učebnica

REGULÁCIA KYBERNETICKEJ BEZPEČNOSTI, OCHRANY SÚKROMIA A KYBERNETICKEJ KRIMINALITY

Andraško, Dražová, Kordík, Mesarčík, Rampášek a kol.

CUSEC
Kompetenčné centrum pre reguláciu kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality

PRÁVNICKÁ FAKULTA
Univerzita Komenského v Bratislave

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

REGULÁCIA KYBERNETICKEJ BEZPEČNOSTI, OCHRANY SÚKROMIA A KYBERNETICKEJ KRIMINALITY

Učebnica

Andraško, Dražová, Kordík, Mesarčík, Rampášek
a kol.

Vzor citácie: Regulácia kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality. Andraško, Jozef – Dražová, Petra – Kordík, Marek – Mesarčík, Matúš – Rampášek, Michal. a kol. 1. vyd. – Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2026, 638 s.

Rok vydania: 2026

Prvé vydanie

Recenzenti: doc. JUDr. Regina Hučková, PhD. (Právnická fakulta, Univerzita Pavla Jozefa Šafárika v Košiciach)
doc. RNDr. JUDr. Pavol Sokol, PhD. et PhD. (Prírodovedecká fakulta, Univerzita Pavla Jozefa Šafárika v Košiciach)

Vydala Právnická fakulta Univerzity Komenského v Bratislave v roku 2026.

ISBN (e-verzia): 978 – 80 – 7160 – 798 – 4

Táto učebnica je výstupom z projektu „Kompetenčné centrum pre reguláciu kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality" financovaného Európskou úniou NextGenerationEU prostredníctvom Plánu obnovy a odolnosti SR v rámci projektu pod číslom 17R05-04-V01-00002.

Viac informácii o projekte nájdete na: https://cusec.flaw.uniba.sk/

O AUTOROCH

Doc. JUDr. Jozef Andraško, PhD. je docentom a riaditeľom Ústavu práva informačných technológií a práva duševného vlastníctva na Právnickej fakulte Univerzity Komenského v Bratislave. Vo svojej pedagogickej a výskumnej činnosti sa zameriava na problematiku kybernetickej bezpečnosti, otvorených údajov a automatizovaných vozidiel. Je spoluautorom prvého komentára k zákonu o kybernetickej bezpečnosti, ako aj viacerých monografií a vedeckých článkov publikovaných v časopisoch indexovaných v databázach WoS a SCOPUS. Pripomienkoval viacero návrhov právnych predpisov v oblasti kybernetickej bezpečnosti, pripravoval návrhy všeobecne záväzných právnych predpisov a zúčastňoval sa aj na rozporových konaniach. Má skúsenosti s realizáciou viacerých medzinárodných aj národných projektov v oblasti práva informačných technológií. Je garantom Kompetenčného centra pre reguláciu kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality (CUSEC). Absolvoval zahraničné výskumné pobyty na Tallinn University of Technology Law School (Estónsko) a Marquette University Law School (Milwaukee, USA).

Doc. JUDr. Katarína Burdová, PhD. pôsobí na Katedre medzinárodného práva a medzinárodných vzťahov Právnickej fakulty Univerzity Komenského v Bratislave a podieľa sa na výučbe predmetov z oblasti medzinárodného práva súkromného, medzinárodného práva obchodného a medzinárodného práva rodinného. Vo svojej výskumnej a publikačnej činnosti sa zameriava na medzinárodné právo súkromné, medzinárodné právo procesné a medzinárodné rodinné právo. Je členkou Slovenskej spoločnosti pre medzinárodné právo a The European Association of Private International Law (EAPIL).

Mgr. Petra Dražová, PhD. pôsobí na pozícii odborný asistent na Ústave práva informačných technológií a práva duševného vlastníctva Právnickej fakulty Univerzity Komenského v Bratislave a vo svojej vedecko-pedagogicko-výskumnej činnosti sa venuje vybraným otázkam kybernetickej kriminality a problematike elektronických dôkazov. Absolvovala zahraničné výskumné pobyty na Viedenskej univerzite, Univerzite v Baskicku či na TalTech Law School. Zároveň pôsobí v aplikačnej praxi ako advokátka špecializujúca sa na odvetvie trestného práva a medzinárodnú justičnú spoluprácu v trestných veciach. Je členkou pracovnej skupiny pre elektronizáciu advokácie a pracovnej skupiny pre trestné právo, ktoré

sú poradnými orgánmi Slovenskej advokátskej komory. Je členkou Európskej komory trestných obhajcov (ECBA). Odborne spolupracuje aj s Radou Európy (HELP program Kybernetická kriminalita a elektronické dôkazy).

Doc. JUDr. Marek Kordík, PhD., LL. M., univ. prof. absolvoval PF UK v Bratislave. Postgraduálne štúdium v Organizácii spojených národov (OSN) so zameraním na medzinárodné trestné právo a právo ozbrojených konfliktov ukončil získaním zvláštnej ceny Vedeckej komisie Inštitútu UNICRI, následne obhájil na PF UK dizertačnú prácu v odbore trestné právo. Od roku 2006 pôsobí na PF UK na Katedre trestného práva, kriminológie a kriminalistiky. Habilitoval sa v odbore trestné právo v roku 2017 a v súčasnosti pôsobí ako univerzitný profesor v odbore trestné právo som zameraním na trestné právo procesné, počítačovú kriminalitu, elektronické dôkazy, crypto a justičnú spoluprácu v trestných veciach. Spolupodieľa sa na národnom hodnotení rizík pre ML/TF. Je expertom EÚ agentúry CEPOL pre oblasť finančného vyšetrovania a zaisťovania majetku. Je členom Vedeckej rady Akadémie PZ v Bratislave, členom redakčnej rady Bulletinu SAK. Je tiež členom slovenskej kryptomenovej asociácie. Je autorom alebo spoluautorom viac ako 150 publikačných výstupov. Je riešiteľom alebo spoluriešiteľom viacerých výskumných projektov v oblasti počítačovej kriminality, elektronických dôkazov a inteligentnej mobility.

Mgr. Stela Košťálová je doktorandkou na Ústave práva informačných technológií a práva duševného vlastníctva Právnickej fakulty Univerzity Komenského v Bratislave. V rámci výskumu sa zameriava na právne aspekty kybernetickej bezpečnosti, data governance a ochranu osobných údajov. Okrem toho sa venuje regulačným sandboxom a skúma, ako môžu podporovať inovácie a zároveň chrániť základné práva. Je súčasťou pracovných skupín Regulácia automatizovanej dopravy a Právo, technológie a spoločnosť. Na Slovensku založila iniciatívu Internet Governance Forum Slovakia.

doc. JUDr. Lukáš Mareček, PhD. je docentom na Katedre medzinárodného práva a medzinárodných vzťahov Právnickej fakulty Univerzity Komenského v Bratislave, lektorom a členom akademickej rady Diplomatickej akadémie Karola Rybárika. Vedecko-výskumne sa zameriava na medzinárodné právo verejné, osobitne na medzinárodné trestné právo. V rámci svojej publikačnej činnosti sa venuje otázkam ako je trestná zodpovednosť právnických osôb

podľa medzinárodného práva, alebo medzinárodný terorizmus. Zúčastnil sa viacerých medzinárodných vedeckých konferencií na Slovensku i v zahraničí. Absolvoval výskumný pobyt na Waseda University v Tokiu.

