VLÁDY SLOVENSKEJ REPUBLIKY PRE INVESTÍCIE A INFORMATIZÁCIU: Používateľská príručka centrálneho metainformačného systému verejnej správy. Bratislava, 2017
33) ENISA: Guidelines for TSPs based on standards. Technical guidelines on trust services. 2017, 95 s.
34) ISO/IEC 27000:2018 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
35) ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity
36) ISO/IEC Guide 2:2004 Standardization and related activities – General vocabulary
37) Article 29 Working Party Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01.
38) www.csirt.gov.sk
39) www.iso.org
40) www.informatizacia.sk
41) www.uniba.sk/infosec
42) https://dataprotection.gov.sk/uoou/sk/dp/dp-breach
43) https://www.enforcementtracker.com/
44) https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/

45) https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/

46) https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9256486
https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2019/30_BfDIverh%C3%A4ngtGeldbu%C3%9Fe1u1.html

47) https://www.cpdp.bg/index.php?p=news_view&aid=1519

48) https://www.etrend.sk/ekonomika/socialna-poistovna-porusila-gdpr-pokutu-50-tisic-eur-nechce-zaplatit.html

49) https://www.etrend.sk/ekonomika/gdpr-zacina-hryzt-telekomunikacny-operator-dostal-pokutu-40-tisic-eur.html

KAPITOLA 3 PRÁVNA ÚPRAVA ZODPOVEDNOSTI VO VEREJNOM PRÁVE S AKCENTOM NA POČÍTAČOVÚ KRIMINALITU A KYBERNETICKÚ BEZPEČNOSŤ

3.1 Úvodné poznámky o (právnej) zodpovednosti

Zodpovednosť predstavuje jeden z najstarších konceptov spoločenského života, ktorému sa venuje všeobecná pozornosť. V rámci spoločenských vied sa zodpovednosti v právnej vede venuje zvýšený záujem. Nie nadarmo, keďže v tradičnom ponímaní je štruktúra právnych noriem[178] tvorená tromi zložkami,[179] kde jednou z nich je **sankcia**, ako právny dôsledok protiprávneho konania a následného vyvodenia zodpovednosti. Sankcia sa tu chápe ako ujma spôsobená v dôsledku toho, že osoba konala inak ako právna norma prikazovala, prípadne umožňovala.

Zodpovednosť v práve súvisí aj s ďalšou skutočnosťou, a to **štátnym donútením**. Štátne donútenie predstavuje jeden zo špecifických znakov práva, ktoré ho odlišuje od iných normatívnych systémov.[180] Ak má štát účinne regulovať spoločenské vzťahy, zabezpečiť v spoločnosti právnu istotu a poriadok, musí zabezpečiť plnenie právnych povinností aj v prípade, ak ich povinnostný subjekt[181] dobrovoľne neplní, ak sa odmieta podrobiť právu. Vzniká tu potreba vynútiť plnenie aj proti vôli povinného subjektu, teda uplatniť štátne donútenie prostredníctvom súdov, polície alebo iných inštitúcií štátu.[182]

O tom, že právo venuje zodpovednosti skutočne široký priestor, svedčí napríklad aj to, že **tomuto právnemu inštitútu sa venujú právne odvetvia naprieč celým právnym poriadkom** Slovenskej republiky. Právnu zodpovednosť vymedzuje preto nielen právna teória, ale aj jednotlivé právne odvetvia, a to bez ohľadu na to, či ide o právne odvetvie súkromného práva (napríklad občianske právo, obchodné právo, pracovné právo) alebo verejného práva (napríklad ústavné právo, trestné právo, správne právo).[183]

Koncepcia právnej zodpovednosti pritom nie je jedinou formou zodpovednosti, ktorá sa uplatňuje v našej spoločnosti. Možno rozoznať **viacero vrstiev foriem zodpovednosti**, a teda nielen tej právnej. S výnimkou právnej zodpovednosti sa v dielach právnej teórie spomína najmä

---

[178] Právna norma vo všeobecnosti predstavuje všeobecne záväzné pravidlo ľudského správania, ktoré je ustanovené alebo uznané štátom (alebo medzinárodným spoločenstvom štátov) a ktorého porušenie štát sankcionuje (resp. štátmi vytvorené medzinárodné inštitúcie); GERLOCH, A. In VEČEŘA, M. a kol. Teória práva. Bratislava : Eurokódex, 2009, s. 36. Jej najčastejšie uvádzanými znakmi sú: normatívnosť, záväznosť, všeobecnosť a štátne donútenie; FÁBRY, B., KASINEC, R., TURČAN, M. *Teória práva*. Bratislava : Wolters Kluwer, 2019, s. 79.

[179] Ide o hypotézu, dispozíciu a sankciu. Hypotéza predstavuje právnu skutočnosť, ktorá keď nastane, jedinec sa musí správať určitým spôsobom (dispozícia) a ak sa tak nespráva, hrozí mu za to normou ustanovený následok (sankcia); pozri bližšie napríklad KNAPP, V. *Teorie práva*. Praha : C. H. Beck, 1995, s. 153 a nasl. alebo PRUSÁK, J. *Teória práva*. Bratislava : VO PraF UK, 1995, s. 223-224. Inými slovami vymedzuje sa konkrétne povolené pravidlo správania sa, ktoré treba realizovať vtedy, keď nastane určitá situácia, pričom ak sa tak osoba nebude správať, bude za to môcť byť konkrétnym spôsobom sankcionovaná.

[180] T. j. systémov, ktoré určujú pravidlá správania; ide napríklad o morálne (etické) pravidlá alebo pravidlá určitej náboženskej skupiny a pod.

[181] T. j. ten, komu splnenie povinnosti prislúcha

[182] OTTOVÁ, E. *Teória práva*. Bratislava : VO PraF UK, 2004, s. 17-18.

[183] K pojmom verejné právo a súkromné právo pozri ďalej v texte.

zodpovednosť politická a morálna,[184] prípadne sa zdôrazňuje, že má rozmer etický, filozofický, sociologický a aj ekonomický.[185] Vidieť, že zodpovednosť ako fenomén sa prejavuje nielen v právnej sfére, ale aj v mimoprávnej sfére. Z hľadiska právnej teórie bude, samozrejme, mať význam analyzovanie koncepcie zodpovednosti z právneho hľadiska. Treba dodať, že ani pritom by sme nemali zabúdať na širšie súvislosti zodpovednosti, a to predovšetkým z hľadiska morálky a etiky.

Právo určuje a upravuje spoločensky žiaduce správanie prostredníctvom právnych noriem. Tie všeobecne určujú práva a povinnosti jednotlivým osobám prostredníctvom príkazov, zákazov, či povolení. Vo vzťahu k právnej zodpovednosti do popredia vystupujú najmä právom uložené povinnosti. Povinnosti jednoznačným spôsobom obmedzujú slobodu jednotlivca, avšak toto obmedzenie je ospravedlnené vyšším cieľom, ktorým je snaha o ochranu spoločnosti ako takej, a v konečnom dôsledku aj samotného jedinca. V právnej teórii sa možno stretnúť aj s názorom, podľa ktorého každá norma obsahuje povinnosť, pričom nie je rozhodujúce, či povinnosť je jednoznačne stanovená, alebo nie, ale v rámci korelačného vzťahu s oprávnením je žiaduce, aby bola určená výkladom (napríklad v normách oprávňujúcich).[186]

Z hľadiska chápania štátu, v rámci ktorého sa bezvýhradne uplatňuje **princíp vlády práva**,[187] ako jedného z najvýznamnejších princípov, ktorý subsumujeme pod koncepciu (materiálneho) právneho štátu, je nesmierne dôležité, aby právne povinnosti boli ustanovované jednoznačne. Táto skutočnosť vyplýva predovšetkým z Ústavy Slovenskej republiky. Základný kameň nášho právneho poriadku v čl. 13 ods. 1 ustanovuje, že povinnosti možno ukladať len zákonom alebo na základe zákona, v jeho medziach a pri zachovaní základných práv a slobôd.

Ústavodarca vychádza z premisy, podľa ktorej **jednotlivec môže byť zaťažený povinnosťami**, avšak musia byť na to splnené tak materiálne, ako aj formálne podmienky. Formálnou podmienkou je, že povinnosť musí byť určená v uznanom prameni práva[188] a materiálnou podmienkou je, že povinnosťou nemožno poprieť základné právo alebo slobodu.[189]

Z určitého hľadiska práve **právne povinnosti sú základným predpokladom existencie inštitútu právnej zodpovednosti**. Je to tak preto, lebo vynútenie oprávnení je na vlastnom zvážení toho subjektu, ktorý je nositeľom toho-ktorého oprávnenia. Uvedené s niekoľkými výnimkami platí aj pre vynútenie povinností. To, či sa uplatní ich vynútenie, je taktiež často na zvážení subjektu, vo

[184] Porovnaj OTTOVÁ, E. *Teória práva.* Šamorín : Heuréka, 2010, s. 283; GERLOCH, A. *Teorie práva.* Plzeň : Aleš Čeněk, 2013, s. 161.
[185] Porovnaj ČAPEK, J. In BOGUSZAK, J., ČAPEK, J., GERLOCH, A. *Teorie práva*. Praha : Eurolex Bohemia, 2001, s. 160.
[186] Pozri bližšie KANÁRIK, I. *In BRÖSTL, A. a kol. Teória práva. Plzeň : Aleš Čeněk, 2013,* s. 145.
[187] *Rule of law* (angl.), *Rechtstaat* (nem.), *règle de loi* (fr.), *imperio de la ley* (šp.), *lagstyre* (šve.).
[188] Okrem spomínaných zákonov a na základe zákona sú to ďalej povinnosti uložené medzinárodnou zmluvou podľa čl. 7 ods. 4 Ústavy Slovenskej republiky, ktorá priamo zakladá práva a povinnosti fyzických osôb a právnických osôb, alebo nariadením vlády Slovenskej republiky podľa čl. 120 ods. 2 Ústavy Slovenskej republiky (tzv. aproximačné nariadenie vlády Slovenskej republiky).
[189] Pozri bližšie DRGONEC, J. *Ústava Slovenskej republiky. Komentár*. Šamorín : Heuréka, 2007, s. 157-159.

vzťahu ku ktorému došlo k ich porušeniu. Rozdiel tu spočíva v tom, že právny štát musí mať vytvorený procedurálny systém vynútenia povinností, zatiaľ čo takýto systém pri vynucovaní povinností nemá svoje opodstatnenie.

Ak by v právnom štáte neexistoval systém donútenia[190] splnenia povinností, neplnil by štát jednu zo svojich hlavných úloh v podobe zabezpečenia rozvoja spoločnosti a potrieb svojich občanov (obyvateľov). Na druhej strane treba zdôrazniť, že tieto pravidlá musia byť určené s jednoznačnou presnosťou, pretože pri ich uplatnení sa postupuje prísne v súlade s čl. 2 ods. 2 Ústavy Slovenskej republiky.[191] Predmetný článok vyjadruje viazanosť orgánov štátu (a rozširujúco aj neštátnych orgánov) právom (právnym poriadkom).

Uvedené myšlienky zároveň aj dokumentujú **rozlíšenie zodpovednosti z právneho hľadiska a z ostatných hľadísk**. Porušenie povinnosti z právneho hľadiska so sebou totiž nesie právne dôsledky v podobe povinnosti zniesť určitý následok. Porušenie morálnej povinnosti a uplatnenie morálnej zodpovednosti so sebou nesie „len" morálne odsúdenie. Hoci totiž právo a morálka v mnohom splývajú, alebo by mali splývať, nemusí to vždy tak byť. Vynútenie morálnych povinností, ktoré nie sú upravené právnym poriadkom, sa zásadne dostáva do pozície spoločenského odsúdenia, t. j. odsúdenia, ktoré smeruje do vlastného svedomia porušiteľa a ktoré ho diskvalifikuje zo spoločenského hľadiska. Táto osoba sa môže, ale aj nemusí, opäť v budúcnosti správať rovnako; záleží od jej presvedčenia.

Porušenie právnej povinnosti často so sebou nesie nielen morálne (spoločenské) odsúdenie, ale zároveň v sebe nesie aj prvky, ktoré by mali zabrániť opätovnému porušeniu právnej povinnosti. Právny dôsledok môže dokonca dospieť aj do stavu, keď porušiteľovi sa siaha na jeho základné práva a slobody a tieto sa mu obmedzujú. **Cieľom je donútiť** porušiteľa, aby už právnu povinnosť v budúcnosti neporušoval (odstrašenie).

Zásah verejnej moci do slobôd jednotlivca, ktorý porušil právnu povinnosť, je vynútený princípom vlády práva. Osoba, ktorá porušila právnu povinnosť, konala protiprávne. Treba zdôrazniť, že protiprávne konanie môže mať podobu tak aktívneho konania, ale aj pasívneho, t. j. opomenutia konania (nečinnosť). **Právny štát si nemôže dovoliť, aby povinnosti** uložené v súlade s jeho vlastným právnym poriadkom, **neboli dodržiavané** a v širšom uhle pohľadu zároveň aj vynútiteľné. Ako sumarizuje právna teória, tak jedným z klasických špecifických znakov práva oproti neprávnym normám, je existencia štátneho donútenia.[192]

Na základe tohto rozboru možno usúdiť, že vo vzťahu k právnej zodpovednosti sú kľúčovými nasledovné pojmy:

---

[190] A to aj proti vôli osoby, ktorá splnenie povinnosti porušila.
[191] T. j. štátne orgány môžu konať len na základe ústavy, v jej medziach a v rozsahu a spôsobom, ktorý ustanoví zákon.
[192] Pozri PRUSÁK, J. *Teória práva.* Bratislava : VO PraF UK, 2001, s. 22.

a) **existencia povinnosti** určenej v súlade s právnym poriadkom,

b) **porušenie ustanovenej povinnosti** (t. j. protiprávne konanie, či už aktívne alebo pasívne),

c) **subjekt, ktorý žiada vynútenie** porušenej povinnosti,

d) právnym poriadkom ustanovené **pravidlá vynútenia** povinnosti,

e) **právne následky** nesplnenia povinnosti, najmä sankcie.

Vo vzťahu k **sankciám** treba dodať, že môžu **mať rôznu podobu**. Nemám na mysli len sankcie typické z hľadiska verejného práva ako napríklad trest odňatia slobody, finančnú pokutu, zákaz činnosti a podobne, ale aj sankcie klasicky súkromnoprávneho charakteru, t. j. napríklad vrátenie neoprávnene získaného majetkového prospechu, odstránenie vád veci, poskytnutie primeranej zľavy, atď.

V. Knapp práve **sankciu považuje za základný všeobecný znak zodpovednosti**. Nazýva ňou povinnosť zniesť ujmu, poprípade aj ujmu ako takú, ako dôsledok, že nastane zákonom ustanovená skutočnosť. Ako ďalej uvádza, tak rozsah pojmu sankcia nepovažuje za úplne jasne daný. Je ňou nepochybne trest, nepochybne ňou je povinnosť nahradiť spôsobenú škodu, môže ňou byť odvolanie z funkcie a niektorí autori za ňu považujú aj neplatnosť zmluvy odporujúcej zákonu, atď.[193] Vo vzťahu k právnej zodpovednosti sa treba vyjadriť aj k **problematike jej vzniku**. Právna teória vychádza z dvoch možných konceptov. Prvý koncept sa označuje pojmami aktívna právna zodpovednosť,[194] perspektívna právna zodpovednosť,[195] prípadne zodpovednosť za porušenie povinnosti.[196] Jeho podstata spočíva v tom, že právna zodpovednosť tu vystupuje priamo ako hrozba sankciou, čiže vzniká spolu so vznikom primárnej právnej povinnosti. Druhá koncepcia sa označuje pojmami pasívna právna zodpovednosť, retrospektívna právna zodpovednosť, prípadne zodpovednosť za porušenie povinnosti.[197] V tomto prípade ide o chápanie právnej zodpovednosti ako sekundárneho vzťahu. Právna zodpovednosť sa tu aktivizuje až v dôsledku nesplnenia primárnej povinnosti. Podstata spočíva v tom, že právna zodpovednosť sa nemôže vyvodiť v prípade, ak nedošlo k porušeniu primárnej právnej povinnosti.