Doc. JUDr. Matúš Mesarčík, PhD., LL.M. je docent na Ústave práva informačných technológií a práva duševného vlastníctva Právnickej fakulty Univerzity Komenského v Bratislave a Ethics and Law Specialist v Kempelenovom inštitúte inteligentných technológií (KInIT). Vo svojej vedecko-výskumnej a pedagogickej činnosti sa špecializuje na reguláciu umelej inteligencie, ochranu osobných údajov a súkromia, reguláciu digitálnych služieb, kybernetickú bezpečnosť a právne aspekty nových technológií. Je autorom prvej slovenskej vysokoškolskej učebnice o ochrane osobných údajov a prvej učebnice o regulácii umelej inteligencie, ako aj viacerých vedeckých monografií a článkov publikovaných v domácich i zahraničných odborných časopisoch. Absolvoval zahraničné výskumné pobyty na Viedenskej univerzite, University of Cambridge, TalTech Law School a Marquette University (Milwaukee, USA). Jeho vedecké práce boli citované okrem iného aj Ústavným súdom Slovenskej republiky a využité v analytických materiáloch Organizácie Spojených národov (OSN) a Organizácie pre hospodársku spoluprácu a rozvoj (OECD). Pôsobí ako člen expertnej skupiny Európskej komisie pre prípravu Kódexu postupov pre modely umelej inteligencie na všeobecné účely podľa aktu o umelej inteligencii (AI Akt) a ako zástupca v AI Advisory Forum. Pravidelne sa podieľa na poradenskej, lektorskej a publikačnej činnosti v oblasti digitálnej regulácie, umelej inteligencie a ochrany základných práv.

JUDr. Ľudovít Máčaj, PhD. v roku 2017 ukončil štúdium na Právnickej fakulte Univerzity Komenského v Bratislave. V roku 2020 úspešne obhájil dizertačnú prácu z oblasti správneho práva a pozemkového práva, so zameraním na právnu ochranu poľnohospodárskej a lesnej pôdy. Pôsobí ako odborný asistent na Katedre správneho a environmentálneho práva Právnickej fakulty Univerzity Komenského v Bratislave, kde sa venuje výučbe správneho práva, pozemkového a agrárneho práva. V súčasnosti je zástupcom vedúceho katedry. Vo svojej vedeckej činnosti sa zameriava najmä na správne právo, pozemkové právo, ochranu poľnohospodárskeho a lesného pôdneho fondu, ako aj na súvisiace otázky environmentálneho práva a energetickej transformácie v kontexte práva Európskej únie. Aktívne sa podieľa na riešení vedeckovýskumných projektov a vystupuje na vedeckých

konferenciách doma i v zahraničí. Absolvoval vedecké pobyty, okrem iného na Université Paris II Panthéon Assas v Paríži.

Mgr. Maroš Pavlovič, PhD., LL.M je absolventom Právnickej fakulty Univerzity Komenského v Bratislave, kde v roku 2021 obhájil dizertačnú prácu na tému Verejná správa a pozemkové právo. Pôsobí ako odborný asistent na Katedre správneho a environmentálneho práva Právnickej fakulty Univerzity Komenského v Bratislave a venuje sa najmä správnemu právu, pozemkovému právu, agrárnemu právu, environmentálnemu právu a právu informačných technológií. V rokoch 2022 – 2025 pôsobil ako prodekan fakulty. Je autorom monografie Verejný záujem a pozemkové úpravy a publikácie Verejná správa a pozemkové právo, ako aj spoluautor publikácie Praktikum pozemkového práva a autor viacerých odborných a vedeckých článkov. Je riešiteľom a koordinátorom projektov podporených zo zdrojov APVV a zo zdrojov EÚ.

JUDr. Michal Rampášek je doktorand a vyučujúci na Právnickej fakulte Univerzity Komenského v Bratislave, pôsobiaci na Ústave práva informačných technológií a práva duševného vlastníctva a Katedre trestného práva, kriminológie a kriminalistiky. Zároveň je advokátom a pôsobí na vládnej jednotke CSIRT.SK. Je členom ISACA Slovensko Chapter a ISA CZ/SK Chapter. Vo svojej odbornej praxi a akademickom výskume sa zameriava najmä na právo informačných a komunikačných technológií, právo kybernetickej bezpečnosti a trestné právo. V publikačnej činnosti sa venuje predovšetkým právnej ochrane bezpečnostných výskumníkov konajúcich v dobrej viere, koordinovanému oznamovaniu zraniteľností (CVD), riadeniu zraniteľností a incidentov v oblasti kybernetickej bezpečnosti a umelej inteligencie.

Mgr. Miroslav Sorkovský je doktorandom na Ústave práva informačných technológií a práva duševného vlastníctva Právnickej fakulty Univerzity Komenského v Bratislave. Vo svojej vedeckej činnosti sa venuje právnym a regulačným aspektom kybernetickej bezpečnosti, umelej inteligencie, ochrany osobných údajov a automatizovanej mobility. Je členom vedeckých pracovných skupín *Regulácia automatizovanej dopravy* a *Právo, technológie a spoločnosť*, v rámci ktorých sa podieľa na interdisciplinárnom výskume dopadov nových technológií na spoločnosť a právny poriadok. Popri akademickej činnosti pôsobí v

súkromnom sektore ako konzultant v oblasti digitálnej regulácie, kybernetickej bezpečnosti, ochrany osobných údajov a zavádzania inovatívnych technologických riešení.

JEDNOTLIVÉ ČASTI SPRACOVALI

doc. JUDr. Jozef Andraško, PhD.	Kapitola 3.1, 3.2 okrem 3.2.1, 3.3 Kapitola 4.1, 4.2, 4.3 Kapitola 5
Mgr. Petra Dražová, PhD.	kapitola 12.1, 12.2, 12.3, kapitola 12.4.1., 12.4.3, 12.5, okrem 12.5.2., 12.5.3 (50% v spoluautorstve s doc. JUDr. Marekom Kordíkom, PhD., LL.M., univ. prof.), 12.5.4
doc. JUDr. Marek Kordík, PhD., LL.M. (univerzitný profesor)	kapitola 12.4.2, 12.4.4, 12.5.2., 12.5.3 (50% v spoluautorstve s Mgr. Petrou Dražovou, PhD.)
doc. JUDr. Matúš Mesarčík, PhD., LL.M	Kapitola 2 v spoluautorstve s Mgr. Stela Košťálová Kapitola 6 Kapitola 7 Kapitola 8
JUDr. Michal Rampášek	Kapitola 1 Kapitola 4.4, 4.5 Kapitola 13
doc. JUDr. Katarína Burdová, PhD.	Kapitola 11.2
doc. JUDr. Lukáš Mareček, PhD.	Kapitola 11.1

Mgr. Maroš Pavlovič, PhD., LL.M.	Kapitola 9.6, 9.7 Kapitola 10
JUDr. Ľudovít Máčaj, PhD.	Kapitola 9.1, 9.2, 9.3, 9.4, 9.5
Mgr. Stela Košťálová	Kapitola 2 v spoluautorstve s doc. JUDr. Matúš Mesarčík, PhD., LL.M Kapitola 3.2.1
Mgr. Miroslav Sorkovský	Kapitola 4.6

PREDHOVOR

Milé čitateľky, milí čitatelia,

do rúk sa Vám dostáva učebnica „Regulácia kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality". Ide o kolektívne dielo, ktorého cieľom je poskytnúť systematický, zrozumiteľný a odborne podložený výklad právnej regulácie v oblastiach, ktoré dnes patria medzi najdynamickejšie a zároveň najdôležitejšie výzvy digitálnej spoločnosti.

Učebnicu sme koncipovali ako študijnú pomôcku pre účastníkov kurzov zabezpečovaných Kompetenčným centrom pre reguláciu kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality (CUSEC) a predmetov poskytovaných na Právnickej fakulte Univerzity Komenského v Bratislave. Zároveň však veríme, že bude užitočná aj pre študentov iných právnických fakúlt, študentov odborov s presahom na informačné technológie, odborníkov z praxe, pracovníkov verejnej správy, regulované subjekty, ako aj všetkých, ktorí sa chcú lepšie zorientovať v právnych otázkach digitálnej bezpečnosti.

Našou snahou bolo vytvoriť učebnicu, ktorá nebude iba prehľadom platných právnych predpisov, ale ktorá čitateľovi umožní pochopiť širšie súvislosti regulácie. Kybernetická bezpečnosť už dávno nie je len technickou a organizačnou otázkou. Dotýka sa ochrany základných práv a slobôd, fungovania štátu, bezpečnosti kritických služieb, ochrany osobných údajov, zodpovednosti organizácií, trestnoprávneho postihu kybernetickej kriminality, ako aj dôvery v digitálne služby a technológie. Právo v tejto oblasti preto musí reagovať nielen na technologický vývoj, ale aj na nové formy rizík, incidentov, útokov a spoločenských dopadov.

Učebnica postupne približuje teoretické základy kybernetickej bezpečnosti, jej ústavnoprávne a ľudskoprávne súvislosti, regulačné nástroje a princípy, právnu úpravu Európskej únie a Slovenskej republiky, ako aj vybrané súvisiace oblasti. Osobitná pozornosť je venovaná ochrane súkromia a osobných údajov, administratívnoprávnej zodpovednosti, medzinárodnoprávnym aspektom kybernetickej bezpečnosti, kybernetickej kriminalite a bezpečnosti operačných technológií. Zámerom bolo ukázať, že tieto témy nemožno vnímať izolovane, ale ako vzájomne previazané časti jedného regulačného ekosystému.

Pri príprave učebnice sme sa snažili spojiť akademickú presnosť s praktickou použiteľnosťou. Tam, kde je to potrebné, text pracuje s právnymi predpismi, judikatúrou, technickými normami, metodickými dokumentmi, bezpečnostnou terminológiou a praktickými príkladmi. Cieľom nie je nahradiť primárne pramene, ale pomôcť čitateľovi porozumieť ich významu, systematike a praktickým dôsledkom.

Sme si vedomí, že oblasť kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality sa vyvíja mimoriadne rýchlo. Právna úprava reaguje na nové technológie, nové bezpečnostné hrozby, meniace sa spôsoby útokov, ako aj na potrebu väčšej odolnosti verejných aj súkromných subjektov. Aj preto nemožno túto učebnicu vnímať ako uzavreté dielo, ale skôr ako východisko pre ďalšie štúdium, odbornú diskusiu a praktické uplatňovanie právnych pravidiel v digitálnom prostredí.

Veríme, že učebnica prispeje k lepšiemu pochopeniu právnej regulácie kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality a že bude užitočná nielen pri výučbe, ale aj pri riešení praktických problémov. Budeme radi, ak sa stane pomôckou pre tých, ktorí sa chcú v tejto oblasti vzdelávať, odborne rásť a podieľať sa na tvorbe bezpečnejšieho a dôveryhodnejšieho digitálneho prostredia.

doc. JUDr. Jozef Andraško, PhD.
za autorský kolektív

OBSAH

ZOZNAM SKRATIEK

Agentúra ENISA znamená Agentúra Európskej únie pre kybernetickú bezpečnosť.

AI znamená Artificial Intelligence – umelá inteligencia.

Akt o kybernetickej bezpečnosti alebo znamená nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013.

Akt o umelej inteligencii alebo AI Akt znamená nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii).

APT znamená Advanced Persistent Threat – pokročilá pretrvávajúca hrozba.

BIA znamená Business Impact Analysis – analýza dopadov na podnikanie / analýza funkčných dopadov.

Budapeštiansky dohovor znamená Dohovor Rady Európy o počítačovej kriminalite, oznámenie MZV SR č. 137/2008 Z. z. o podpísaní Dohovoru o počítačovej kriminalite.

CASP znamená poskytovateľ služieb kryptoaktív.

CEN znamená European Committee for Standardization – Európsky výbor pre normalizáciu.

CENELEC znamená European Committee for Electrotechnical Standardization – Európsky výbor pre normalizáciu v elektrotechnike.

Charta znamená Charta základných práv Európskej únie.

CRA alebo Akt o kybernetickej odolnosti znamená nariadenia Európskeho parlamentu a Rady (EÚ) 2024/2847 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami (akt o kybernetickej odolnosti)

CSIRT znamená Computer Security Incident Response Team – jednotka pre riešenie počítačových bezpečnostných incidentov, určená alebo zriadená podľa smernice NIS 2.

CVE znamená Common Vulnerabilities and Exposures – spoločné identifikátory zraniteľností.

CVSS znamená Common Vulnerability Scoring System – spoločný systém hodnotenia závažnosti zraniteľností.

DDoS znamená Distributed Denial of Service – distribuované odmietnutie služby / distribuovaný útok na dostupnosť služby.

Dohovor znamená Dohovor Rady Európy o ochrane základných ľudských práv a slobôd.

DORA znamená nariadenie (EÚ) 2022/2554 o digitálnej prevádzkovej odolnosti finančného sektora (angl. Digital Operational Resilience Act).

e-Evidence nariadenie znamená nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1543 z 12. júla 2023 o európskych príkazoch na predloženie elektronických dôkazov a európskych príkazoch na uchovanie elektronických dôkazov v trestnom konaní a na výkon trestu odňatia slobody v nadväznosti na trestné konanie.

e-Evidence smernica znamená smernica Európskeho parlamentu a Rady (EÚ) 2023/1544 z 12. júla 2023, ktorou sa stanovujú harmonizované pravidlá určovania určených prevádzkarní a vymenúvania právnych zástupcov na účely zhromažďovania dôkazov v trestnom konaní.

EBA znamená Európsky orgán pre bankovníctvo (angl. European Banking Authority).

ECB znamená Európska centrálna banka (angl. European Central Bank).

EDĽP znamená Európsky dohovor o ochrane ľudských práv a základných slobodách.

EIOPA znamená Európsky orgán pre poisťovníctvo a dôchodkové poistenie zamestnancov (angl. European Insurance and Occupational Pensions Authority).

EN znamená European Norm / European Standard – európska norma.

ENISA znamená European Union Agency for Cybersecurity – Agentúra Európskej únie pre kybernetickú bezpečnosť.

ES znamená Európske spoločenstvo (v označení právnych aktov, napr. nariadenie (ES) č. 1060/2009).

ESĽP znamená Európsky súd pre ľudské práva.

ESMA znamená Európsky orgán pre cenné papiere a trhy (angl. European Securities and Markets Authority).

ETSI znamená European Telecommunications Standards Institute – Európsky inštitút pre telekomunikačné normy.
EÚ znamená Európska únia.