Týmto koncepciám právnej zodpovednosti sa venovali mnohí velikáni právnej vedy. Osobitne treba spomenúť názor akademika Š. Lubyho, podľa ktorého **o vzniku zodpovednosti možno hovoriť až vtedy, keď došlo k porušeniu právnej povinnosti**. Vznik zodpovednostného vzťahu teda možno vidieť až v dôsledku protiprávneho konania a nikdy nie pred porušením právnej povinnosti.[198] Uvedený koncept prispieva k presnému a jednoznačnému vymedzeniu obsahu

[193] KNAPP, V. *Teorie práva*. Praha : C. H. Beck, 1995, s. 200.
[194] Pozri napríklad HOUBOVÁ, D. *In HARVÁNEK, J. a kol. Teorie práva*. Plzeň : Aleš Čeněk, 2008, s. 383.
[195] Pozri napríklad ZOUBEK, V. *Právověda a státověda. Úvod do právního a státovědního myšlení*. Plzeň : Aleš Čeněk, 2010, s. 193.
[196] Pozri napríklad KANÁRIK, I. *In BRÖSTL, A. a kol. Teória práva*. Plzeň : Aleš Čeněk, 2013, s. 148.
[197] Pozri bližšie napríklad diela uvedené v poznámkach pod čiarou č. 9 až 11.
[198] LUBY, Š. Výber z diel a myšlienok. Bratislava : Iura Edition, 1998, s. 72.

právnych pojmov a k dôslednému rozlišovaniu právnych javov a vzťahov od iných, neprávnych sociálnych javov a vzťahov.[199] Tento koncept je zároveň konceptom, z ktorého vychádza táto kapitola.

Na základe toho, čo bolo spomenuté, možno pristúpiť k definovaniu právnej zodpovednosti a jej funkciám. Vo všeobecnosti sa zodpovednosťou rozumie **nevyhnutnosť niesť následky svojho správania, ktoré je v rozpore so stanoveným vzorom správania**.[200] V literatúre sa možno stretnúť s viacerými možnými spôsobmi definovania právnej zodpovednosti. Podľa E. Ottovej sa právnou zodpovednosťou rozumie povinnosť strpieť právom ustanovené nepriaznivé následky protiprávneho konania.[201] A. Gerloch uvádza, že právna zodpovednosť je osobitná forma právneho vzťahu, v ktorom dochádza na základe porušenia právnej povinnosti k vzniku novej právnej povinnosti sankčnej povahy.[202] J. Čapek vychádza z myšlienky, že právnou zodpovednosťou sa rozumie povinnosť strpieť následky za porušenie povinností ustanovené právnymi normami v rámci zodpovednostného právneho pomeru.[203]

Zosumarizovaním týchto poznatkov a vlastných myšlienok, možno dospieť k záveru, že právna zodpovednosť predstavuje **povinnosť subjektu niesť nepriaznivé právne následky vyvolané porušením (ohrozením) právnej povinnosti, ktorá bola uložená v súlade s právnym poriadkom alebo na jeho základe, či už aktívnym alebo pasívnym protiprávnym konaním**.
Existenciu právnej zodpovednosti možno odôvodniť viacerými základnými funkciami, ktoré napĺňa. Zaraďujú sa medzi ne najmä tieto **funkcie: preventívna, reparačná, satisfakčná, represívna.**[204]

Cieľom existencie **preventívnej funkcie** právnej zodpovednosti je najmä pôsobiť *ex ante (pro futuro)*. Podstata spočíva v takom pôsobení, aby k vzniku porušenia právnych povinností, a teda možnosti uplatnenia a vyvodenia právnej zodpovednosti, ani nedošlo. Takúto všeobecnú preventívnu funkciu napĺňa napríklad § 415 Občianskeho zákonníka, podľa ktorého je každý povinný počínať si tak, aby nedochádzalo ku škodám na zdraví, na majetku, na prírode a na životnom prostredí. Preventívnu funkciu môže napĺňať aj trest odňatia slobody, ktorý má zabrániť ďalšiemu páchaniu trestnej činnosti páchateľa. Z uvedeného hľadiska možno zároveň usúdiť, že preventívna funkcia napĺňa znaky najvšeobecnejšej funkcie právnej zodpovednosti a v istom slova zmysle je súčasťou aj ostatných funkcií.

Reparačná (kompenzačná) funkcia sa spomína predovšetkým v súvislosti s vyvodením zodpovednosti pri porušeniach majetkového charakteru. Jej cieľom je predovšetkým odčiniť škodlivý následok, ktorý vznikol v dôsledku porušenia právnej povinnosti. Spolu s funkciou

[199] HOUBOVÁ, D. In HARVÁNEK, J. a kol. *Teorie práva*. Plzeň : Aleš Čeněk, 2008, s. 384.
[200] KANÁRIK, I. *In BRÖSTL, A. a kol. Teória práva*. Plzeň : Aleš Čeněk, 2013, s. 146.
[201] OTTOVÁ, E. *Teória práva*. Šamorín : Heuréka, 2010, s. 283.
[202] GERLOCH, A. In VEČEŘA, M. a kol. *Teória práva*. Žilina : EUROKÓDEX, 2013, s. 249.
[203] ČAPEK, J. In BOGUSZAK, J., ČAPEK, J., GERLOCH, A. *Teorie práva*. Praha : ASPI, 2003, s. 166.
[204] Pozri napríklad KNAPP, V. *Teorie práva*. Praha : C. H. Beck, 1995, s. 201.

satisfakčnou a represívnou predstavujú funkcie zodpovednosti, ktoré sa uplatňujú až v prípade, keď už reálne došlo k porušeniu právnej povinnosti, t. j. *ex post*. Reparačná funkcia sa prejavuje v podobe *restitutio in integrum*, t. j. v obnovení do pôvodného stavu. Možno sa stretnúť aj s pojmom naturálna reštitúcia. Ak nemožno dosiahnuť navrátenie do pôvodného stavu, potom sa prejavuje v podobe reparácie, čiže odškodnenia, ktorého podstata spočíva v náhrade spôsobenej ujmy. Treba si povšimnúť, že prednosť má vždy snaha o navrátenie do pôvodného stavu, kde pod pôvodným stavom sa má na mysli stav, ktorý by tu bol, ak by nedošlo k porušeniu povinnosti.

Satisfakčná funkcia predstavuje funkciu, na základe ktorej dochádza v dôsledku vyvodenia zodpovednosti k poskytnutiu zadosťučinenia. Uplatňuje sa najmä pri neoprávnenom zásahu do práva na ochranu osobnosti,[205] kde fyzická osoba má podľa § 11 Občianskeho zákonníka právo na ochranu svojej osobnosti, najmä života a zdravia, občianskej cti a ľudskej dôstojnosti, ako aj súkromia, svojho mena a prejavov osobnej povahy. Vo vzťahu k právnickým osobám (podnikateľom zapísaných v Obchodnom registri Slovenskej republiky) treba pre úplnosť upozorniť na § 12 Obchodného zákonníka, ktorý upravuje ochranu obchodného mena a na § 44 a nasl. Obchodného zákonníka, ktoré upravujú nekalú súťaž. V danom prípade môže dôjsť k naplneniu tejto funkcie napríklad zverejnením ospravedlnenia v médiách.

Represívna funkcia je zrejme funkciou, ktorá je najpríznačnejšia pre právnu zodpovednosť. Jej podstata totiž spočíva v tom, že osobe, ktorá porušila právnu povinnosť vznikne z tohto dôvodu konkrétna ujma. V jej dôsledku dochádza k postihnutiu (sankcionovaniu, potrestaniu) toho, kto porušil právnu povinnosť. Represívna funkcia sa uplatňuje predovšetkým v právnych odvetviach, ktoré v našich právnych podmienkach tradične zaraďujeme pod odvetvia verejného práva. Konkrétne sankcie potom vyplývajú z príslušných noriem, ktoré upravujú to-ktoré právne odvetvie. Niektorí autori uvádzajú **aj ďalšie funkcie** právnej zodpovednosti, ako napríklad signalizačnú funkciu, ktorej podstata spočíva v tom, že z počtu porušení právnych predpisov v konkrétnej oblasti v rôznych časových horizontoch možno získavať štatistické a iné údaje.[206]

3.2 Súkromnoprávna zodpovednosť a verejnoprávna zodpovednosť

Právnu zodpovednosť právna teória tradične **člení na súkromnoprávnu a verejnoprávnu**.[207] Uvedené členenie vyplýva z tradičného členenia právneho poriadku Slovenskej republiky, ktoré vychádza z recepcie rímskeho práva (tzv. kontinentálny právny systém), na právo verejné a právo súkromné. Pod súkromnoprávnu zodpovednosť budeme preto radiť

[205] HOUBOVÁ, D. In HARVÁNEK, J. a kol. *Teorie práva*. Plzeň : Aleš Čeněk, 2008, s. 385.
[206] Pozri napríklad GERLOCH, A. *Teorie práva*. Plzeň : Aleš Čeněk, 2013, s. 164.
[207] Pozri napr. OTTOVÁ, E. Teória práva. Šamorín : Heuréka, 2010, s. 285; ČAPEK, J. *In VEVERKA, V., BOGUSZAK, J., ČAPEK, J. Základy teorie práva a právní filozofie*. Praha : Nakladatelství CODEX, 1996, s. 146; GERLOCH, A. *In VEČEŘA, M. a kol. Teória práva*. Žilina : EUROKÓDEX, 2013, s. 251-252; HOUBOVÁ, D. In HARVÁNEK, J. a kol. *Teorie práva*. Plzeň : Aleš Čeněk, 2008, s. 386.

zodpovednostné vzťahy, ktoré vznikajú v rámci odvetví súkromného práva ako napríklad občianskeho práva, obchodného práva alebo pracovného práva. Verejnoprávna zodpovednosť je tá, ktorá vzniká v rámci vzťahov v odvetviach verejného práva ako napríklad ústavného práva, trestného práva alebo správneho práva.

Tam, kde bude z právneho vzťahu, ktorý bol porušený, vyplývať **nadradenosť a podradenosť medzi jeho subjektmi, tam možno hovoriť o verejnoprávnej zodpovednosti**. Zodpovednostný vzťah tu vznikol medzi osobou, ktorá porušila svoje právne povinnosti a reprezentantom verejnej moci (štátom, samosprávou). Tam, kde bude medzi subjektmi **prevládať vzájomná rovnosť, budeme hovoriť o súkromnoprávnej zodpovednosti**. Zodpovednostný vzťah tu vzniká medzi osobami pôvodného právneho vzťahu, pričom v odvodenom zodpovednostnom vzťahu ide o vzťah medzi delikventom (porušiteľom) a poškodeným.

Jedným zo základných členení právnej zodpovednosti je preto jej členenie podľa toho, či je upravená verejnoprávnou alebo súkromnoprávnou metódou regulácie, a to na zodpovednosť verejnoprávnu a súkromnoprávnu. Zaužívalo sa aj označovanie, podľa ktorého nesplnenie súkromnoprávnej povinnosti možno označiť pojmom **súkromnoprávny delikt** a nesplnenie verejnoprávnych povinností je známe aj pod označením **verejnoprávny delikt**.[208]

Rozdiel medzi súkromnoprávnym a verejnoprávnym poňatím zodpovednosti spočíva v

a) **prameňoch** právnej úpravy, v ktorých sa nachádzajú,

b) **spôsobe ochrany**, ktorý je poskytnutý objektu verejnoprávneho a súkromnoprávneho deliktu,

c) tom, **kto vynucuje** porušené povinnosti a

d) v **povahe realizácie donútenia**.

V ďalšom texte sa zamieram najprv na súkromnoprávnu koncepciu právnej zodpovednosti, teda na tzv. súkromné (súkromnoprávne) delikty a potom na verejnoprávnu zodpovednosť.

3.2.1 Súkromnoprávna zodpovednosť

Súkromnoprávna koncepcia právnej zodpovednosti vypovedá o zodpovednostnom **vzťahu, ktorý vznikol medzi delikventom (porušiteľom) a poškodeným**. Ak vychádzame z už načrtnutej Lubyho koncepcie vzniku zodpovednosti, potom ide o sekundárny právny vzťah, ktorého existencia je odvodená od primárneho právneho vzťahu. Pôvodný právny vzťah vznikol medzi dvomi alebo viacerými osobami, pričom jeho obsahom boli synalagmatické (vzájomné) práva a povinnosti. Jeden zo subjektov si svoju povinnosť nesplnil, v dôsledku čoho možno hovoriť o vzniku sekundárneho, a to už zodpovednostného vzťahu. Subjekt, ktorý nesplnil povinnosť, možno označiť

[208] Všeobecne porušenie (a najmä zavinené) právnej povinnosti možno označiť pojmom delikt (právny delikt).

pojmom delikvent alebo porušiteľ. Subjekt, vo vzťahu ku ktorému malo dôjsť k splneniu povinnosti, je poškodeným, teda tým, komu vznikla ujma.[209]

Zásadným rozdielom oproti verejnoprávnej koncepcii zodpovednosti je najmä skutočnosť, že **oprávnenie zo zodpovednostného vzťahu vzniká priamo tomu subjektu, ktorému bolo protiprávnym konaním porušené právo**.[210] Treba dodať, že ide o súkromnoprávnu koncepciu právnej zodpovednosti aj napriek tomu, že vymáhanie splnenia povinnosti sa uskutočňuje prostredníctvom tretieho subjektu, ktorým je tradične sudca ako reprezentant verejnej moci. Môže ním však byť aj rozhodca, arbiter, atď.

Veľmi významným odlíšením súkromnoprávnej koncepcie zodpovednosti je ďalej aj uplatnenie funkcií, ktoré sú pre ňu typické. **Do popredia** sa dostáva predovšetkým **funkcia preventívna** a **reparačná**, **prípadne satisfakčná**. Využitie týchto funkcií vyplýva predovšetkým z faktu, že súkromnoprávna zodpovednosť je tradične zodpovednosťou majetkového charakteru. Využitie reparačnej funkcie znamená, že ako náprava vzniknutého protiprávneho stavu sa bude využívať primárne *restitutio in integrum*, čiže navrátenie do pôvodného stavu. Ak nebude možné toto navrátenie, možno uvažovať aj o poskytnutí primeraného zadosťučinenia (satisfakčná funkcia).

Dôsledkom uvedeného pre delikventa je, že je povinný strpieť uloženú sekundárnu **povinnosť, ktorá vedie práve k navráteniu do pôvodného stavu**, **prípadne** k úkonu, ktorým sa poskytne **primerané zadosťučinenie**.

Súkromnoprávnu zodpovednosť upravujú viaceré zákony, **neexistuje jednotná koncepcia jej vyvodzovania**. Najzákladnejšie pravidlá jej vyvodzovania možno nájsť v zákonoch kódexového charakteru. Z nich má najväčší význam koncepcia vyvodzovania zodpovednosti v Občianskom zákonníku,[211] Obchodnom zákonníku[212] a v Zákonníku práce.[213]

Nie je pritom vylúčené, aby súkromnoprávnym deliktom došlo zároveň k naplneniu verejnoprávneho deliktu, či už v podobe trestného činu, priestupku alebo iného správneho deliktu.