EUCC znamená European Common Criteria-based Cybersecurity Certification Scheme – európska schéma kybernetickej certifikácie založená na Common Criteria; vykonávacie nariadenie Komisie (EÚ) 2024/482 z 31. januára 2024, ktorým sa stanovujú pravidlá uplatňovania nariadenia (EÚ) 2019/881, pokiaľ ide o prijatie európskej schémy kybernetickej certifikácie založenej na Common Criteria (EUCC).

EUR znamená euro (mena).

FOSS znamená Free and Open-Source Software – slobodný softvér a softvér s otvoreným zdrojovým kódom.

GDPR znamená 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).

IEC znamená International Electrotechnical Commission – Medzinárodná elektrotechnická komisia.

IKT znamená informačné a komunikačné technológie.

IoT znamená Internet of Things – internet vecí.

ISMS znamená Information Security Management System – systém riadenia informačnej bezpečnosti.

ISO znamená International Organization for Standardization – Medzinárodná organizácia pre normalizáciu.

ITVS znamená informačné technológie vo verejnej správe.

KEV znamená Known Exploited Vulnerabilities – známe zneužívané zraniteľnosti.

KPI znamená Key Performance Indicators – kľúčové ukazovatele výkonnosti.

LLM znamená Large Language Model – veľký jazykový model.

MIRRI SR znamená Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky.

Nariadenie (EÚ) 2018/1805 znamená nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1805 zo 14. novembra 2018 o vzájomnom uznávaní príkazov na zaistenie a príkazov na konfiškáciu.

Nariadenie eIDAS znamená nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES.

NBÚ znamená Národný bezpečnostný úrad.

NIST znamená National Institute of Standards and Technology – Národný inštitút pre štandardy a technológie.

OSINT znamená informácia z otvorených zdrojov alebo otvorené vyšetrovanie.

OSN znamená Organizácia Spojených národov.

OT znamená Operational Technology – prevádzkové technológie.

Predpis OSN č. 155 znamená Predpis OSN č. 155 – Jednotné ustanovenia na účely typového schvaľovania vozidiel vzhľadom na kybernetickú bezpečnosť a systém riadenia kybernetickej bezpečnosti [2021/387].

PriesZ znamená zákon SNR č. 372/1990 Zb. o priestupkoch.

prostriedok IKT znamená prostriedok informačno-komunikačných technológií.

PZS znamená prevádzkovateľ základnej služby.

PKZS znamená prevádzkovateľ kritickej základnej služby.

SDEÚ znamená Súdny dvor Európskej únie.

Smernica (EÚ) 2016/1148 znamená 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.

Smernica (EÚ) 2019/713 znamená smernica Európskeho parlamentu a Rady (EÚ) 2019/713 zo 17. apríla 2019 o boji proti podvodom s bezhotovostnými platobnými prostriedkami a proti ich falšovaniu a pozmeňovaniu, ktorou sa nahrádza rámcové rozhodnutie Rady 2001/413/SVV.

Smernica 2013/40/EÚ znamená 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.

Smernica 2014/41/EÚ znamená smernica Európskeho parlamentu a Rady 2014/41/EÚ z 3. apríla 2014 o európskom vyšetrovacom príkaze v trestných veciach.

Smernica NIS alebo NIS znamená 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.

Smernica NIS 2 alebo NIS 2 znamená smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2).

Smernica o odolnosti kritických subjektov znamená smernica Európskeho parlamentu a Rady (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/114/ES.

Smernica RED znamená smernica Európskeho parlamentu a Rady 2014/53/EÚ o harmonizácii právnych predpisov členských štátov týkajúcich sa sprístupňovania rádiových zariadení na trhu

Správny poriadok znamená zákon č. 71/1967 Zb. o správnom konaní (správny poriadok).

SR znamená Slovenská republika.

SRB znamená Jednotná rada pre riešenie krízových situácií (angl. Single Resolution Board).

TIBER-EÚ znamená európsky rámcový program pre etický red teaming založený na spravodajských informáciách o hrozbách (angl. Threat Intelligence-based Ethical Red Teaming); jeho slovenskou implementáciou je TIBER-SK (Národná banka Slovenska).

TLPT znamená penetračné testovanie na základe konkrétnej hrozby (angl. Threat-Led Penetration Testing), čl. 26 DORA.

Trestný poriadok / TP znamená zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov.

Trestný zákon / TZ znamená zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov.

Ú. v. EÚ znamená Úradný vestník Európskej únie.

Ústava SR znamená Ústava Slovenskej republiky č. 460/1992 Zb.

Vykonávacie nariadenie Komisie (EÚ) 2024/2690 znamená vykonávacie nariadenie Komisie (EÚ) 2024/2690 zo 17. októbra 2024, ktorým sa stanovujú pravidlá uplatňovania smernice (EÚ) 2022/2555, pokiaľ ide o technické a metodické požiadavky na opatrenia na riadenie kybernetických rizík a o bližšie určenie prípadov, v ktorých sa incident považuje za významný, vo vzťahu k poskytovateľom služieb DNS, správcom názvov TLD, poskytovateľom služieb

cloud computingu, poskytovateľom služieb dátového centra, poskytovateľom sietí na sprístupňovanie obsahu, poskytovateľom riadených služieb, poskytovateľom riadených bezpečnostných služieb, poskytovateľom online trhov, internetových vyhľadávačov a platforiem služieb sociálnej siete a poskytovateľom dôveryhodných služieb.

Zákon o kritickej infraštruktúre znamená zákon č. 367/2024 Z. z. o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov.

Zákon o ochrane pred odpočúvaním znamená zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným odpočúvaním a použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

ZEK znamená zákon č. 452/2021 Z. z. o elektronických komunikáciách v znení neskorších predpisov.

ZEÚ znamená Zmluva o Európskej únii.

ZFEÚ znamená Zmluva o fungovaní Európskej únie.

ZoEVP znamená zákon č. 236/2017 Z. z. o európskom vyšetrovacom príkaze v trestných veciach v znení neskorších predpisov.

ZoITVS znamená zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.

ZoKB alebo zákon o kybernetickej bezpečnosti znamená zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

ZoTZPO znamená zákon č. 91/2016 Z. z. o trestnej zodpovednosti právnických osôb a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

ZPZ znamená zákon č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov.

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

1. TEORETICKÉ ZÁKLADY KYBERNETICKEJ BEZPEČNOSTI

Rozvoj informačných a komunikačných technológií zásadne mení fungovanie verejnej správy, hospodárstva aj každodenného života. Digitalizácia služieb, cloudové platformy, masívne prepojenie zariadení (Internet of Things - IoT) a rýchlo rastúca dostupnosť systémov umelej inteligencie vytvárajú nové možnosti, no zároveň zvyšujú závislosť spoločnosti od bezpečného a spoľahlivého fungovania sietí a informačných systémov. Súčasne rastie prepojenie tradičných IT prostredí s prevádzkovými technológiami (operational technology - OT), ktoré riadia fyzické procesy v energetike, priemysle, doprave či zdravotníctve. Americký inštitút pre štandardy a technológie (NIST) výslovne zdôrazňuje, že OT zahŕňa široký rozsah programovateľných systémov a zariadení, ktoré priamo interagujú s fyzickým prostredím (monitorovaním a riadením zariadení, procesov a udalostí), pričom majú špecifické požiadavky na dostupnosť, spoľahlivosť a bezpečnosť.[1] Práve tieto požiadavky vysvetľujú, prečo sa OT bezpečnosť nedá zredukovať na bežnú IT bezpečnosť a prečo sa v praxi presadzujú technické normy pre priemyselné automatizačné a riadiace systémy, ako je ISA/IEC 62443, ktorý sa zameriava na požiadavky a procesy zavádzania a udržiavania bezpečnosti v priemyselných riadiacich prostrediach.

Kybernetická bezpečnosť sa pritom v posledných rokoch čoraz zreteľnejšie posúva z domény „technického problému" do jadra verejnej politiky a regulácie, ako aj do oblasti trestného práva. Európska únia reaguje na rastúcu kritickosť digitálnych služieb a infraštruktúr komplexným regulačným rámcom. Základným pilierom je smernica NIS2, ktorá posilňuje požiadavky na riadenie rizík, nahlasovanie incidentov a dohľad v sektoroch vysokej kritickosti (napr. energetika, doprava, zdravotníctvo, digitálna infraštruktúra). Paralelne sa rozvíja aj rámec fyzickej a organizačnej odolnosti kritických subjektov prostredníctvom smernice CER. V sektoroch, kde je kybernetická odolnosť úzko spätá s bezpečnosťou dodávateľských reťazcov a produktov, nadobúda význam aj Akt o kybernetickej odolnosti (CRA), ktorý zavádza horizontálne požiadavky na kybernetickú bezpečnosť produktov s digitálnymi prvkami počas ich životného cyklu. Na podporu dôvery a harmonizácie sa opiera

[1] STOUFFER, Keith a kol. Guide to Operational Technology (OT) Security. NIST Special Publication 800-82 Revision 3. Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2023. dostupné na: https://doi.org/10.6028/NIST.SP.800-82r3.

o európsky rámec certifikácie podľa Aktu o kybernetickej bezpečnosti (CSA)[2], ktorý vytvára mechanizmy pre schémy kybernetickej certifikácie IKT produktov a služieb. K tomu sa pridávajú sektorové pravidlá, napríklad v energetike delegované nariadenie vytvárajúce sieťový kód pre kybernetickú bezpečnosť cezhraničných tokov elektriny. V oblasti AI je kľúčovým míľnikom nariadenie o umelej inteligencii (AIA), ktorý zavádza harmonizované pravidlá pre systémy AI vrátane režimu vysokorizikových systémov, modely AI pre všeobecné použitie a povinností v dodávateľskom reťazci.

S rastom regulácie však paralelne rastie aj fenomén kybernetickej kriminality a hybridných hrozieb. ENISA v prehľade hrozieb za rok 2025 poukazuje na dynamický vývoj hrozieb v podmienkach geopolitickej eskalácie, pričom zdôrazňuje význam trendov ako ransomware, zneužívanie zraniteľností, dodávateľské reťazce a zvyšujúcu sa sofistikovanosť útočných kampaní.[3] Europol vo svojej pravidelnej hodnotiacej správe o internetovej organizovanej kriminalite za rok 2025 opisuje, že kyberkriminalita v EÚ sa vyvíja v objeme, intenzite aj v potenciály ujmy a reaguje na nové technológie, ktoré znižujú bariéry vstupu a podporujú škálovanie útokov.[4] Z akademického a praktického hľadiska je preto vhodné vnímať kybernetickú bezpečnosť ako interdisciplinárne pole, v ktorom sa stretávajú technické opatrenia (architektúra, kryptografia, monitoring), organizačné mechanizmy (governance, riadenie rizík, incident response) a právne nástroje (regulačné povinnosti, zodpovednosť, trestnoprávne hranice).

Osobitný dôraz si zaslúži rýchly rozvoj umelej inteligencie, ktorá do kybernetickej bezpečnosti vstupuje dvojako. Na jednej strane zvyšuje schopnosti obrany, napríklad pri detekcii anomálií, korelácii udalostí alebo automatizácii reakcie na incidenty. Na druhej strane sa AI stáva nástrojom útoku, keď umožňuje personalizované sociálne inžinierstvo, generovanie presvedčivých phishingových kampaní, automatizáciu prieskumu cieľov alebo tvorbu deepfake obsahu využiteľného pri podvodoch a vydieraní. Na úrovni verejnej správy a regulovaných sektorov preto nadobúda význam nielen „klasická" kybernetická hygiena, ale

[2] V januári 2026 bol predstavený návrh nového nariadenia (CSA 2)

[3] ENISA. ENISA Threat Landscape 2025. Athens: European Union Agency for Cybersecurity (ENISA), October 2025. ISBN 978-92-9204-723-8. DOI: 10.2824/1946374. Dostupné na: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.

[4] EUROPOL, *Steal, deal and repeat - How cybercriminals trade and exploit your data – Internet Organised Crime Threat Assessment*, Publications Office of the European Union, Luxembourg, 2025. dostupné na: https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data.

aj schopnosť organizácií nastavovať politiky bezpečného používania AI, kontrolovať integrácie nástrojov, spravovať prístupové práva a auditovať používanie produktov alebo služieb, ktoré integrujú alebo samy sú systémami alebo modelmi AI.

Uvedené technologické trendy zároveň posilňujú význam otázok odolnosti a vyspelosti (maturity) sektorov. ENISA hodnotí kritickosť a zrelosť sektorov spadajúcich pod NIS2 a poskytuje komparatívny prehľad medzier, ktoré majú členské štáty a regulačné orgány prioritizovať.[5] Táto perspektíva je dôležitá pre úvod do kybernetickej bezpečnosti aj preto, že posúva diskusiu od izolovaných incidentov k systémovej pripravenosti odvetví, k riadeniu dodávateľských vzťahov, k zdieľaniu informácií a k štandardizácii bezpečnostných postupov.

Cieľom úvodnej časti učebnice preto nie je len vysvetliť technické pojmy, ale najmä ukázať, prečo je kybernetická bezpečnosť právne relevantná a prečo sa jej ochrana premieta do povinností organizácií, do dohľadových kompetencií štátu a do trestnoprávnej úpravy. Kybernetická bezpečnosť sa dnes týka ochrany základných funkcií spoločnosti, dôvery v digitálne služby a schopnosti štátu aj súkromných subjektov predchádzať incidentom a zvládať ich dopady. Práve v prostredí prepojenia IT, OT a AI je kľúčové porozumieť tomu, kde vznikajú riziká, aké typy incidentov sú typické, aké sú minimálne bezpečnostné štandardy a akými nástrojmi právo formuje prevenciu, oznamovanie, zodpovednosť a dohľad vrátane ukladania sankcií.