3.2.2 Verejnoprávna zodpovednosť

Na tomto mieste považujem za vhodné zdôrazniť a bližšie rozviesť tie rozdiely, ktoré sú typické pre verejnoprávnu koncepciu zodpovednosti.

Verejnoprávna zodpovednosť v prvom rade plní **čiastočne odlišné funkcie** oproti súkromnoprávnej zodpovednosti. V právnej teórii sa k funkciám verejnoprávnej zodpovednosti

[209] V literatúre sa možno stretnúť s označením tohto vzťahu ako paritného (*inter partes*). KANÁRIK, I. In BRÖSTL, A. a kol. Teória práva. Plzeň : Aleš Čeněk, 2013, s. 150.
[210] Pozri ČAPEK, J. In BOGUSZAK, J., ČAPEK, J., GERLOCH, A. *Teorie práva*. Praha : Eurolex Bohemia, 2001, s. 170.
[211] Pozri § 415 až 450 Občianskeho zákonníka.
[212] Pozri § 373 až 386 Obchodného zákonníka, § 757 Obchodného zákonníka.
[213] Pozri § 186 až 219 Zákonníka práce.

radia najmä: funkcia ochranná, regulatívna, preventívna a represívna.[214] Som toho názoru, že **zdôrazniť treba najmä funkciu represívnu**, pretože tá sa v súkromnom práve zásadne nevyužíva v takom rozsahu.

Podstatou represívnej funkcie je najmä skutočnosť, že **pôsobí ako individuálna prevencia voči konkrétnemu delikventovi, ale aj ako generálna prevencia voči spoločnosti**, teda pôsobí na verejnú mienku. Aj keď by sa represívna funkcia mala využiť až ako *ultima ratio*, t. j. posledná možnosť, keď ostatné možnosti nápravy nie sú možné, z hľadiska klasickej teórie práva[215] je predsa len represívna funkcia a jej využitie tým najvýraznejším odlíšením verejnoprávnej zodpovednosti od zodpovednosti súkromnoprávnej.

Dôležité je aj to, medzi kým vznikne zodpovednostný vzťah. V prípadoch verejnoprávnej zodpovednosti **pôjde o vzťah, ktorý vznikne medzi delikventom, čiže osobou, ktorá sa správala protiprávne, a orgánom verejnej moci**. Rozlišuje sa pritom chápanie tohto vzťahu z hľadiska hmotného práva a z procesného práva.[216] V prípade hmotnoprávneho vzťahu ide o vzťah medzi orgánom verejnej moci a delikventom; vzťah vznikne okamihom porušenia verejnoprávnej povinnosti. Odlišným je potom vzťah procesnoprávny, ktorý vzniká medzi orgánom verejnej moci na strane jednej a osobou, ktorá je obvinená z porušenia procesnoprávnej povinnosti. Tento vzťah vznikne až na základe úkonu orgánu verejnej moci, ktorým sa osoba oboznámi s podstatou obvinenia (túto osobu možno nazvať obvinený). Rozdiel tu spočíva v tom, že osoba obvinená z porušenia právnej povinnosti ešte nemusí byť aj skutočne osobou, ktorá túto povinnosť porušila.

Až procesným postupom orgánu verejnej moci zavŕšeným právoplatným rozhodnutím vo veci, sa určí, či ide o osobu páchateľa alebo nie.

Porušenie právnej povinnosti v prípadoch verejnoprávnej zodpovednosti môže, ale aj nemusí mať majetkový rozmer. V oblasti **verejného práva sa stretávame s ochranou aj iných než majetkových hodnôt, a to najmä života, zdravia, životného prostredia, riadneho chodu vecí verejných a pod.** Práve z tohto dôvodu tu vystupuje do popredia postavenie orgánu verejnej moci, ktorým je buď súd, alebo správny orgán, ktorý musí preskúmať, či skutočne došlo k porušeniu právnych povinností v tom-ktorom odvetví verejného práva a vyvodiť z toho príslušné konzekvencie.

Ak vznikla škoda majetkového charakteru a poškodeným je fyzická osoba alebo právnická osoba, samozrejme, má právo domáhať sa náhrady vzniknutej škody. Ako však vyplýva zo

[214] Pozri napríklad MENCEROVÁ, I. In MENCEROVÁ, I., TOBIÁŠOVÁ, L., TURAYOVÁ, Y. a kol. *Trestné právo hmotné. Všeobecná časť*. Šamorín : Heuréka, 2013, s. 16.
[215] Napríklad GERLOCH, A. *Teorie práva*. Plzeň : Aleš Čeněk, 2013, s. 182.
[216] Analogicky v prípade trestného práva pozri bližšie napríklad STRÉMY, T. In MAŠĽANYOVÁ, D. a kol. *Trestné právo hmotné*. Plzeň : Aleš Čeněk, 2011, s. 17.

základných funkcií vyvodzovania verejnoprávnej zodpovednosti, tak **rozhodovanie o určení výšky škody a povinnosti jej uhradenia nie je jej prvoradým cieľom**.

Hoci by sa tak mohlo zdať, že určovanie výšky škody a jej náhrady v konaniach verejnoprávneho charakteru je preto na „vedľajšej koľaji", nie je to tak. Právna teória v súvislosti s touto problematikou hovorí o tzv. **adhéznom konaní**. Napríklad v oblasti trestného práva sa uvádza, že adhézne konanie nie je samostatnou oddelenou časťou trestného konania, ale splýva s ním, a to najmä v štádiu dokazovania. V adhéznom konaní súd rozhoduje o náhrade škody podľa hmotného práva inej povahy, než trestnej, avšak vo forme trestného konania.[217] Orgány činné v trestnom konaní sú povinné zisťovať výšku škody, lebo je spravidla ako „následok" znakom skutkovej podstaty trestného činu.[218] Subjektom adhézneho konania nie je každý poškodený, ale len ten, ktorý má nárok na náhradu škody, ktorú možno vyčísliť v peniazoch. V adhéznom konaní musí trestný súd pri rozhodovaní o povinnosti obvineného nahradiť spôsobenú škodu použiť všetky príslušné hmotnoprávne predpisy občianskeho práva (prípadne iného odvetvia práva).[219] V trestnom konaní nemožno zisťovať výšku škody len voľnou úvahou; je nutné zistiť aspoň minimálnu výšku škody.[220]

Význam adhézneho konania spočíva v tom, že **umožňuje poškodenému, ktorý je stranou v trestnom konaní, aby bol súbežne s trestným stíhaním obvineného (obžalovaného) objasnený aj jeho nárok na náhradu škody** a aby poškodený dosiahol, že mu bude zároveň s rozhodnutím o podanej obžalobe prisúdená náhrada škody. Tento postup má pre poškodeného význam z hľadiska rýchlosti rozhodnutia o jeho nároku (v civilnom konaní by súd musel najprv vyčkať na právoplatné ukončenie trestnej veci), pričom nevyžaduje od poškodeného zvýšené výdavky.[221]

Z hľadiska koncepcie verejnoprávnej zodpovednosti má ďalej mimoriadny význam aj skutočnosť, že sa pri nej prísne uplatňuje **princíp *nullum crimen sine lege***.[222] Ide o základný princíp, ktorého podstata spočíva v tom, že nemožno považovať za protiprávne také konanie, ktoré za protiprávne nevyhlási zákon. Súkromnoprávna koncepcia vyvodzovania zodpovednosti pritom pozná aj vyvodenie zodpovednosti za porušenie zmluvy (delikt *ex contracto*).

---

[217] ŠÁMAL, P., BAXA, J. In ŠÁMAL, P., MUSIL, J., KUCHTA, J. a kol. *Trestní právo procesní*. Praha : C. H. Beck, 2013, s. 765.
[218] MATHERN, V. In IVOR, J. a kol. *Trestné právo procesné*. Bratislava : Iura Edition, 2010, s. 72.
[219] POLÁK, P. In IVOR, J. a kol. *Trestné právo procesné*. Bratislava : Iura Edition, 2010, s. 248.
[220] BAXA, J. In MUSIL, J., KRATOCHVÍL, V., ŠÁMAL, P. a kol. *Trestní právo procesní*. Praha : C. H. Beck, 2007, s. 860.
[221] ŠÁMAL, P., BAXA, J. In ŠÁMAL, P., MUSIL, J., KUCHTA, J. a kol. *Trestní právo procesní*. Praha : C. H. Beck, 2013, s. 765.
[222] S tým súhlasí aj právna teória, ktorá tento princíp spomína na mnohých miestach. Pozri napríklad CEPEK, B. *In VRABKO, M. a kol. Správne právo hmotné. Všeobecná časť*. Bratislava : C. H. Beck, 2012, s. 276; SREBALOVÁ, M. *In VRABKO, M. a kol. Správne právo procesné. Všeobecná časť. Bratislava : C. H. Beck, 2013*, s. 42 a nasl.; SREBALOVÁ, M. *In SREBALOVÁ, M. a kol. Zákon o priestupkoch. Komentár. Bratislava : C. H. Beck, 2015*, s. 249 a nasl.; KOŠIČIAROVÁ, S. *Verejná správa a právo na spravodlivý proces*. Krakov : Spolok Slovákov v Poľsku, 2014, s. 72; KOŠIČIAROVÁ, S. *Princípy dobrej verejnej správy a Rada Európy*. Bratislava : Iura Edition, 2012, s. 324 a nasl.; PRÁŠKOVÁ, H. *Základy odpovědnosti za správní delikty*. Praha : C. H. Beck, 2013, s. 31 a nasl.

Posledným významným rozdielom medzi súkromnoprávnou a verejnoprávnou koncepciou zodpovednosti, ktorému by som sa na tomto mieste chcel venovať, je **systém dôsledkov porušenia právnej povinnost**i. V zásade možno povedať, že základným dôsledkom porušenia súkromnoprávnych predpisov, je vznik druhotnej povinnosti v podobe navrátenia do pôvodného stavu, ak je možný, a ak nie je možný, tak potom povinnosť uhradiť skutočnú škodu.

V prípade verejnoprávnej koncepcie to nie je až tak „jednoduché". Som toho názoru, že **aj koncepcia verejnoprávnej zodpovednosti by mala mať za cieľ *restitutio in integrum*, avšak musí ho nevyhnutne skĺbiť aj s princípom *nullum poena sine lege***. Podstata tohto princípu spočíva v tom, že nemožno delikventovi uložiť inú sankciu, než tú, ktorú upravuje zákon. Možno si povšimnúť, že tu dochádza k istému posunu, pretože už hovorím o sankcii.

Sankcia vo všeobecnosti predstavuje určitý zásah do práv a slobôd delikventa, ktorý mu bol uložený v dôsledku porušenia jeho povinností a ktorý je povinný strpieť. Zastávam názor, že pojem **sankcia nemožno stotožňovať s pojmom trest a nemožno ju stotožňovať ani s pojmom právny dôsledok spáchania správneho deliktu**.

V tejto kapitole vychádzam z názoru, že pojem **právny dôsledok za spáchanie správneho deliktu je oveľa širším pojmom, než pojem sankcia a aj ako trest**. Právnymi dôsledkami spáchania správneho deliktu sú aj prostriedky, ktoré nemajú vyslovene represívny charakter, ale ktoré majú preventívny účinok, t. j. najmä ochranné opatrenia.[223] V najširšom slova zmysle pod pojem právny dôsledok spáchania správneho deliktu možno zahrnúť aj špecifické prostriedky, ktorými disponuje verejná správa v podobe napríklad zrušenia živnostenského oprávnenia,[224] prípadne nariadenia odstránenia stavby[225] a ďalšie, ktoré môžu, ale nemusia mať sankčný charakter, avšak zasahujú do právneho postavenia osoby v dôsledku porušenia zákonom určených povinností. Pod pojem právny dôsledok spáchania správneho deliktu v oblasti verejnoprávnej koncepcie zodpovednosti preto treba zahrnúť:

a) sankcie, kam radíme tresty, sankcie netrestného charakteru a ochranné opatrenia a

b) iné právne dôsledky za spáchanie verejnoprávneho deliktu.

K sankciám v oblasti verejného práva zaraďujeme tresty, sankcie netrestného charakteru a ochranné opatrenia. Ide o zhrnujúci pojem pre tieto odlišné právne dôsledky spáchania verejnoprávneho deliktu.

Rozdiel medzi nimi spočíva v tom, že **trest ako taký má výslovne represívny charakter**. Jeho cieľom je potrestať páchateľa a odradiť ho od opätovného páchania protiprávnej činnosti.

[223] K ochranným opatreniam pozri bližšie HORVAT, M. *In SREBALOVÁ, M. a kol. Zákon o priestupkoch. Komentár. Bratislava : C. H. Beck, 2015*, s. 78-92.
[224] § 58 zákona č. 455/1991 Zb. o živnostenskom podnikaní (živnostenský zákon).
[225] § 88 SZ.

K typickým trestom sa radí napríklad trest odňatia slobody, peňažný trest, trest prepadnutia majetku, trest prepadnutia veci, trest domáceho väzenia, trest povinnej práce.

Sankcie netrestného charakteru predstavujú také opatrenia, kde sa sankcionuje len páchateľ verejnoprávneho deliktu, **avšak cieľom uloženia takejto sankcie nie je represia, ale cieľom je náprava** (navrátenie do pôvodného stavu). Uloženie takejto sankcie je spôsobené porušením povinnosti páchateľom, pričom subjekt, ktorý ukladá túto sankciu má za cieľ odstrániť protiprávny stav a obnoviť stav zákonný. S tým je spojený aj fakt, že ak páchateľ dodatočne splní svoju povinnosť a takáto sankcia mu ešte nebola uložená, jej dodatočné uloženie už nie je možné. Tieto sankcie **môžu mať aj peňažný charakter**. Najznámejším príkladom sú tzv. poriadkové pokuty. Tie sa ukladajú v prípade, ak páchateľ nesplnil procesnoprávnu povinnosť, t. j. neplní si povinnosti súvisiace s priebehom určitého konania (napríklad trestného konania, správneho konania, či civilného konania) a tým znemožňuje jeho bezproblémový chod alebo ho aspoň sťažuje. Príkladom môže byť nepredloženie listiny alebo nedostavenie sa na výzvu orgánu na ústne pojednávanie. Uložením poriadkovej pokuty sa tu príslušný orgán snaží prinútiť páchateľa, aby si túto povinnosť splnil.

Ochranné opatrenia predstavujú spolu s trestami druhý okruh inštitútov, ktoré môže uplatniť orgán verejnej moci páchateľovi. Uložením ochranného opatrenia orgán verejnej moci na základe Ústavy Slovenskej republiky a v jej medziach, ako aj v medziach zákona zasahuje do osobnej slobody, slobody pohybu, prípadne do vlastníckeho práva páchateľa, prípadne aj inej osoby. Na rozdiel od trestov, ktorých hlavný účel spočíva v represii, náprave a odstránení nebezpečenstva voči spoločnosti, **pre ochranné opatrenia sú typické iba vlastnosti nápravného pôsobenia a ochrany spoločnosti.** Požiadavky na ochranné opatrenia vyplývajú z toho, že nie vždy sa ako vhodné javí použiť trest. V niektorých prípadoch je účelnejšie a pre ochranu spoločnosti výhodnejšie aj iné opatrenie než výlučne represívne (t. j. uloženie trestu), a preto zákonodarca upravuje aj ochranné opatrenia, ktoré z povahy veci vždy pôsobia *pro futuro*. Spôsobenie ujmy nie je základným charakteristickým dôsledkom uloženia ochranného opatrenia, ale až jeho druhotným cieľom vo vzťahu k ochrane spoločnosti a páchateľa. Preto ho nemožno považovať za trest.