1.1 Informačná bezpečnosť, kybernetická bezpečnosť a kybernetická odolnosť

V bežnej praxi sa pojmy informačná bezpečnosť a kybernetická bezpečnosť často zamieňajú. Na úvod je však užitočné ich odlíšiť, pretože pracujú s podobnými princípmi, ale s odlišným ťažiskom ochrany. Informačná bezpečnosť sa tradične chápe ako ochrana informácií ako aktíva bez ohľadu na to, či sú v papierovej, ústnej alebo digitálnej podobe. V praxi sa preto dotýka aj archívov, dokumentácie, režimu prístupov, režimu utajenia, fyzického zabezpečenia nosičov či riadenia interných procesov. Kybernetická bezpečnosť sa naproti tomu sústreďuje na bezpečnosť informácií a služieb v prostredí sietí a informačných systémov, teda v priestore, kde informácie vznikajú, prenášajú sa, spracúvajú a poskytujú ako

[5] ENISA: *ENISA NIS360 2024. Cybersecurity Maturity & Criticality Assessment of NIS2 sectors.* Luxembursko: Európska agentúra pre kybernetickú bezpečnosť (ENISA), 2025. ISBN 978-92-9204-687-3. DOI: 10.2824/1378797. Dostupné na: https://www.enisa.europa.eu/publications/enisa-nis360-2024.

digitálne služby. **Informačnú bezpečnosť** je možné definovať ako „*zachovanie dôvernosti, integrity a dostupnosti informácií*".[6] Na druhej strane **kybernetická bezpečnosť** je definovaná ako „*zachovanie dôvernosti, integrity a dostupnosti informácií v kybernetickom priestore*".[7] **Kybernetický priestor** je „*komplexné prostredie, ktoré je výsledkom interakcie ľudí, softvéru a služieb na internete prostredníctvom technologických zariadení a sietí, ktoré sú k nemu pripojené, a ktoré neexistujú v žiadnej fyzickej podobe*".[8]

Autori von Solms a van Niekerk upozorňujú, že kybernetická bezpečnosť sa síce s informačnou bezpečnosťou významne prekrýva, ale nie je totožná.[9] Kybernetická bezpečnosť podľa nich presahuje hranice tradičnej informačnej bezpečnosti, keďže sa netýka iba informačných aktív, ale aj ďalších aktív a v konečnom dôsledku aj ochrany osôb a ich záujmov v digitálnom prostredí. Toto rozlíšenie je podstatné najmä preto, že regulácia a zodpovednosť sa v praxi viažu raz na informácie (napr. osobné údaje, obchodné tajomstvo, utajované skutočnosti), inokedy na siete a informačné systémy a ich odolnosť, a často na kombináciu oboch.

Obdobne ZoKB pracuje s kľúčovým pojmom kybernetický priestor, ktorý definuje ako „globálny dynamický otvorený systém sietí a informačných systémov", vytváraný aktivovanými prvkami, osobami vykonávajúcimi aktivity a vzťahmi a interakciami medzi nimi. Dôležité je, že ZoKB týmto spôsobom nepopisuje iba technickú infraštruktúru. Výslovne do konceptu kybernetického priestoru zahŕňa aj ľudský faktor a interakcie. To je praktický dôvod, prečo je kybernetická bezpečnosť nevyhnutne interdisciplinárna. Nestačí jej technické riešenie, pretože incidenty často vznikajú aj z organizačných zlyhaní, z ľudských omylov, zo zlej správy prístupov alebo zo zlyhania dodávateľských vzťahov.

CIA triáda

Bez ohľadu na terminologické rozdiely sa informačná aj kybernetická bezpečnosť opierajú o rovnaké základné princípy, ktoré sa v literatúre tradične opisujú ako CIA triáda,

[6] International Organization for Standardization, International Electrotechnical Commission. ISO/IEC 27000: 2018 - Information technology—Security techniques—Information security management systems—Overview and vocabulary.
[7] International Organization for Standardization, International Electrotechnical Commission. ISO/IEC 27032: 2012 – Information technology—Security techniques—Guidelines for cybersecurity.
[8] Tamtiež.
[9] Rossouw von Solms, Johan van Niekerk, From information security to cyber security, Computers & Security, Volume 38, 2013, Pages 97-102, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2013.04.004.

teda dôvernosť, integrita a dostupnosť. Tieto princípy sú zakotvené aj v zákonných definíciách, ktoré upravuje ZoKB. Zákon definuje dôvernosť ako záruku, že údaj alebo informácia nie je prezradená neoprávnenému subjektu alebo procesu. Dostupnosť definuje ako záruku, že údaj alebo poskytovaná služba sú prístupné vtedy, keď sú potrebné a požadované. Integritu opisuje ako záruku, že bezchybnosť, úplnosť alebo správnosť údajov neboli narušené. Tieto tri princípy sú prakticky použiteľné aj ako „mapa" typických dopadov incidentov. Pri narušení dôvernosti ide spravidla o únik informácií, neoprávnené sprístupnenie alebo odhalenie obsahu. Pri narušení integrity ide o neoprávnenú zmenu údajov alebo konfigurácií, prípadne o poškodenie, ktoré spôsobí, že údaje už nie sú spoľahlivé. Pri narušení dostupnosti ide o výpadok služby, degradáciu výkonu alebo odmietnutie prístupu, typicky aj v dôsledku útokov typu DoS. Z právneho hľadiska je významné, že rovnaký incident môže zasiahnuť viacero princípov naraz. Ransomvér napríklad často narúša dostupnosť, pretože zašifruje systémy, ale môže narušiť aj dôvernosť, ak útočníci údaje pred šifrovaním exfiltrovali. Od triády k „hexáde" a prepojenie s pojmom pravosti V praxi sa však ukazuje, že CIA triáda nie vždy postačuje na presné zachytenie povahy incidentu. Preto sa v literatúre často uvádza rozšírený model známy ako Parkerian Hexad. Donn B. Parker ho predstavil ako kritiku príliš zjednodušeného chápania bezpečnosti a doplnil k CIA triáde tri ďalšie vlastnosti informácie, konkrétne držbu alebo kontrolu, autentickosť a užitočnosť.[10] Tento rozšírený model je pre kybernetickú bezpečnosť mimoriadne užitočný aj v právnom kontexte, lebo lepšie vystihuje situácie, keď formálne nedochádza k úniku obsahu, no napriek tomu nastáva bezpečnostný problém. Držba alebo kontrola zdôrazňuje, že bezpečnostný incident môže spočívať aj v strate kontroly nad nosičom alebo systémom, hoci obsah údajov nemusí byť bezprostredne prezradený. Užitočnosť zasa pomáha vysvetliť situácie, keď sú údaje síce „dostupné", ale v takej forme, že ich nemožno efektívne použiť, napríklad keď sa stratí dešifrovací kľúč alebo keď je dátový súbor poškodený tak, že ho systém nevie interpretovať. Autentickosť potom reaguje na riziká falšovania pôvodu alebo identity, ktoré sú v ére deepfake a generatívnej AI osobitne výrazné.

Zaujímavé je, že slovenská legálna definícia kybernetickej bezpečnosti v ZoKB už pracuje aj s prvkom, ktorý CIA triáda neobsahuje explicitne. ZoKB definuje kybernetickú bezpečnosť ako stav, v ktorom sú siete a informačné systémy schopné odolávať konaniu

[10] Parker, D. B. Fighting Computer Crime: A new Framework for Protecting Information New York. 1998, Wiley Computer Publishing, John Wiley & Sons, Inc.

ohrozujúcemu dostupnosť, *pravosť*, integritu alebo dôvernosť údajov a súvisiacich služieb. Práve „pravosť" sa obsahovo približuje k otázkam autenticity v širších modeloch bezpečnosti. Moderná regulácia už nemieri iba na klasické incidenty ako únik údajov či výpadok služby, ale aj na manipuláciu identity, pôvodu informácií a dôveryhodnosti digitálnych výstupov.