Ochranným opatrením v oblasti verejného práva mám na mysli **najmä obmedzujúce opatrenia, ochranné liečenie, ochranná výchova, ochranný dohľad, detencia, či zhabanie veci**. **Inými právnymi dôsledkami** spáchania verejnoprávneho deliktu sú rôzne špecifické prostriedky ako už napríklad spomenuté zrušenie živnostenského oprávnenia, prípadne nariadenie odstránenia stavby alebo rôzne návrhy na odobratie licencií, či povolení, vykázanie z miesta a podobne.
Vzhľadom na charakter sankcií je potom len zrejmé, že ich môžu (musia) ukladať len orgány, ktoré sú na to priamo zákonom splnomocnené. Primárne ide o súdy a správne orgány.

V nasledujúcom texte budem vychádzať z členenia zodpovednosti podľa právnych odvetví, pričom vzhľadom na obsahové zameranie tejto kapitoly budem venovať pozornosť najprv

trestnému právu a potom správnemu právu a podmienkam vyvodzovania zodpovednosti podľa týchto odvetví. Text bude doplnený o analýzu základných rozdielov vyvodzovania zodpovednosti podľa týchto dvoch právnych odvetví.

3.3 Súdne delikty a správne delikty

Správne delikty spolu so súdnymi deliktmi tvoria **verejnoprávne delikty**. Verejnoprávne preto, lebo sú súčasťou právnych odvetví verejného práva (správneho práva a trestného práva), kde pri vyvodzovaní zodpovednosti vystupuje do popredia najmä represívna funkcia príslušných právnych odvetví.

Súdne delikty sa nazývajú aj pojmom **trestný čin**. Trestné činy sú definované v Trestnom zákone. Podľa tohto zákona je trestný čin protiprávny čin, ktorého znaky sú uvedené v Trestnom zákone, ak tento zákon neustanovuje inak. Trestné činy sa delia na prečiny a zločiny, pričom Trestný zákon presne vymedzuje, čo je prečin a čo je zločin.

Správne delikty sú kategóriou verejnoprávnych deliktov, o ktorých nerozhodujú súdy (ako v prípade trestných činov), ale orgány verejnej správy (správne orgány). Právna teória člení správne delikty na priestupky, správne disciplinárne delikty, správne poriadkové delikty, iné správne delikty fyzických osôb a správne delikty právnických osôb a podnikajúcich fyzických osôb, ako aj fyzických osôb vykonávajúcich kvalifikované činnosti.[226] Z nich len priestupky sú legálne definované; vymedzenie ostatných druhov správnych deliktov je ponechané na právnu teóriu.

Aj keď táto podkapitola je venovaná najmä odlišnostiam súdnych deliktov a správnych deliktov, treba spomenúť aj to, že k ich **spoločným znakom** patrí najmä to **skutková podstata** týchto deliktov je tvorená **štyrmi obligatórnymi znakmi, a to subjektom, subjektívnou stránkou, objektom a objektívnou stránkou.**

Skutkovú podstatu verejnoprávnych deliktov možno definovať ako súhrn objektívnych a subjektívnych typových znakov, pomocou ktorých sú jednotlivé druhy verejnoprávnych deliktov charakterizované a ktorými sa od seba aj navzájom odlišujú.[227] Súhrn týchto znakov musí vždy vyjadrovať spoločenskú škodlivosť verejnoprávneho deliktu.

Objekt deliktu. Objekt deliktu predstavuje konkrétnu **spoločenskú hodnotu, ktorá je chránená právnym poriadkom**. Objekt preto predstavuje právom chránený záujem, ktorý spoločnosť považuje za potrebný osobitnej ochrany. Vo všeobecnosti je objektom správnych deliktov záujem na riadnom a efektívnom chode verejnej správy, ale čoraz viac sa do právneho

[226] HAMUĽÁKOVÁ, Z. *In VRABKO, M. a kol. Správne právo hmotné. Všeobecná časť. Bratislava : C. H. Beck, 2018*, s. 208.
[227] Porovnaj FIALA, Z., HORZINKOVÁ, E. In FIALA, Z., FRUMAROVÁ, K., HORZINKOVÁ, E., ŠKUREK, M. a kol. *Správní právo trestní.* Praha : Leges, 2017, s. 30.

poriadku dostáva aj ochrana iných spoločenských záujmov, ako napríklad zdravie, majetok, či životné prostredie. Objektom súdnych deliktov je tradične život, zdravie a majetok a ďalšie hodnoty. Podľa stupňa všeobecnosti rozlišujeme objekt všeobecný, druhový a individuálny.[228] Všeobecným objektom sa rozumie súhrn chránených spoločenských vzťahov, záujmov a právnych hodnôt. Druhový objekt deliktu vyjadruje spoločné druhové znaky individuálnych objektov jednotlivých správnych deliktov, spoločné záujmy v určitej vecnej oblasti, preto je druhový objekt základom utriedenia skutkových podstát deliktov. Napríklad podľa druhového objektu je usporiadaná osobitná časť zákona o priestupkoch. Individuálny objekt je obligatórnym znakom každej skutkovej podstaty deliktu. Je ním konkrétny jednotlivý záujem, proti ktorému delikt smeruje a na ktorého ochranu je príslušné ustanovenie určené.[229]

Subjekt deliktu. Delikt musí spáchať konkrétna osoba (t. j. nie vyššia moc), aby bolo možné vyvodiť voči nej zodpovednosť. V súčasnosti platí, že vo všeobecnej rovine verejnoprávny delikt môžu spáchať tak fyzické osoby, ako aj právnické osoby. Konkrétne potom bude záležať od druhu deliktu; napríklad priestupok môže spáchať len fyzická osoba, právnické osoby nie sú priestupkovo zodpovedné. Subjekt deliktu tak vypovedá o tom, kto môže byť právne zodpovedný za spáchanie deliktu, kto je spôsobilým subjektom niesť zodpovednosť. Subjekt deliktu teda nie je páchateľ ako taký, ale ten, voči komu možno zodpovednosť vyvodiť; v subjekte deliktu sa tak kumulujú podmienky nadobudnutia deliktuálnej spôsobilosti v oblasti právnej zodpovednosti.

O tom, kto konkrétne môže byť subjektom deliktu bude vypovedať konkrétny druh deliktu. V prípade správnych deliktov právnických osôb to budú právnické osoby, a to od okamihu zápisu do príslušného registra, s ktorým je spojený vznik takejto osoby. To isté bude platiť vo vzťahu k trestnej zodpovednosti právnických osôb. V prípade priestupku ide o fyzickú osobu, ktorá dovŕšila vek 15 rokov a v čase spáchania priestupku bola príčetná.

Subjekt deliktu podľa vymedzenia stupňa jeho všeobecnosti rozlišujeme subjekt všeobecný, špeciálny a individuálny.

Všeobecným subjektom rozumieme akúkoľvek osobu, ktorá je deliktuálne spôsobilá. Vo všeobecnej rovine tu bude záležať od konkrétneho druhu deliktu, aby sme vedeli určiť, kto je a kto nie je potenciálne zodpovedný za spáchanie deliktu. V skutkovej podstate deliktov je všeobecný

[228] MACHAJOVÁ, J. In MACHAJOVÁ, J. a kol. *Všeobecné správne právo.* Žilina : Eurokódex, 2009, s. 203.
[229] Pozri HAMUĽÁKOVÁ, Z. *In VRABKO, M. a kol. Správne právo hmotné. Všeobecná časť. Bratislava : C. H. Beck, 2018*, s. 206.

subjekt vymedzený všeobecne pomocou pojmov ako „kto“,[230] „fyzická osoba“,[231] „právnická osoba“.[232]

V prípade špeciálneho subjektu pristupujú k všeobecným podmienkam nadobudnutia právnej zodpovednosti aj ďalšie podmienky, ktoré zodpovednú osobu bližšie špecifikujú. Ide o podmienky špeciálnej spôsobilosti, postavenia, či vlastnosti takejto osoby. Osoba bude zodpovedať za spáchanie správneho deliktu len v takom prípade, ak tieto špeciálne podmienky napĺňa.[233]

Individuálnym subjektom je taký subjekt, kde miera špecifickosti je natoľko výrazná, že zásadne môže ísť iba o jednu konkrétnu osobu, ktorá je zodpovedná za spáchanie správneho deliktu.[234]

Objektívna stránka deliktu. Objektívnou stránkou deliktov sa od seba jednotlivé delikty najvýraznejšie odlišujú. Je to dané skutočnosťou, že objektívna stránka deliktu reprezentuje prejav deliktu v reálnom živote; objektívna stránka je postihnuteľná zmyslami človeka, možno ju vnímať a pozorovať. Z daného dôvodu je objektívna stránka v skutkovej podstate vymedzená slovesom (či už dokonavým vidom alebo nedokonavým vidom).

Objektívna stránka deliktu je daná konaním, protiprávnym následkom a príčinnou súvislosťou medzi konaním a protiprávnym následkom. **Konanie** predstavuje prejav vôle osoby vo vonkajšom svete, ktoré je spojené s aktivitou ľudského tela ako prejavu vôle človeka. Prejavu konania vo vonkajšom svete vždy predchádza vnútorná vôľa človeka určitým spôsobom konať. Niekedy sa môže stať, že tieto zložky sa nespoja; vtedy nemožno hovoriť o delikte, napríklad v prípade epileptického záchvatu osoby alebo jej ochrnutia a pod. Konanie môže mať aktívnu podobu konania, ide o tzv. komisívne konanie, alebo môže mať pasívu podobu (opomenutie konania) – tzv. omisívne konanie. Pokiaľ zo skutkovej podstaty deliktu nevyplýva inak, možno delikt spáchať tak komisívne, ako aj omisívne.

---

[230] Priestupku sa dopustí ten, *kto* neuposlúchne výzvu verejného činiteľa pri výkone jeho právomoci [§ 47 ods. 1 písm. a) zákona o priestupkoch; pozri aj SREBALOVÁ, M. In SREBALOVÁ, M. a kol. *Zákon o priestupkoch. Komentár.* Bratislava : C. H. Beck, 2015, s. 213].

[231] Priestupku sa dopustí *fyzická osoba*, ktorá poruší povinnosť uvedenú v § 12 ods. 1 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti [§ 30 ods. 1 písm. a) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti; pozri aj GÁBRIŠ, T. *In ANDRAŠKO, J., GÁBRIŠ, T., HOCHMANN, J., OLEJÁR, D. Zákon o kybernetickej bezpečnosti*. Bratislava : Wolters Kluwer, 2018, s. 263-267].

[232] Správneho deliktu sa dopustí *právnická osoba*, ak poruší nariadenie [§ 27b ods. 1 písm. a) zákona o obecnom zriadení; pozri aj KOŠIČIAROVÁ, S. *Zákon o obecnom zriadení.* Bratislava : Eurokódex, 2018, s. 177-180.

[233] Napríklad: priestupku v oblasti prevádzkovania hazardných hier, propagovania hazardných hier alebo súvisiacich činností sa dopustí *fyzická osoba, ktorá je dozorovaným subjektom* podľa § 80 písm. b) až k) zákona č. 30/2019 Z. z. o hazardných hrách a (...); priestupku sa dopustí *fyzická osoba, ktorá nie je oprávnená na podnikanie* a (...) podľa § 41a ods. 1 zákona č. 106/2004 Z. z. o spotrebnej dani z tabakových výrobkov; Národný bezpečnostný úrad uloží pokutu od 300 eur do 30 000 eur *poskytovateľovi digitálnej služby* (poskytovateľom digitálnej služby je právnická osoba alebo fyzická osoba – podnikateľ, ktorá poskytuje digitálnu službu a zároveň zamestnáva aspoň 50 zamestnancov a má ročný obrat alebo celkovú ročnú bilanciu viac ako 10 000 000 eur), ktorý sa dopustí správneho deliktu tým, že (...) podľa § 31 ods. 3 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti.

[234] Napríklad *poplatník* podľa zákona č. 329/2018 Z. z. o poplatkoch za uloženie odpadov, kde poplatníkom je posledný držiteľ odpadu alebo *správca informačného systému verejnej správy* podľa § 56 ods. 1 písm. b) zákona č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci (zákon o e-Governmente).

V legislatívnej praxi sa môžeme stretnúť aj s nepravými omisívnymi deliktmi. V danom prípade chýba vyjadrenie objektívnej stránky prostredníctvom slovesa, ale objektívna stránka je vyjadrená iba protiprávnym následkom; je preto irelevantné, akým konaním (opomenutím konania) došlo k protiprávnemu následku, podstatná je tu skutočnosť, že tento protiprávny následok nastal.[235]

Protiprávny následok je dôsledkom konania páchateľa deliktu. Je v ňom vyjadrený škodlivý následok, ktorý je spojený s páchaním protiprávnej činnosti. Ten môže nastať ohrozením určitej spoločenskej hodnoty alebo jej porušením. Pre správne delikty platí, že pokiaľ nie je ustanovené inak, treba na naplnenie tohto znaku porušiť spoločenskú hodnotu, nestačí ju len ohroziť.

Príčinná súvislosť alebo tzv. *kauzálny nexus* predstavuje vyjadrenie myšlienky, že každá akcia má svoju reakciu. Ten, kto vyvodzuje zodpovednosť, je povinný páchateľovi preukázať kauzálny nexus nad všetku pochybnosť, inak voči nemu nemožno vyvodiť zodpovednosť. Inými slovami, treba preukázať tú skutočnosť, že práve týmto konaním danej osoby nastal práve tento protiprávny následok.

Nepovinnými súčasťami objektívnej stránky deliktu sú napríklad miesto konania,[236] doba konania,[237] spôsob uskutočnenia,[238] hmotný predmet útoku,[239] účinok[240] a použité prostriedky.[241,242]

Subjektívna stránka deliktu. Subjektívna stránka deliktu vyjadruje zavinenie páchateľa. Ide o vnútorný vzťah páchateľa k spáchanému deliktu. Subjektívna stránka deliktu sa nevyžaduje vo vzťahu ku každému druhu deliktu, ale len pri tých, ktoré sú vybudované na princípe subjektívnej zodpovednosti, takýto deliktom sú napríklad trestné činy spáchané fyzickou osobou alebo priestupky. Pri správnych deliktoch, ktoré sú vybudované na základe princípe objektívnej zodpovednosti, ako napríklad správne delikty právnických osôb a správne delikty fyzických osôb podnikateľov, sa zavinenie neskúma.

Zavinenie sa skladá z dvoch zložiek, a to zo zložky vedomostnej (intelektuálnej, rozumovej) a zložky vôľovej. Vo všeobecnosti sa uznáva, že intelektuálna zložka predstavuje nielen vnímanie

---

[235] Ako príklad môže slúžiť už spomínaný správny delikt podľa § 27b ods. 1 písm. a) zákona o obecnom zriadení, podľa ktorého sa správneho deliktu dopustí právnická osoba, ak poruší nariadenie, pričom zákon bližšie neuvádza, akým spôsobom môže dôjsť k tomuto porušeniu nariadenia.

[236] Podľa § 47 ods. 1 písm. l) zákona o priestupkoch sa priestupku dopustí ten, kto v súvislosti *s účasťou na verejnom zhromaždení alebo kultúrnom podujatí prístupnom verejnosti* (...).

[237] Podľa § 159 ods. 2 písm. a) bod 21 zákona č. 87/2018 Z. z. o radiačnej ochrane príslušný orgán radiačnej ochrany uloží pokutu od 500 eur do 30 000 eur fyzickej osobe – podnikateľovi alebo právnickej osobe, ak vysiela zasahujúcu osobu k zásahu *v núdzovej situácii* bez jej súhlasu.

[238] Podľa § 27 zákona č. 17/2018 Z. z. o veterinárnych prípravkoch a veterinárnych technických pomôckach sa priestupku dopustí ten, kto *vyrába, uvádza na trh alebo distribuuje* veterinárny prípravok alebo veterinárnu technickú pomôcku..

[239] Podľa § 30 ods. 1 písm. a) zákona o priestupkoch sa priestupku sa dopustí ten, kto predá, podá alebo inak umožní požitie alkoholických nápojov *osobe zjavne ovplyvnenej alkoholickým nápojom alebo inou návykovou látkou, osobe mladšej ako osemnásť rokov* (...).

[240] Podľa § 49 ods. 1 písm. b) zákona o priestupkoch sa priestupku sa dopustí ten, kto inému z nedbanlivosti *ublíži na zdraví.*

[241] Podľa § 47a ods. 1 písm. a) zákona o priestupkoch sa priestupku extrémizmu dopustí ten, kto použije na verejnosti *písomné, grafické, obrazové, zvukové alebo obrazovo-zvukové vyhotovenie textov a vyhlásení, zástav, odznakov, hesiel alebo symbolov skupín alebo hnutí a ich programov alebo ideológií*, ktoré smerujú k potláčaniu základných ľudských práv a slobôd.

[242] FIALA, Z., HORZINKOVÁ, E. In FIALA, Z., FRUMAROVÁ, K., HORZINKOVÁ, E., ŠKUREK, M. a kol. *Správní právo trestní.* Praha : Leges, 2017, s. 33.

skutočnosti páchateľom, ale znamená aj jeho predstavu o skutočnosti, ktorá vyplýva z jeho predchádzajúcich skúseností. Zložka vôle vo svojej podstate znamená vôľu páchateľa vyvolať určité konkrétne následky svojho konania a o ktorých sa predpokladá, že ich chce dosiahnuť, alebo je aspoň o nich uzrozumený.

Kombináciou a odstupňovaním vedomostnej a vôľovej zložky sa rozlišuje nedbanlivosť (nevedomá a vedomá) a úmysel (priamy a nepriamy). Vo všeobecnosti možno povedať, že na vyvodenie zodpovednosti za správny delikt nepostačuje len vyvolať škodlivý následok, ale tento následok treba aj zaviniť.

Delikt je spáchaný **z nedbanlivosti**, ak páchateľ

a) vedel, že môže svojím konaním porušiť alebo ohroziť záujem chránený zákonom, ale bez primeraných dôvodov sa spoliehal na to, že tento záujem neporuší alebo neohrozí, alebo

b) nevedel, že svojím konaním môže porušiť alebo ohroziť záujem chránený zákonom, hoci to vzhľadom na okolnosti a na svoje osobné pomery vedieť mal a mohol.

Delikt je spáchaný **úmyselne**, ak páchateľ

a) chcel svojím konaním porušiť alebo ohroziť záujem chránený zákonom alebo

b) vedel, že svojím konaním môže porušiť alebo ohroziť záujem chránený zákonom, a pre prípad, že ho poruší alebo ohrozí, bol s tým uzrozumený.

V oblasti **správneho trestania** sa všeobecne akceptuje, že pokiaľ skutková podstata správneho deliktu neustanovuje inak, **postačuje na vznik zodpovednosti preukázať nedbanlivostné konanie páchateľa**. Ak však skutková podstata výslovne vyžaduje úmyselné konanie, takýto správny delikt nemožno spáchať nedbanlivostne; správny orgán v takom prípade nemôže vyvodiť zodpovednosť. Ak správny delikt výslovne vyžaduje nedbanlivostné konanie páchateľa, možno takýto správny delikt spáchať aj úmyselne.

Inak to bude v **prípade trestných činov**, kde platí, že pre trestnosť činu spáchaného fyzickou osobou **treba úmyselné zavinenie**, ak zákon výslovne neustanovuje, že stačí zavinenie z nedbanlivosti.

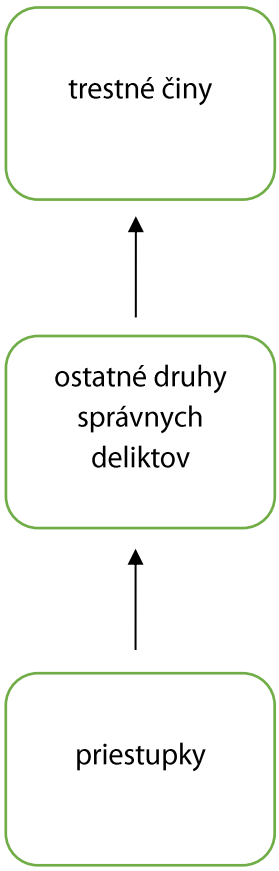
K fakultatívnym znakom zavinenia sa zaraďuje najmä pohnútka, cieľ, či účel. V prípade, ak skutková podstata deliktu uvádza pohnútku, cieľ alebo účel, musí orgán preukázať zavinenie aj vo vzťahu k týmto znakom skutkovej podstaty deliktu. Pohnútka, cieľ alebo účel môžu ovplyvniť určenie druhu sankcie a jej výmeru.[243]

Pre správne delikty vybudované na základe objektívneho princípu platí, že ich skutková podstata sa teda skladá len z **troch obligatórnych znakov**, a to subjekt, objekt a objektívna stránka.

[243] Pozri HORVAT, M. In SREBALOVÁ, M. a kol. *Zákon o priestupkoch. Komentár.* Bratislava : C. H. Beck, 2015, s. 20-21.

V praxi môže vzniknúť otázka, **ktoré či z hľadiska vyvodzovania zodpovednosti má prednosť vyvodenie zodpovednosti za súdny delikt alebo za správny delikt.** Môže sa totiž stať, že skutková podstata trestného činu a správneho deliktu sa budú v časti objektívnej stránky prekrývať. Vzhľadom na to, že v právnom štáte sa uplatňuje princíp *ne bis in idem*, t. j. nie dvakrát v tej istej veci, je nevyhnutné zaviesť pravidlo, ktoré by určilo, vyvodenie ktorej zodpovednosti má prednosť.
Vzhľadom na skutočnosť, že **trestná činnosť** sa považuje za **spoločensky závažnejší** protiprávny čin, vyvodenie administratívnoprávnej zodpovednosti ustupuje vyvodeniu zodpovednosti trestnoprávnej. Inými slovami, ak je čin trestným činom, potom sa bude vyvodzovať trestnoprávna zodpovednosť a nie správnoprávna.

Istá **hierarchia** potom panuje aj **v rámci správnych deliktov**, kde špeciálnymi správnymi deliktmi sú všetky ostatné delikty okrem priestupkov. To vyplýva z legálnej definície pojmu priestupok, podľa ktorej priestupkom nie je konanie, ktoré vykazuje znaky iného správneho deliktu. To znamená, že vyvodenie zodpovednosti za priestupok ustupuje vyvodeniu zodpovednosti za ostatné druhy správnych deliktov tak, aby aj v tomto prípade bol dodržaný princíp *ne bis in idem*.
Pre zjednodušenie uvádzame **obrázok**, ktorý reprezentuje nielen členenie verejnoprávnych deliktov, ale taktiež aj hierarchiu medzi jednotlivými druhmi deliktov.



V čom sa od seba **odlišujú** správne delikty a trestné činy?

Právna teória ako ani právna prax **nedospela k jednoznačnému deliacemu kritériu**, kedy určité protiprávne konanie je správnym deliktom a kedy už trestným činom. Táto skutočnosť vychádza najmä z toho, že deliace kritérium nemožno vysledovať v akomkoľvek prirodzenoprávnom koncepte. Jednoznačne akceptovateľné kritérium teda v súčasnosti nenachádzame.[244] Podvedome možno usúdiť, že **kritériom by mala byť závažnosť** skutku alebo **dôležitosť** ochrany objektu vymedzenom v skutkovej podstate. V oboch prípadoch však ide o neurčité pojmy, ktorých obsah sa môže meniť a vyvíjať. Reálnym deliacim kritériom preto v zásade ostáva vôľa zákonodarcu, či určité konanie označí za právom povolené konanie, správny delikt alebo trestný čin.

V zásade k rovnakému záveru prichádza aj súdna **judikatúra**, ktorá konštantne uvádza, že je potrebné zdôrazniť, že formálne označenie určitého typu protispoločenského konania a tomu zodpovedajúce zaradenie medzi trestné činy, priestupky, iné správne delikty a z toho vyvodené následky v podobe sankcií, vrátane príslušného konania, pritom či už ide o oblasť súdneho alebo správneho trestania, **je len vyjadrením reálnej trestnej politiky štátu**, teda reflexia názoru spoločnosti na potrebnú mieru ochrany jednotlivých vzťahov a záujmov. Kriminalizácia, či naopak dekriminalizácia určitého konania nachádza výraz v platnej právnej úprave a v ich zmenách, voľbe procesných nástrojov potrebných k odhaleniu a dokázaniu konkrétnych skutkov, ako aj prísnosti postihu delikventa.[245]

Aj na základe uvedeného preto nasledujúce odlíšenia správnych deliktov a trestných činov majú len podporný význam.

Trestné činy sú zákonodarcom priamo definované a ich výpočet je taxatívne vymedzený v jednom právnom predpise. Správne delikty s výnimkou priestupkov nie sú legálne definované, skutkové podstaty správnych deliktov môžu byť vymedzené aj demonštratívne a sú vymedzené v množstve právnych predpisov.

Trestné činy sú definované v Trestnom zákone. Trestný čin je protiprávny čin, ktorého znaky sú uvedené v Trestnom zákone, ak tento zákon neustanovuje inak. Trestný čin **je prečin a zločin** (tzv. bipartícia trestných činov). Prečin je trestný čin spáchaný z nedbanlivosti alebo úmyselný trestný čin, za ktorý Trestný zákon v osobitnej časti ustanovuje trest odňatia slobody s hornou hranicou trestnej sadzby neprevyšujúcou päť rokov. Zločin je úmyselný trestný čin, za ktorý Trestný zákon v osobitnej časti ustanovuje trest odňatia slobody s hornou hranicou trestnej sadzby prevyšujúcou päť rokov. O zločin ide aj vtedy, ak v prísnejšej skutkovej podstate prečinu spáchaného úmyselne je ustanovená horná hranica trestnej sadzby prevyšujúca päť rokov. Zločin, za ktorý Trestný zákon ustanovuje trest

[244] Porovnaj MACHAJOVÁ, J. In MACHAJOVÁ, J. a kol. *Všeobecné správne právo.* Žilina : Eurokódex, 2009, s. 193.
[245] Pozri napríklad tieto rozhodnutia Najvyššieho súdu: sp. zn. 8 Sžo 28/2007 zo 6. marca 2008, sp. zn. 8Sžo/35/2012 z 13. júna 2013, sp. zn. 10Sžo/265/2015 z 28. septembra 2016, sp. zn. 7Sžo/60/2016 zo 14. decembra 2017.

odňatia slobody s dolnou hranicou trestnej sadzby najmenej desať rokov, sa považuje za obzvlášť závažný.[246] **Skutkové podstaty** trestných činov sú **vymedzené v** § 144 až 435 **Trestného zákona**.

Správne delikty zákonom definované nie sú. Výnimku tvorí priestupok, ktorý je legálne definovaný v § 2 ods. 1 zákona o priestupkoch. Všetky ostatné druhy správnych deliktov sú vymedzené len z pohľadu právnej teórie. Rovnako tak platí, že **skutkové podstaty** správnych deliktov nie sú vymedzené v jednom zákone, ale **v množstve rôznych zákonov**. Pre správne delikty potom aj platí, že na základe zákona môže byť skutková podstata bližšie vymedzená aj v podzákonnom právnom predpise, napríklad v nariadení územnej samosprávy[247] alebo vo vnútorných predpisoch profesijnej komory (typicky v Etickom kódexe alebo inak obdobne nazvanom internom predpise[248]).

Ďalším významným rozdielom je **rozdiel v orgánoch**, ktoré prejednávajú tieto verejnoprávne delikty. Rozhodovať o vine a treste za spáchaný **trestný čin môžu len súdy**, a to na základe žaloby, ktorú môže podať len prokurátor. Súdy pri rozhodovaní o vine a treste majú postavenie nezávislých a nestranných orgánov; toto ich postavenie vyplýva nielen z Ústavy Slovenskej republiky, ale aj z množstva medzinárodných dohovorov, ktorými je Slovenská republika viazaná. Vecná a miestna príslušnosť na trestné konanie vyplýva z Trestného poriadku.

Rozhodovať o vine a treste za spáchané **správne delikty môžu len správne orgány** ako orgány reprezentujúcu verejnú správu; o správnom delikte v zmysle rozhodovania o vine a sankcii za spáchaný správny delikt nerozhodujú súdy. Súdy, konkrétne v oblasti verejnej správy tzv. správne súdy, iba preskúmavajú rozhodnutia správnych orgánov vo veci správneho trestania, t. j. preskúmavajú, či konanie a rozhodnutie správneho orgánu neprekročilo medze a hranice zákona; o vine ako takej správne súdy nerozhodujú. Správne orgány taktiež nemajú postavenie nezávislých a nestranných orgánov. Príslušnosť správneho orgánu na konanie vo veci vyplýva z príslušných osobitných právnych predpisov.

Súdy v trestnom konaní **rozhodujú na základe** jedného procesnoprávneho predpisu, ktorým je **Trestný poriadok**.

Procesný režim, ktorým sa riadia **správne orgány** pri vyvodzovaní zodpovednosti, **nie je tak jednoduchý a kodifikovaný**. V prípade priestupkov sa postupuje primárne podľa osobitného predpisu, ktorý upravuje skutkovú podstatu priestupku, ktorý sa obvinenému kladie za vinu s podporným použitím najprv zákona o priestupkoch a následne aj Správneho poriadku. V prípade iných správnych deliktov sa postupuje podľa osobitného predpisu s podporným použitím Správneho poriadku. Špecifikom sú správne disciplinárne delikty, kde sa postupuje podľa interných

[246] § 8 až 11 Trestného zákona.
[247] Pozri napríklad § 27b ods. 1 písm. a) zákona o obecnom zriadení.
[248] Pozri napríklad § 56 ods. 1 zákona č. 586/2003 Z. z. o advokácii.

predpisov vydaných na základe zákonného splnomocnenia s podporným použitím Správneho poriadku a v prípade niektorých správnych disciplinárnych deliktov dokonca s použitím Trestného poriadku a nie Správneho poriadku.[249]

Z hľadiska objektu je **trestnoprávna ochrana** poskytovaná najmä takým hodnotám, ako sú **život, zdravie, majetok osôb**. V prípade **správnych deliktov** by mala byť objektom **predovšetkým ochrana riadneho výkonu verejnej správy**. V súčasnosti však toto deliace kritérium je len veľmi všeobecné, pretože aj správnymi deliktami sa chránia mnohé významné spoločenské hodnoty, ako sú spomínaný život, zdravie, majetok, či životné prostredie.

Skutočnosť, že osoba je odsúdená za spáchanie trestného činu, má pre túto osobu aj dôsledky v spoločenskom živote. S odsúdením za trestný čin je totiž spojený **zápis do registra trestov.** V registri trestov sa evidujú údaje o osobách a nimi spáchaných trestných činoch. Výpis z registra trestov je verejná listina, ktorou sa preukazuje, či osoba bola alebo nebola právoplatne odsúdená; uvádzajú sa v ňom len nezahladené odsúdenia. Výpis z registra trestov „bez záznamu" je potrebný na preukazovanie bezúhonnosti osoby. **Bezúhonnosť** môže byť podmienkou napríklad možnosti uchádzania sa o pozície v štátnej službe,[250] či napríklad podmienka získania živnostenského oprávnenia[251] atď.