Kybernetická odolnosť

Kybernetická bezpečnosť a kybernetická odolnosť (cyber resilience) sa v praxi často zamieňajú, no ide o rozdielne i keď komplementárne koncepty. **Kybernetická bezpečnosť** sa tradične sústreďuje najmä na znižovanie pravdepodobnosti úspešného útoku alebo zneužitia zraniteľnosti prostredníctvom opatrení ako segmentácia, riadenie prístupov, hardening, detekcia a reakcia. Kybernetická odolnosť, teda schopnosť systémov odolávať, prispôsobovať sa a uspieť aj napriek úspešným a často nezisteným útokom, sa tak stala čoraz dôležitejšou a je potrebné ju vnímať ako faktický štandard pre profesionálny rozvoj bezpečnostných stratégií. **Kybernetická odolnosť** vychádza z realistického predpokladu, že ani kvalitná ochrana nezaručí že incidenty nenastanú, a preto kladie dôraz na *udržanie kritických funkcií* a *schopnosť organizácie prežiť incident* s prijateľnými dopadmi a v primeranom čase obnoviť svoju činnosť.

Najvýraznejšie je prebiehajúce rozsiahle zavádzanie technológií strojového učenia do tradičnejších systémov novou výzvou pre bezpečnosť, s problémami týkajúcimi sa okrem iného (chýbajúcej) vysvetliteľnosti, detekcie skreslenia, kontroly nad tréningovými údajmi a modelmi, ako aj problému neustále sa meniacej povahy modelov v posilňovacom učení. Všetky tieto nové výzvy sa týkajú problému detekcie úspešných útokov, a preto je obzvlášť dôležité navrhnúť odolné systémy, ktoré môžu naďalej fungovať za týchto okolností, a to aj v súvislosti s princípom ovládateľnej umelej inteligencie. Okrem tohto zamerania na dáta, prebiehajúca integrácia OT systémov s IT sieťami ďalej zvyšuje plochu útoku na kritické odvetvia a infraštruktúry. V závislosti od aktuálneho OT systému sa nové výzvy netýkajú len fázy detekcie, ale aj zmierňovanie už zistených problémov môže byť problematické alebo dokonca nemožné kvôli obmedzeniam spôsobeným technickými nedostatkami, prevádzkovými požiadavkami alebo dokonca regulačnými požiadavkami. Systémy preto musia byť schopné vysporiadať sa s úspešne zistenými, ale neodstrániteľnými útokmi.[11]

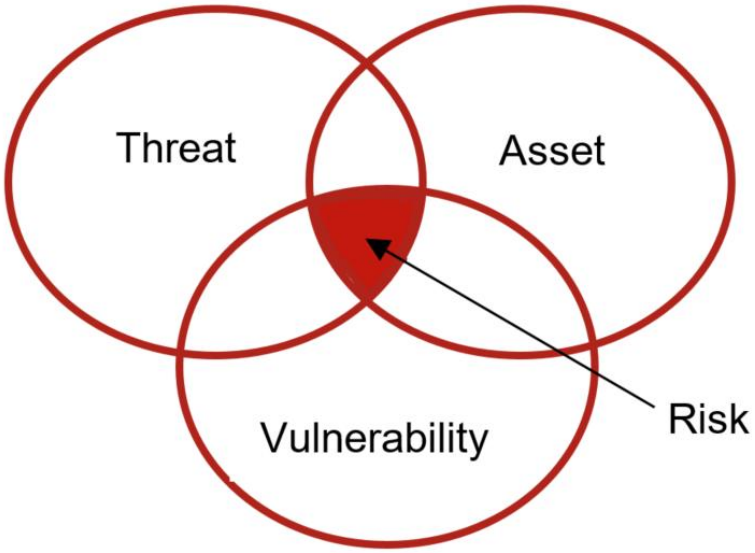
[11] Tjoa, Simon; Gafić, Melisa; Kieseberg, Peter. *Cyber Resilience Fundamentals*. Cham: Springer, 2024. (Studies in Systems, Decision and Control; vol. 520). https://doi.org/10.1007/978-3-031-52064-8

V neposlednom rade ekonomický a technologický vývoj viedol k sieti vzájomne závislých spoločností a organizácií, čo viedlo k extrémne zložitým štruktúram, najmä v dodávateľských reťazcoch. Preto sa dnes skutočne kritické systémy často neprekrývajú s hranicami samotnej spoločnosti. Pre firmu môže byť kľúčový systém externého dodávateľa dôležitejší než niektoré jej vlastné interné systémy, čo robí čisto organizačne zameraný pohľad na kybernetickú bezpečnosť problematickým. Kybernetická odolnosť sa preto musí posudzovať z hľadiska vzájomných závislostí a aj mimo samotnú spoločnosť.

Uchopiteľnú definíciu kybernetickej odolnosti ponúka NIST, ktorý ju definuje ako „**schopnosť predvídať, odolať, zotaviť sa a adaptovať sa** na nepriaznivé podmienky, stres, útoky alebo kompromitácie v systémoch, ktoré používajú alebo sú umožnené kybernetickými zdrojmi".[12] Tento posun od ochrany k odolnosti je dôležitý aj pre chápanie povinností. Už nejde iba o to, či subjekt zaviedol primerané preventívne opatrenia, ale aj o to, či vie preukázať pripravenosť na incidenty, udržanie poskytovania svojej činnosti a obnovu. V európskom kontexte sa práve táto logika odráža aj v dôraze právnej úpravy na kontinuitu a odolnosť kritických sektorov v smerniciach NIS2 a CER.

Praktickým mostom medzi „bezpečnosťou" a „odolnosťou" sú **testy odolnosti a cvičenia**, ktoré cielene overujú schopnosť organizácie zvládnuť vážne incidenty. ENISA napríklad v metodike kybernetických stresových testov definuje stresový test ako „cielené posúdenie odolnosti organizácií a ich schopnosti odolať a zotaviť sa zo závažných kybernetických incidentov pri zabezpečení poskytovania kritických služieb v rôznych rizikových scenároch".[13] Kybernetická odolnosť sa následne prenáša do merateľných prvkov (určenie cieľovej doby obnovy a cieľového bodu obnovy, plán zálohovania, plán obnovy, postupy reakcie na incidenty, testovanie obnovy, apod.) a cez zdokumentované opatrenia ako sú záznamy o testoch, výsledky auditov, plány kontinuity.

[12] Dostupné na: https://csrc.nist.gov/glossary/term/cyber_resiliency.
[13] Dostupné na: https://www.enisa.europa.eu/news/putting-eu-resilience-to-the-test-enisa-handbook-on-cyber-stress-testing.



Obrázok č. 1: Riziko v kontexte hrozby, aktíva a zraniteľnosti.

1.2 Aktíva

Ak má mať kybernetická bezpečnosť v organizácii zmysel, musí začať otázkou hodnoty. V praxi sa riadenie kybernetickej bezpečnosti začína inventúrou vlastných aktív a ich priebežnou aktualizáciou. Kým neviete, čo všetko má pre organizáciu hodnotu (a kde sa to nachádza, kto to spravuje a od čoho to závisí), nedá sa rozumne nastaviť ani ochrana, ani zodpovednosti, ani proporcionalita opatrení. Preto si organizácie vedú evidenciu aktív, často úplne jednoducho (napríklad v tabuľke) a dopĺňajú ju o údaje, ktoré umožňujú aktívum identifikovať, priradiť mu zodpovednú osobu a určiť jeho význam pre služby a procesy organizácie. Z právneho hľadiska je identifikácia aktív dôležitá aj preto, že slúži ako podklad pre posúdenie či organizácia konala primerane, či vedela (alebo mala vedieť), čo chráni, a či mala nastavené minimálne procesy na ochranu najdôležitejších prvkov svojho fungovania.