Vo vzťahu k správnych deliktom **neexistuje ich centrálna evidencia**. Takéto evidencie si interne môže viesť orgán verejnej správy, ale takáto povinnosť mu nevyplýva z právneho predpisu. Neexistencia centrálnej evidencie môže spôsobovať v praxi problémy najmä v súvislosti s recidívou.[252] Jedinou výnimkou v tejto súvislosti sú priestupky, kde ústredné orgány štátnej správy sú povinné viesť evidenciu priestupkov.[253] Spáchanie správneho deliktu so sebou nenesie stratu bezúhonnosti, ako je to v prípade spáchania trestného činu.

Z pohľadu sankcií treba tiež pripomenúť, že **za spáchanie správneho deliktu páchateľovi nehrozí trest odňatia slobody alebo trest zrušenia právnickej osoby**. Tieto závažné sankcie môžu byť ukladané len súdom v rámci trestného konania; ide teda iba o sankcie za spáchanie trestného činu.

K rozdielom medzi súdnymi deliktami a správnymi deliktami *de lege lata* môžeme radiť aj to, že v **prípade správnych deliktov sa tradične za trestné považuje len dokonanie správneho**

---

[249] Pozri § 57 ods. 7 zákona č. 586/2003 Z. z. o advokácii, § 28 ods. 10 zákona č. 314/2018 Z. z. o Ústavnom súde Slovenskej republiky, § 150 ods. 2 zákona č. 385/2000 Z. z. o sudcoch a prísediacich.

[250] MASLEN, M. In CEPEK, B. a kol. *Správne právo hmotné. Všeobecná časť.* Bratislava : Wolters Kluwer, 2018, s. 264; § 38 ods. 1 písm. c) zákona o štátnej službe.

[251] HORVAT, M In HORVAT, M. a kol. *Živnostenský zákon. Komentár.* Bratislava : Wolters Kluwer, 2019, s. 83 a nasl.; 6 ods. 1 písm. c) živnostenského zákona.

[252] Recidíva predstavuje situáciu, keď ten istý páchateľ znovu spácha správny delikt po tom, ako bol právoplatne uznaný za vinného rozhodnutím správneho orgánu.

[253] SREBALOVÁ, M. In SREBALOVÁ, M. a kol. *Zákon o priestupkoch. Komentár.* Bratislava : C. H. Beck, 2015, s. 455-461; § 89a zákona o priestupkoch.

deliktu a nie jeho vývinové štádium (pokus, príprava). Inými slovami, pokus alebo príprava správneho deliktu nezakladá administratívnoprávnu zodpovednosť. Výnimku môže ustanoviť len zákon.[254] V prípade **trestných činov** platí, že trestné môžu byť a sú aj niektoré jeho **vývinové štádiá.** Podľa Trestného zákona **pokus trestného činu** je konanie, ktoré bezprostredne smeruje k dokonaniu trestného činu, ktorého sa páchateľ dopustil v úmysle spáchať trestný čin, ak nedošlo k dokonaniu trestného činu. Pokus trestného činu je trestný podľa trestnej sadzby ustanovenej na dokonaný trestný čin. **Príprava na zločin** je konanie, ktoré spočíva v úmyselnom organizovaní zločinu, zadovažovaní alebo prispôsobovaní prostriedkov alebo nástrojov na jeho spáchanie, v spolčení, zhluknutí, návode, objednávaní alebo pomoci na taký zločin alebo v inom úmyselnom vytváraní podmienok na jeho spáchanie, ak nedošlo k pokusu ani dokonaniu zločinu. Príprava na zločin je trestná podľa trestnej sadzby ustanovenej za zločin, ku ktorému smerovala.

Vidno, že pokus je trestný vo vzťahu k všetkým trestným činom, avšak príprava je trestná len vo vzťahu k zločinom. Oboch prípadoch platí, že **sú trestné podľa trestnej sadzby ustanovenej ako za dokonaný trestný čin**.

3.4 Trestnoprávna zodpovednosť

V rámci výkladu o zodpovednosti začneme s jej trestnoprávnou rovinou. V súvislosti s predmetom tejto kapitoly sa v trestnoprávnej náuke hovorí o **tzv. počítačovej kriminalite**. Tá patrí medzi najrýchlejšie rastúcu oblasť trestnej činnosti v posledných rokoch. Stále viac páchateľov využíva rýchle, pohodlné a najmä anonymné prostredie internetu alebo počítačových sietí k páchaniu celej škály trestných činov, ktoré nepoznajú hranice a spôsobujú vážne ujmy a hrozby obetiam na celom svete.[255] Hoci v právnej praxi sa tento pojem používa a počítačová kriminalita je zdokumentovaná už od 60. rokov minulého storočia, nie je tento pojem dodnes všeobecne uspokojivo definovaný.

Podľa dôvodovej správy k návrhu zákona o európskom ochrannom príkaze v trestných veciach a o zmene a doplnení niektorých zákonov je počítačová kriminalita, ako jedna z oblastí **modernej kriminálnej činnosti**, ktorej rozmach je sledovaný najmä v posledných rokoch v súvislosti s nástupom digitálneho veku, **súborom protiprávnych konaní, ktorých hlavným znakom je využívanie informačných technológií, najmä počítačov, na páchanie trestnej činnosti.** Jej rozmach je priamoúmerný postupujúcej informatizácii a „internetizácii" spoločnosti.[256]

---

[254] Ide o veľmi výnimočné situácie. K nim možno zaradiť § 50 zákona o priestupkoch, podľa ktorého priestupku proti majetku sa dopustí ten, kto úmyselne spôsobí škodu na cudzom majetku krádežou, spreneverou, podvodom alebo zničením alebo poškodením veci z takého majetku, *alebo sa o takéto konanie pokúsi*.

[255] BENEDEKOVÁ, D. In MARKOVÁ, V. (ed.) *Aktuálne otázky trestného práva v teórii a* praxi. Bratislava : Akadémia Policajného zboru v Bratislave, 2016, s. 20.

[256] ZÁHORA, J. Aktuálne trendy v postihu počítačovej kriminality v Slovenskej republike. *In Justičná revue, 68, 2016, č. 3*, s. 324.

Zároveň treba uviesť, že počítačová kriminalita predstavuje v Európskej únii tzv. „európsky trestný čin" (pozri čl. 83 ods. 1 Zmluvy o fungovaní Európskej únie v znení Lisabonskej zmluvy).[257] Z daného dôvodu sa v rámci slovenského trestného zákonodarstva odráža právna úprava, ktorej základy nám „prinieslo" členstvo v Európskej únii.

Záujem medzinárodného spoločenstva o počítačovú kriminalitu je daný aj tým, že **počítačová kriminalita „nepozná hranice"**. Vzhľadom na to, že počítačová kriminalita je nadnárodný fenomén, riešeniu tejto problematiky sa venujú **viaceré medzinárodné, resp. nadnárodné organizácie.** Z medzinárodných nástrojov možno spomenúť napríklad Odporúčanie Výboru ministrov Rady Európy o počítačovej kriminalite. Z ďalších dokumentov Rady Európy možno poukázať na Dohovor o počítačovej kriminalite, ktorý pre Slovenskú republiku nadobudol platnosť 1. mája 2008 a ktorý možno považovať za najkomplexnejší nástroj na boj proti počítačovej kriminalite, obsahujúci jednak hmotnoprávne ustanovenia, ale aj procesné ustanovenia a ustanovenia o medzinárodnej spolupráci. Vo vzťahu k detskej pornografii, ku kriminalizácii vedomého získavania prístupu cez informačné alebo komunikačné technológie k detskej pornografii, zaväzuje čl. 20 ods. 1 písm. f) Dohovoru o ochrane detí pred sexuálnym vykorisťovaním a sexuálnym zneužívaním, ktorý je v Slovenskej republike v štádiu ratifikačného procesu. Vo vzťahu k počítačovej kriminalite páchanej zločineckými skupinami určité aspekty upravuje aj čl. 29 ods. 1 písm. h) Dohovoru OSN proti nadnárodnému organizovanému zločinu. Z ďalších medzinárodných nástrojov možno spomenúť napríklad Rezolúciu VZ OSN o boji proti zneužívaniu informačných technológií. Významným legislátorom v tejto oblasti je aj Európska únia, resp. Európske spoločenstvá. Už v roku 1991 bola prijatá Smernica o právnej ochrane počítačových programov, v roku 2000 Smernica o elektronickom obchode, v roku 2001 Rámcové rozhodnutie o boji proti podvodom a falšovaniu bezhotovostných platobných prostriedkov, v roku 2002 Smernica o súkromí a elektronických komunikáciách, v roku 2005 Rámcové rozhodnutie o útokoch na informačné systémy, v roku 2006 Smernica o uchovávaní údajov vytvorených alebo spracovaných v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb alebo verejných komunikačných sietí, v roku 2011 Smernica o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorá zaväzuje členské štáty kriminalizovať distribúciu, resp. získavanie detskej pornografie pomocou informačných a komunikačných technológií, a medzi posledné akty možno zaradiť Smernicu o útokoch na informačné systémy, ktorá zohľadňuje nové metódy páchania počítačových trestných činov a významne rozširuje komplex protiprávnych konaní v súvislosti s neoprávneným prístupom do počítačových systémov, neoprávneným zásahom do počítačových systémov a počítačových údajov,

[257] KLIMEK, L. Boj proti útokom na informačné systémy na úrovni Európskej únie. *In Justičná revue, 68, 2016, č. 2*, s. 185 a nasl.

neoprávneným zachytávaním počítačových údajov a nakladanie s nástrojmi určenými na spáchanie týchto trestných činov.[258]

Z uvedených medzinárodných dokumentov treba osobitne spomenúť dva, a to

a) **Dohovor o počítačovej kriminalite z roku 2001**, ktorý je na medzinárodnej úrovni považovaný za **najúplnejšiu súčasnú medzinárodnú normu**. Je to právny dokument, ktorý poskytuje komplexný a ucelený rámec zahŕňajúci viaceré aspekty počítačovej kriminality v medzinárodnom európskom kontexte. (...) uvedený Dohovor je právnym referenčným rámcom pre boj proti počítačovej kriminalite vrátane útokov na informačné systémy. Nadväznosť EÚ na tento Dohovor bola vyjadrená už pred viac než pätnástimi rokmi, a to prostredníctvom Spoločnej pozície 1999/364/SVV o rokovaniach uskutočnených v rámci Rady Európy, ktoré sa týkajú návrhu Dohovoru o počítačovej kriminalite. Na základe tejto Spoločnej pozície členské štáty EÚ mali podporiť vypracovanie návrhu Dohovoru Rady Európy o počítačovej kriminalite a mali sa zasadzovať o zahrnutie ustanovení do Dohovoru, ktoré uľahčia efektívne vyšetrovanie a stíhanie trestných činov spojených s počítačovými systémami a údajmi,[259] a

b) **smernica Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy**, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV. Cieľom smernice je **aproximácia trestného práva členských štátov v oblasti útokov na informačné systémy ustanovením minimálnych pravidiel týkajúcich sa vymedzenia trestných činov a príslušných sankcií**, ako aj zlepšenie spolupráce medzi príslušnými orgánmi vrátane policajných a iných špecializovaných orgánov presadzovania práva v členských štátoch a príslušných špecializovaných agentúr a orgánov Únie, akými sú Eurojust, Europol a jeho Európske centrum pre počítačovú kriminalitu,[260] či Európska agentúra pre bezpečnosť sietí a informácií (ENISA).[261]

Práve smernica Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV je veľmi významnou z pohľadu národného právneho poriadku. Táto **smernica bola transponovaná do**

---

[258] ZÁHORA, J. Aktuálne trendy v postihu počítačovej kriminality v Slovenskej republike. *In Justičná revue, 68, 2016, č. 3*, s. 325-326.

[259] KLIMEK, L. Boj proti útokom na informačné systémy na úrovni Európskej únie. *In Justičná revue, 68, 2016, č. 2*, s. 185 a nasl.

[260] Hlavnou úlohou Európskeho centra boja proti počítačovej kriminalite je narušiť operácie sietí organizovaného zločinu, ktoré páchajú veľký podiel závažných a organizovaných počítačových trestných činov. Patria sem trestné činy vytvárajúce veľké zisky, ktoré spôsobujú vážnu škodu ich obetiam, alebo tie trestné činy, ktoré ovplyvňujú našu životne dôležitú infraštruktúru a IT systémy. Ide napríklad o podvod v oblasti platobného styku, kybernetické útoky na informačné systémy, alebo sexuálne vykorisťovanie detí online (napríklad vedomé získavanie prístupu k detskej pornografii pomocou informačných a komunikačných technológií); KLIMEK, L. Európske centrum boja proti počítačovej kriminalite. *In Justičná revue, 67, 2015, č. 8-9*, s. 1032.

[261] BENEDEKOVÁ, D. In MARKOVÁ, V. (ed.) *Aktuálne otázky trestného práva v teórii a praxi.* Bratislava : Akadémia Policajného zboru v Bratislave, 2016, s. 21-22.

Trestného zákona jeho novelou z konca roka 2015, keď prijala Národná rada Slovenskej republiky zákon č. 398/2015 Z. z. o európskom ochrannom príkaze v trestných veciach a o zmene a doplnení niektorých zákonov, ktorý je účinný od 1. januára 2016. Z hľadiska zmien Trestného zákona prináša tento zákon **úplne novú úpravu počítačovej kriminality** vzhľadom na to, že sa nanovo definujú skutkové podstaty trestných činov neoprávneného prístupu do počítačového systému, neoprávneného zásahu do počítačového systému, neoprávneného zásahu do počítačového údaja, neoprávneného zachytávania počítačových údajov a trestný čin výroby a držby prístupového zariadenia, hesla do počítačového systému alebo iných údajov.[262]

Konkrétne sa táto smernica dotkla týchto ustanovení:

a) § 247 neoprávnený prístup do počítačového systému,[263]

b) § 247a neoprávnený zásah do počítačového systému,[264]

c) § 247b neoprávnený zásah do počítačového údaja,[265]

d) § 247c neoprávnené zachytávanie počítačových údajov,[266]

e) § 247d výroba a držba prístupového zariadenia, hesla do počítačového systému alebo iných údajov.[267]

Ad a) Objektom trestného činu je **ochrana počítačového systému ako celku alebo** ktorejkoľvek **jeho časti** (jeho obsah vrátane technického a programového vybavenia). Na trestnosť páchateľa bude stačiť, ak prekoná bezpečnostné opatrenia a tým získa neoprávnený prístup do počítačového systému (jeho časti), pričom sa nevyžaduje spôsobenie škody. Získaním neoprávneného prístupu do počítačového systému je akékoľvek konanie, ktoré páchateľovi umožní neoprávnenú dispozíciu počítačovým systémom, resp. jeho časťou a využitie jeho informačného obsahu.[268]

---

[262] Tamtiež, s. 22.

[263] Kto prekoná bezpečnostné opatrenie, a tým získa neoprávnený prístup do počítačového systému alebo jeho časti, potrestá sa odňatím slobody až na dva roky.

[264] Kto obmedzí alebo preruší fungovanie počítačového systému alebo jeho časti
a) neoprávneným vkladaním, prenášaním, poškodením, vymazaním, zhoršením kvality, pozmenením, potlačením alebo zneprístupnením počítačových údajov, alebo
b) tým, že urobí neoprávnený zásah do technického alebo programového vybavenia počítača a získané informácie neoprávnene zničí, poškodí, vymaže, pozmení alebo zníži ich kvalitu, potrestá sa odňatím slobody na šesť mesiacov až tri roky.

[265] Kto úmyselne poškodí, vymaže, pozmení, potlačí alebo zneprístupní počítačové údaje alebo zhorší ich kvalitu v rámci počítačového systému alebo jeho časti, potrestá sa odňatím slobody na šesť mesiacov až tri roky.

[266] Kto neoprávnene zachytáva počítačové údaje prostredníctvom technických prostriedkov neverejných prenosov počítačových údajov do počítačového systému, z neho alebo v jeho rámci vrátane elektromagnetických emisií z počítačového systému, ktorý obsahuje takéto počítačové údaje, potrestá sa odňatím slobody na šesť mesiacov až tri roky.

[267] Kto v úmysle spáchať trestný čin neoprávneného prístupu do počítačového systému podľa § 247, neoprávneného zásahu do počítačového systému podľa § 247a, neoprávneného zásahu do počítačového údaja podľa § 247b alebo neoprávneného zachytávania počítačových údajov podľa § 247c vyrobí, dovezie, obstará, kúpi, predá, vymení, uvedie do obehu alebo akokoľvek sprístupní
a) zariadenie vrátane počítačového programu vytvorené na neoprávnený prístup do počítačového systému alebo jeho časti, alebo
b) počítačové heslo, prístupový kód alebo podobné údaje umožňujúce prístup do počítačového systému alebo jeho časti, potrestá sa odňatím slobody až na dva roky.

[268] Komentár k § 247 Trestného zákona. Dostupné v systéme ASPI.

Z hľadiska subjektívnej stránky sa na spáchanie tohto trestného činu vyžaduje **úmyselné** zavinenie. Trestný čin neoprávneného prístupu do počítačového systému je vo svojej základnej skutkovej podstate **prečinom** (trest odňatia slobody až na dva roky) a vo svojej najprísnejšej kvalifikovanej skutkovej podstate (odsek 3) zločinom (trest odňatia slobody na tri roky až osem rokov).

Ad b) Objektom takto charakterizovaného trestného činu je najmä **ochrana počítačového systému ako celku alebo jeho časti pred neoprávneným zásahom**, ktorý je, vzhľadom na široké spektrum možných negatívnych aspektov, neakceptovateľný; rovnako tak dôvernosť počítačových údajov, ich integrita a dostupnosť. Chránený je hmotný substrát (hardvér), ale aj nehmotný obsah informácií pred zneužitím, zničením, zhoršením kvality, zneprístupnením a pod. Tým sa chránia prejavy osobnej povahy, obchodné tajomstvo, súkromie, autorské právo, údaje o pacientoch, zaknihovaných cenných papieroch, či utajovaných skutočnostiach.[269]

Z hľadiska subjektívnej stránky sa na spáchanie tohto trestného činu vyžaduje **úmyselné** zavinenie. Trestný čin neoprávneného zásahu do počítačového systému je vo svojej základnej skutkovej podstate **prečinom** (trest odňatia slobody na šesť mesiacov až tri roky) a vo svojej najprísnejšej kvalifikovanej skutkovej podstate (odsek 3) zločinom (trest odňatia slobody na štyri roky až desať rokov).

Ad c) Individuálnym objektom tohto trestného činu je **ochrana tajomstva informácie prenášanej prostredníctvom elektronickej komunikačnej služby**, alebo tajomstva neverejného prenosu počítačových dát do počítačového systému, z neho alebo v jeho rámci. Na účely transpozície smernice sa neoprávneným zachytávaním rozumie odpočúvanie a monitorovanie obsahu komunikácie alebo jej sledovanie resp. získavanie obsahu údajov buď priamo, prostredníctvom prístupu a využívania informačného systému, alebo nepriamo, prostredníctvom využívania elektronického odpočúvania alebo odpočúvacieho zariadenia technickými prostriedkami.[270]

Z hľadiska subjektívnej stránky sa na spáchanie tohto trestného činu vyžaduje **úmyselné** zavinenie. Trestný čin neoprávneného zásahu do počítačového údaju je vo svojej základnej skutkovej podstate **prečinom** (trest odňatia slobody na šesť mesiacov až tri roky) a vo svojej najprísnejšej kvalifikovanej skutkovej podstate (odsek 3) zločinom (trest odňatia slobody na štyri roky až desať rokov).

---

[269] ZÁHORA, J. Aktuálne trendy v postihu počítačovej kriminality v Slovenskej republike. *In Justičná revue, 68, 2016, č. 3*, s. 328.

[270] BENEDEKOVÁ, D. In MARKOVÁ, V. (ed.) *Aktuálne otázky trestného práva v teórii a praxi.* Bratislava : Akadémia Policajného zboru v Bratislave, 2016, s. 25.

Ad d) Individuálnym objektom tohto trestného činu je **ochrana tajomstva informácie prenášanej prostredníctvom elektronickej komunikačnej služby**, alebo tajomstva neverejného prenosu počítačových dát do počítačového systému, z neho alebo v jeho rámci. Na účely transpozície smernice sa neoprávneným zachytávaním rozumie odpočúvanie a monitorovanie obsahu komunikácie alebo jej sledovanie resp. získavanie obsahu údajov buď priamo, prostredníctvom prístupu a využívania informačného systému, alebo nepriamo, prostredníctvom využívania elektronického odpočúvania alebo odpočúvacieho zariadenia technickými prostriedkami.[271]

Z hľadiska subjektívnej stránky sa na spáchanie tohto trestného činu vyžaduje **úmyselné** zavinenie. Trestný čin neoprávneného zachytávania počítačových údajov je vo svojej základnej skutkovej podstate **prečinom** (trest odňatia slobody na šesť mesiacov až tri roky) a vo svojej najprísnejšej kvalifikovanej skutkovej podstate (odsek 3) zločinom (trest odňatia slobody na štyri roky až desať rokov).

Ad e) Objektom, v zmysle tohto trestného činu, je najmä **ochrana pred možným ohrozením vyplývajúcim z nekontrolovanej distribúcie prostriedkov slúžiacich na nedovolené zásahy do počítačových systémov**. Sekundárne sa tu chráni aj integrita počítačového systému ako celku alebo jeho časti pred neoprávneným zásahom, ktorý je vzhľadom na široké spektrum možných negatívnych aspektov neakceptovateľný, ďalej to môže byť dôvernosť počítačových údajov, ich integrita, dostupnosť a ochrana prejavov osobnej povahy, napríklad súkromia, obchodného tajomstva a autorského práva.[272]

Z hľadiska subjektívnej stránky sa na spáchanie tohto trestného činu vyžaduje **úmyselné** zavinenie. Trestný čin výroby a držby prístupového zariadenia, hesla do počítačového systému alebo iných údajov je **prečinom** (trest odňatia slobody na šesť mesiacov až tri roky) a vo svojej najprísnejšej kvalifikovanej skutkovej podstate (odsek 4) zločinom (trest odňatia slobody na štyri roky až desať rokov).

Pre úplnosť uvediem, že tieto trestné činy **môže spáchať aj právnická osoba**, čo vyplýva z § 3 zákona č. 91/2016 Z. z. o trestnej zodpovednosti právnických osôb.[273]

3.5 Správnoprávna zodpovednosť

Vo vzťahu k prejednávanej problematike má z pohľadu správnoprávnej zodpovednosti veľký **význam najmä zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti** (ďalej len „ZoKB"). Vzhľadom

[271] Tamtiež, s. 25.
[272] ZÁHORA, J. Aktuálne trendy v postihu počítačovej kriminality v Slovenskej republike. *In Justičná revue, 68, 2016, č. 3*, s. 329.
[273] K tomu pozri najmä BURDA, E. In BURDA, E., KORDÍK, M., KURILOVSKÁ, L., STRÉMY, T. a kol. *Zákon o trestnej zodpovednosti právnických osôb. Komentá*r. Bratislava : C. H. Beck, 2018, s. 76 a nasl.

na to, že právna úprava priestupkov je vo všeobecnej rovine predmetom zákona o priestupkoch a vzhľadom na priestor, ktorý môže byť daný tejto kapitole, odkazujem na odbornú literatúru venujúcu sa tomuto zákonu.[274] V tejto podkapitole sa budeme venovať len **odlišnostiam zakotveným v ZoKB oproti všeobecnej právnej úprave**.

Z hľadiska správnych deliktov upravuje ZoKB **priestupky a (iné) správne delikty**. Tie sú upravené v § 30 a § 31 ZoKB.

ZoKB upravuje **priestupky** v § 30. Osobitne sa tu vymedzujú:

a. skutkové podstaty priestupkov,
b. pokuty za ich spáchanie a
c. vecná príslušnosť na prejednanie priestupku.

Vo zvyšku sa na konanie o priestupku použije zákon o priestupkoch.[275]

V § 30 ods. 1 zákonodarca vymedzuje **v piatich písmenách skutkové podstaty priestupkov, ktoré možno spáchať na úseku kybernetickej bezpečnosti**. Ako **subjekt** týchto priestupkov zákon vymedzuje **fyzickú osobu**. Hneď na úvod treba povedať, že nepôjde o fyzickú osobu ktorúkoľvek, ktorá je priestupkovo zodpovedná,[276] ale ide o fyzickú osoba, ktorá okrem toho bude musieť splniť ďalšie podmienky (tzv. špeciálny subjekt), ktoré však zo ZoKB vyplývajú len nepriamo, a to priamo z textu konkrétnej skutkovej podstaty zachytenej v jednotlivých písmenách.

V písmene a) sa **chráni povinnosť mlčanlivosti**, ktorá súvisí so zachovaním kybernetickej bezpečnosti. Pri naplnení objektívnej stránky dochádza k tomu, že táto mlčanlivosť bola porušená a mohlo dôjsť k vyzradeniu skutočností, ktorými môže dôjsť k narušeniu kybernetickej bezpečnosti. Je právne irelevantné, akým spôsobom došlo k porušeniu mlčanlivosti, dôležité je, že mlčanlivosť nebola zachovaná. Rovnako tak je právne irelevantné, či došlo k ohrozeniu alebo až porušeniu kybernetickej bezpečnosti, naplnenie tohto dôsledku zákon nevyžaduje.

K naplneniu skutkovej podstaty nemôže dôjsť, ak boli vyzradené skutočnosti, ktoré už boli verejne známe.

Ak som hovoril, že nie každá priestupkovo zodpovedná osoba podľa zákona o priestupkoch bude zodpovedná aj podľa ZoKB, tak môžeme si uvedené ilustrovať práve na príklade písmena a). Priestupkovo zodpovednou bude v tomto prípade len osoba, ktorá je v pracovnoprávnom vzťahu alebo vzťahu obdobnom pracovnému vzťahu vrátane služobného pomeru k NBÚ alebo má uzatvorenú dohodu o spolupráci s NBÚ (pozri § 12 ods. 1 ZoKB). Z daného dôvodu musí NBÚ pri

[274] SREBALOVÁ, M. a kol. *Zákon o priestupkoch. Komentár.* Bratislava : Wolters Kluwer, 2015, 484 s.; POTASCH, P. a kol. *Zákon o priestupkoch. Veľký komentár*. Bratislava : Eurokódex, 2016, 408 s.; SPIŠIAKOVÁ, H. *Zákon o priestupkoch. Komentár.* Bratislava : Wolters Kluwer, 2015, 816 s.

[275] ZoKB v § 30 ods. 3 a 5 ešte upravuje, že na priestupky a ich prejednávanie sa vzťahuje všeobecný predpis o priestupkoch a že príjem z pokút je príjmom štátneho rozpočtu; tieto ustanovenia sú z legislatívno-technického hľadiska nadbytočné, pretože vyplývajú priamo aj zo zákona o priestupkoch (porovnaj § 2 ods. 1, § 13 ods. 3 a § 51 zákona o priestupkoch).

[276] T. j. fyzická osoba, ktorá v čase spáchania priestupku dovŕšila 15 rok veku a bola príčetná (§ 5 zákona o priestupkoch).

vyvodzovaní zodpovednosti skúmať, či tu tento vzťah existuje alebo existoval; podľa ZoKB totiž táto mlčanlivosť ostáva zachovaná aj po ukončení daného vzťahu.

Nositeľmi tejto povinnosti preto budú najmä **zamestnanci NBÚ,** resp. pracovníci kontroly, ako aj zamestnanci kontrolovaných subjektov, prevádzkovateľov základných služieb a prevádzkovateľov digitálnych služieb.[277] Okrem toho táto povinnosť dopadá aj na toho, kto uzatvoril s NBÚ písomnú dohodu o spolupráci (§ 5 ods. 2 ZoKB).

Priestupky vymedzené v písmene b) až d) vymedzujú **odkazovou formou porušenia ktorých konkrétnych povinností podľa ZoKB sú považované za protiprávne v podobe priestupku.** Vo všetkých prípadoch platí, že **subjektom** tohto deliktu je **prevádzkovateľ (základnej) služby**. Problematickým sa javí najmú tá skutočnosť, že tento subjekt bude zodpovedať podľa tohto ustanovenia len vtedy, ak bude prevádzkovateľom v podobe fyzickej osoby a nie právnickej osoby (čo zrejme v praxi často nenastane). Výklad tohto ustanovenia potom môže viesť aj k tomu, že zodpovedať bude konkrétna fyzická osoba (zrejme zamestnanec prevádzkovateľa), ktorá bola v mene prevádzkovateľa povinná zabezpečovať plnenie daných povinností. Zistenie **páchateľa** v tomto prípade môže **preto v praxi byť celkom 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 zákonu.[278]

V písmene e) zákon potom presne špecifikuje skutkovú podstatu, a to tak, že zodpovednou bude tá osoba, ktorá **nepostupovala v súlade s technickými, organizačnými alebo personálnymi opatreniami prijatými prevádzkovateľom základnej služby**. Predpokladom je tu prijatie týchto opatrení (pozri § 20 ods. 1 ZoKB). Ak by neboli prijaté, nemožno spáchať tento priestupok. Opäť ide o priestupok, kde subjektom bude najmä zamestnanec prevádzkovateľa základnej služby.

Z logiky veci vyplýva, že **vecne príslušným** na prejednanie daných priestupkov bude **Národný bezpečnostný úrad**. Tento úrad môže páchateľovi uložiť pokutu, a to v **minimálnej výške 100 eur a v maximálnej 5 000 eur**. 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.

Vzhľadom na subsidiárne použitie zákona o priestupkoch možno 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.

---

[277] GÁBRIŠ, T. In ANDRAŠKO, J., GÁBRIŠ, T., HOCHMANN, J., OLEJÁR, D. *Zákon o kybernetickej bezpečnosti. Komentár.* Bratislava : Wolters Kluwer, 2018, s. 365.

[278] Pozri ANDRAŠKO, J., GÁBRIŠ, T., HOCHMANN, J., OLEJÁR, D. *Zákon o kybernetickej bezpečnosti. Komentár.* Bratislava : Wolters Kluwer, 2018, s. 490.

Zákon o priestupkoch umožňuje ďalej uložiť aj sankciu zákazu činnosti a pokarhania. Zákaz činnosti uložiť nemožno, pretože by to musel ZoKB priamo pripúšťať, čo sa však v texte zákona neuskutočnilo (porovnaj znenie § 14 ods. 1 zákona o priestupkoch). Pokarhanie taktiež nemožno uložiť, a to z toho dôvodu, prečo nemožno zároveň uložiť pokutu (porovnaj tú skutočnosť, že zákon ustanovuje dolnú sadzbu pokuty; t. j. NBÚ bude pokutu ukladať povinne vždy) a pokarhanie (porovnaj znenie § 11 ods. 1 veta za bodkočiarkou zákona o priestupkoch).

ZoKB upravuje **správne delikty v § 31**. Hoci to z názvu ustanovenia nevyplýva, tak **svojou povahou ide o druh správneho deliktu, ktorý sa nazýva správny delikt právnickej osoby a podnikajúcej fyzickej osoby, prípadne (ak to okolnosti pripustia), iný správny delikt fyzickej osoby.** V praxi však ako subjekt deliktu budú vystupovať primárne právnické osoby (to platí aj v prípade odseku 5).

Konkrétne skutkové podstaty jednotlivých správnych deliktov sú vymedzené v piatich odsekoch. **Subjektom** správneho deliktu podľa odseku 1 a 2 je **prevádzkovateľ základnej služby**. Subjektom správneho deliktu podľa **poskytovateľ digitálnej služby**. Subjektom podľa odseku 5 sú v spojení s § 7 ods. 3 ZoKB **ústredné orgány a iné orgány štátnej správy.**[279,280]

Z pohľadu právnej istoty možno pozitívne vnímať, že **všetky skutkové podstaty, ktoré sú tu upravené, sú upravené odkazovou metódou**. Vždy je preto jasné, porušenie ktorého ustanovenia so sebou nesie riziko spáchania správneho deliktu. Vo všetkých prípadoch **ide o porušovacie delikty**, t. j. ak dôjde len k ohrozeniu objektu chráneného skutkovo podstatou, tak ešte nemožno hovoriť o dokonaní správneho deliktu.

V odseku 1 a 2 sú upravené delikty, **ktorých subjektom je prevádzkovať základnej služby.** Pri analýze týchto ustanovení vo vzťahu k § 30 ZoKB možno dospieť k záveru, že ak by porušila tieto povinnosti fyzická osoba, dopustila by sa priestupku a ak osoba právnická, tak správneho deliktu podľa § 31. O dvojitom postihu (*ne bis in idem*) v tomto prípade nemožno hovoriť, keďže sú tu rozdielne subjekty. Postihnúť preto možno súbežne oba subjekty. Správny orgán preto nemôže ani len uskutočniť spoločné konanie o týchto deliktoch, ale vo veci musia riadne prebehnúť dve konania. Zákon ustanovuje za spáchanie daného deliktu **minimálnu spodnú sadzbu** pokuty vo výške 300 eur. **Maximálna výška pokuty** je v prípade odseku 1 30 000 eur a v prípade odseku 2 do výšky 1 % celkového ročného obratu za predchádzajúci účtovný rok najviac však 300 000 eur.

Vecne príslušným orgánom na prejednanie správneho deliktu je **Národný bezpečnostný úrad.**

---

[279] Tieto pojmy sú na účely ZoKB ponímané odlišne, než sa vymedzuje v právnej teórii. Vyplýva to z definície týchto pojmov na účely ZoKB, ktoré nachádzame v § 4 písm. b) a c).

[280] K teoretickému vymedzeniu pojmu ústredný orgán štátnej správy a iný orgán štátnej správy pozri HORVAT, M. *In CEPEK, B. a kol. Správne právo hmotné. Všeobecná časť. Bratislava : Wolters Kluwer, 2018*, s. 153 a nasl.

Subjektom správnych deliktov vymedzených v odseku 3 a 4 je **poskytovateľ digitálnych služieb.** Aj v tomto prípade sú jednotlivé skutkové podstaty postavené do roviny odkazovacích noriem, kde vymedzujú presne porušenie ktorých povinností so sebou nesie riziko spáchania správneho deliktu. Aj v tomto prípade je výška pokuty vymedzené **minimálnou sadzbou** 300 eur (odseky 3 aj 4) a **maximálnou výškou** 30 000 eur (odsek 3), resp. do výšky 1 % celkového ročného obratu za predchádzajúci účtovný rok najviac však 300 000 eur.

Vecne príslušným orgánom na prejednanie správneho deliktu je **Národný bezpečnostný úrad.**

Národný bezpečnostný úrad je vecne príslušným aj na prejednanie posledného správneho deliktu zachytenému v § 31, a to v odseku 5. Subjektom tohto deliktu sú **ústredné orgány[281] a iné orgány štátnej správy[282]** tak, ako sú vymedzené v § 4 ZoKB. Hoci by sa mohlo zdať, že subjektom bude v tomto prípade ktokoľvek (porovnaj formuláciu „tomu, kto na výzvu"), nie je to tak. Povinnými subjektmi na poskytnutie informácie sú iba spomínané ústredné orgán a iné štátne orgány, ako sú vymedzené v § 7 ods. 3 v spojení s § 4 písm. b) a c) ZoKB.

Pokuta v tomto prípade hrozí vo výške od 300 eur do 100 000 eur.

Zákonodarca v rozoberanom ustanovení rieši **aj otázku prípadnej recidívy.** Recidíva je vo všeobecnosti závažným protispoločenským javom, pretože páchateľ po rozhodnutí, ktorým bol uznaný za vinného a bola mu uložená pokuta, opätovne spáchal protiprávny čin. Dá sa preto povedať, že došlo tu k zlyhaniu, pretože pôvodne uložená pokuta nesplnila svoj represívny a ani prevenčný charakter – neodradila páchateľa od páchania ďalšej protiprávnej činnosti.

Reakciou preto v tomto prípade je sprísnenie pokút, ktoré môže NBÚ ukladať. Podľa odseku 7 sa v tomto prípade sadzby pokút zvyšujú o polovicu. Dolná sadzba je vo všetkých prípadoch 600 eur. Horná sadzba v prípade odsekov 1 a 3 najviac 60 000 eur, v prípade odseku 5 maximálne 200 000 eur a v prípade odsekov 2 a 4 do výšky 2 % celkového ročného obratu za predchádzajúci účtovný rok najviac však 600 000 eur.

Za recidívu sa podľa zákona **však považuje len spáchanie toho istého deliktu porušením tej istej povinnosti,** t. j. ak napríklad páchateľ spáchal deliktu podľa § 31 ods. 3, a to tým, že porušil povinnosť podľa § 21 ods. 5, o recidívu pôjde len vtedy, ak opätovne poruší povinnosť podľa § 21

[281] Národný bezpečnostný 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.
[282] 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 reguláciu sieťových odvetví a iné štátne orgány v rozsahu svojej pôsobnosti.

ods. 5 a nie povinnosť podľa § 22 ods. 4 alebo § 23 ods. 2, a to aj napriek tomu, že sú vymedzené v jednej skutkovej podstate (spomenutý § 31 ods. 3 ZoKB).

Rovnako treba povedať, že za **recidívu sa považuje len situácia, ak porušeniu tejto povinnosti došlo v dobe jedného roka od nadobudnutia právoplatnosti rozhodnutia o uložení pokuty.** 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.

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.** Táto právna norma je mimoriadne dôležitá, pretože posilňuje dôveru v právny štát a zamedzuje svojvôli v rozhodovaní úradu. Ten totiž musí na základe týchto kritérií páchateľovi vysvetliť, prečo mu uložil pokutu a prečo práve v tej výške, ktorá je uvedené v odôvodnení rozhodnutia. Zdôvodnenie výšky pokuty sa vykonáva v časti rozhodnutia o uložení pokuty, ktoré sa nazýva odôvodnenie.

Podľa súdnej judikatúry zákonom ustanovená povinnosť orgánov verejnej moci dbať na splnenie zákonných náležitostí samotného výroku rozhodnutia, ako aj jeho odôvodnenia (vrátane zistenia skutkového stavu a jeho hodnotenia v dostatočnom rozsahu) predstavuje nielen jednu zo základných podmienok na zákonu zodpovedajúce rozhodnutie, ale je tiež jedným zo základných znakov ústavou garantovaného postupu podľa čl. 46 ods. 1 Ústavy Slovenskej republiky a ochrany práv účastníkov konania. **Odôvodnenie rozhodnutia správneho orgánu musí v zmysle naplnenia tejto požiadavky obsahovať relevantné a dostatočné dôvody, na základe ktorých bolo vydané.** Rozsah tejto povinnosti sa môže meniť podľa povahy rozhodnutia a musí sa posúdiť vo svetle okolností každej veci.[283]

V prípade správneho trestania súd sleduje, či správny orgán náležite zdôvodnil uloženie sankcie v určitej výške, ak zákon pripúšťa rozpätie sankcie, prihliadol na okolnosti viazané na subjekt, samotný skutok a jeho následok. (...) **Určenie výšky pokuty v rámci určitého rozpätia je síce vecou voľného uváženia, to však neznamená, 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. Pri uložení pokuty správny orgán prihliadne na závažnosť, spôsob i čas trvania následkov protiprávneho konania.[284]

[283] Rozsudok Najvyššieho súdu Slovenskej republiky z 25. januára 2018 sp. zn. 8Sžo/116/2015.
[284] Rozsudok Najvyššieho súdu Slovenskej republiky z 19. apríla 2017, sp. zn. 10Sžo/40/2016.

ZoKB v časti o iných správnych deliktoch ustanovuje aj **lehotu na vyvodenie zodpovednosti**.[285] Na rozdiel od priestupkov, kde je formulované len lehota objektívna, je v prípade ZoKB lehota vybudovaná ako kombinácia lehoty objektívnej a subjektívnej.[286] Asi najdôležitejším poznatkom vo vzťahu k týmto lehotám je, že plynutie subjektívnej lehoty je možné len v rámci lehoty objektívnej; subjektívna lehota nemôže nikdy „predbehnúť" lehotu objektívnu.

Podľa ZoKB je **subjektívna** lehota vymedzená ako **dvojročná**. Táto lehota sa počíta od subjektívneho okamihu, ktorým je zistenie NBÚ, že došlo k porušeniu povinnosti.

Objektívna lehota je ustanovená ako **štvorročná**. 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.

V týchto lehotách musí **rozhodnutie** o vine a uloženej pokute **aj nadobudnúť právoplatnosť**, nepostačuje, že sa konanie začalo alebo že bolo rozhodnutie len vydané v tejto lehote.

Uložená pokuta je splatná do 30 dní od nadobudnutia právoplatnosti rozhodnutia vo veci samej, pričom **splatená pokuta je príjmom štátneho rozpočtu**.

Z dôvodu právnej istoty ešte zákonodarca upravuje v zákone aj pojem „celkový ročný obrat" a „predchádzajúce účtovné obdobie". Tieto pojmy sú vymedzené len na účely tohto zákona, nemajú preto záväzný charakter pre iné oblasti práva. Zákonodarca ich vymedzuje z toho dôvodu, aby posilnil právnu istotu pri výpočte sadzieb pokút v § 30 ods. 2 a 4 ZoKB a kde sú tieto pojmy využité.

ZOZNAM POUŽITEJ LITERATÚRY

1) ANDRAŠKO, J., GÁBRIŠ, T., HOCHMANN, J., OLEJÁR, D. Zákon o kybernetickej bezpečnosti. Bratislava : Wolters Kluwer, 2018,

2) BOGUSZAK, J., ČAPEK, J., GERLOCH, A. Teorie práva. Praha : Eurolex Bohemia, 2001,

3) BRÖSTL, A. a kol. Teória práva. Plzeň : Aleš Čeněk, 2013,

4) BURDA, E., KORDÍK, M., KURILOVSKÁ, L., STRÉMY, T. a kol. Zákon o trestnej zodpovednosti právnických osôb. Komentár. Bratislava : C. H. Beck, 2018,

5) CEPEK, B. a kol. Správne právo hmotné. Všeobecná časť. Bratislava : Wolters Kluwer, 2018,

6) DRGONEC, J. Ústava Slovenskej republiky. Komentár. Šamorín : Heuréka, 2007,

7) FÁBRY, B., KASINEC, R., TURČAN, M. Teória práva. Bratislava : Wolters Kluwer, 2019,

8) FIALA, Z., HORZINKOVÁ, E. In FIALA, Z., FRUMAROVÁ, K., HORZINKOVÁ, E., ŠKUREK, M. a kol. Správní právo trestní. Praha : Leges, 2017,

9) GERLOCH, A. Teorie práva. Plzeň : Aleš Čeněk, 2013,

[285] V prípade priestupkov sa uplatní všeobecná úprava podľa § 20 ods. 1 zákona o priestupkoch.
[286] K členeniu lehôt pozri SREBALOVÁ, M., HORVAT, M. *In Všeobecné správne konanie. Bratislava : PraF UK, 2009*, s. 129 a nasl.

10) HARVÁNEK, J. a kol. Teorie práva. Plzeň : Aleš Čeněk, 2008,

11) HORVAT, M. a kol. Živnostenský zákon. Komentár. Bratislava : Wolters Kluwer, 2019,

12) IVOR, J. a kol. Trestné právo procesné. Bratislava : Iura Edition, 2010,

13) KLIMEK, L. Boj proti útokom na informačné systémy na úrovni Európskej únie. In Justičná revue, 68, 2016, č. 2,

14) KLIMEK, L. Európske centrum boja proti počítačovej kriminalite. In Justičná revue, 67, 2015, č. 8-9,

15) KNAPP, V. Teorie práva. Praha : C. H. Beck, 1995,

16) KOŠIČIAROVÁ, S. Princípy dobrej verejnej správy a Rada Európy. Bratislava : Iura Edition, 2012,

17) KOŠIČIAROVÁ, S. Verejná správa a právo na spravodlivý proces. Krakov : Spolok Slovákov v Poľsku, 2014,

18) KOŠIČIAROVÁ, S. Zákon o obecnom zriadení. Bratislava : Eurokódex, 2018,

19) LUBY, Š. Výber z diel a myšlienok. Bratislava : Iura Edition, 1998,

20) MACHAJOVÁ, J. a kol. Všeobecné správne právo. Žilina : Eurokódex, 2009,

21) MARKOVÁ, V. (ed.) Aktuálne otázky trestného práva v teórii a praxi. Bratislava : Akadémia Policajného zboru v Bratislave, 2016,

22) MENCEROVÁ, I., TOBIÁŠOVÁ, L., TURAYOVÁ, Y. a kol. Trestné právo hmotné. Všeobecná časť. Šamorín : Heuréka, 2013,

23) MUSIL, J., KRATOCHVÍL, V., ŠÁMAL, P. a kol. Trestní právo procesní. Praha : C. H. Beck, 2007,

24) OTTOVÁ, E. Teória práva. Bratislava : VO PraF UK, 2004,

25) POTASCH, P. a kol. Zákon o priestupkoch. Veľký komentár. Bratislava : Eurokódex, 2016,

26) PRÁŠKOVÁ, H. Základy odpovědnosti za správní delikty. Praha : C. H. Beck, 2013,

27) PRUSÁK, J. Teória práva. Bratislava : VO PraF UK, 1995,

28) SPIŠIAKOVÁ, H. Zákon o priestupkoch. Komentár. Bratislava : Wolters Kluwer, 2015,

29) SREBALOVÁ, M. a kol. Zákon o priestupkoch. Komentár. Bratislava : C. H. Beck, 2015,

30) STRÉMY, T. In MAŠĽANYOVÁ, D. a kol. Trestné právo hmotné. Plzeň : Aleš Čeněk, 2011,

31) ŠÁMAL, P., BAXA, J. In ŠÁMAL, P., MUSIL, J., KUCHTA, J. a kol. Trestní právo procesní. Praha : C. H. Beck, 2013,

32) VEČEŘA, M. a kol. Teória práva. Bratislava : Eurokódex, 2009,

33) VEVERKA, V., BOGUSZAK, J., ČAPEK, J. Základy teorie práva a právní filozofie. Praha : Nakladatelství CODEX, 1996,

34) VRABKO, M. a kol. Správne právo hmotné. Všeobecná časť. Bratislava : C. H. Beck, 2012,

35) VRABKO, M. a kol. Správne právo hmotné. Všeobecná časť. Bratislava : C. H. Beck, 2018,

36) VRABKO, M. a kol. Správne právo procesné. Všeobecná časť. Bratislava : C. H. Beck, 2013,

37) ZÁHORA, J. Aktuálne trendy v postihu počítačovej kriminality v Slovenskej republike. In Justičná revue, 68, 2016, č. 3,

38) ZOUBEK, V. Právověda a státověda. Úvod do právního a státovědního myšlení. Plzeň : Aleš Čeněk, 2010.

ISBN: 978-80-7160-539-3