Pojem „aktívum" (asset) treba chápať širšie, než je bežné v laickej reči. V platnej právnej úprave kybernetickej bezpečnosti sa aktívum definuje ako „hmotný alebo nehmotný komponent informačnej architektúry, ktorý má pre prevádzkovateľa základnej služby hodnotu, najmä služby, procesy, informácie alebo údaje."[14] Aktívum je čokoľvek, čo má pre organizáciu hodnotu, prípadne čokoľvek, bez čoho organizácia nevie túto hodnotu vytvárať,

[14] § 2 písm. a) vyhlášky NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach.

poskytovať alebo chrániť.[15] Preto aktívami nie sú len počítače či servery. Aktívom môžu byť informácie, služby, systémy a siete, výrobné a produkčné technológie[16] vrátane operačných technológie (OT), ľudia a ich know-how, dodávatelia a externé služby, ale aj reputácia a dôvera.

Metodické odporúčania zdôrazňujú, že medzi aktívami treba zaradiť aj osobné údaje, duševné vlastníctvo, interné dokumenty a personál, teda prvky, ktorých poškodenie sa prejaví až sekundárne, napríklad stratou klientov či zmluvnými sankciami.[17]

Na účely riadenia kybernetickej bezpečnosti je užitočné rozlišovať medzi primárnymi a podpornými aktívami.[18] Primárne aktíva sú tie, ktoré priamo tvoria hodnotu organizácie a slúžia na dosahovanie jej cieľov[19], najmä služby, ktoré organizácia poskytuje, a informácie, s ktorými pri tom pracuje. Podporné aktíva sú všetko, čo umožňuje primárnym aktívam fungovať, teda na ktorých sú závislé jedno alebo viacero primárnych aktív[20], a to technológie, komunikačné prostriedky, programové vybavenie, priestory, ľudské zdroje, dodávatelia a externé systémy či služby. Ak sa organizácia dopustí zanedbania pri podpore, dôsledok sa často prejaví ako zlyhanie primárneho aktíva, teda napríklad ako výpadok služby alebo únik informácií. Pri zodpovednosti potom nebýva kľúčové, že „spadol server", ale že nebola dostupná kritická služba, prípadne došlo k narušeniu integrity alebo dôvernosti informácií. Dobrou metodickou cestou identifikácie primárnych aktív je postupovať od účelu služby. Najprv treba pomenovať službu a jej význam pre organizáciu a až následne identifikovať informácie, ktoré služba spracúva alebo bez ktorých nevie fungovať. Následne sa dá identifikovať, čo je potrebné na zabezpečenie tejto služby: infraštruktúra, sieť, dodávatelia,

[15] International Organization for Standardization. ISO 55000:2014 Asset management — Overview, principles and terminology.

[16] Pod pojmom výrobné a produkčné technológie sa rozumejú technické, softvérové a organizačné prostriedky, ktoré slúžia na riadenie, automatizáciu, monitorovanie a vykonávanie procesov výroby, spracovania alebo distribúcie fyzických produktov, energií, surovín alebo služieb. Ide najmä o systémy operačných technológií (OT), ako sú programovateľné logické automaty (PLC), systémy SCADA, HMI, senzorika, akčné členy a súvisiaca infraštruktúra, ktoré umožňujú kontinuálne a bezpečné fungovanie priemyselných a technologických procesov. (z dôvodovej správy k vyhláške č. 227/2025 Z. z.)

[17] NBÚ: Správa aktív. 7 februára 2024, dostupné na https://www.sk-cert.sk/sk/rady-a-navody/ransomware/pred-incidentom/sprava-aktiv/index.html, rovnako tiež NÚKIB: Stanovení rozsahu řízení kybernetické bezpečnosti, 24. října 2025 Verze 1.0, dostupné na: https://portal.nukib.gov.cz/storage/uploads/2025/10/24/podpurny-material-stanoveni-rozsahu-rizeni-kb_uid_68fb3ad3ad575.pdf

[18] Toto delenie aktív priamo uvádza aj právna úprava v § 6 vyhlášky NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach

[19] Porov. definíciu primárneho aktíva podľa § 2 písm. b) vyhlášky NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach

[20] Porov. definíciu podporného aktíva podľa § 2 písm. c) vyhlášky NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach

prístupové práva, administrátorské roly. Metodiky odporúčajú práve tento prístup, vrátane rozhovorov s vedúcimi útvarov a mapovania väzieb medzi službami a informáciami.[21]

Z praktického hľadiska je užitočné rozlíšiť aspoň tri vrstvy aktív. Prvou sú informačné aktíva, teda údaje a informačné systémy dôležité pre fungovanie organizácie. Príkladom môže byť zákaznícka databáza e-shopu s históriou objednávok alebo dokumentácia k produktu a jeho konfiguráciám. Druhou sú fyzické aktíva, čiže hmotné veci, ktoré organizácia vlastní alebo používa, napr. notebooky zamestnancov, servery v dátovom centre, bezpečnostné kamery, sieťové prvky. Treťou vrstvou sú aktíva, ktoré sa zvyknú podceňovať, a to reputácia, dôvera partnerov, know-how kľúčových ľudí, prístupové práva, schopnosť rozhodovať a koordinovať.

Pri identifikácií aktív právna úprava naviac požaduje, aby boli jednoznačne určené hranice jednotlivých sietí a informačných systémov a tiež rozhrania medzi nimi.[22] Organizácia musí vedieť jasne pomenovať, čo ešte patrí do „jej" systému (a teda čo má riadiť a chrániť) a kde sa jej systém končí. Ak to nevie, vzniká problém pri akejkoľvek otázke zodpovednosti, napríklad pri incidente, pri reklamácii služby, pri kontrole zo strany orgánu verejnej moci alebo pri spore s dodávateľom. Bez jasných hraníc sa totiž nedá presvedčivo tvrdiť, ktoré opatrenia mala organizácia prijať sama a ktoré už boli povinnosťou dodávateľa. „Hranica" sietí a systémov pritom nie je len niečo fyzické ako serverovňa alebo konkrétny router. Vo veľa prípadoch ide o hranicu logickú, napríklad vyčlenená časť cloudového prostredia (tenant), konkrétny sieťový segment (VLAN), oddelená OT sieť vo výrobe alebo integračné rozhranie, cez ktoré spolu komunikujú dva systémy (napr. ERP systém cez API rozhranie). Práve na týchto rozhraniach býva v praxi najviac rizík, nakoľko sa tam prenášajú dáta, delegujú prístupy a vzniká zodpovednosť viacerých subjektov.

S identifikáciou aktív úzko súvisí inventár aktív, teda evidencia. Aktívum sa identifikuje a vedie v evidencii aktív.[23] Evidencia aktív má mať takú mieru presnosti a aktuálnosti, aby podporila tri situácie: každodenné riadenie bezpečnosti, hodnotenie rizík a riešenie incidentu. V praxi by mala organizácia vedieť zistiť, kde sa aktívum nachádza, kto zaň zodpovedá, aké má závislosti a aký dopad má jeho zlyhanie. Preto by inventár mal zachytávať

[21] NÚKIB: Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti, 2022, Dostupné na: https://nukib.gov.cz/cs/infoservis/aktuality/1868-nukib-zverejnil-pruvodce-rizenim-aktiv-a-rizik-dle-vyhlasky-o-kyberneticke-bezpecnosti/

[22] § 6 ods. 2 vyhlášky NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach

[23] § 6 ods. 1 vyhlášky NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach

identitu aktíva, jeho umiestnenie, zodpovednú rolu, väzby na iné aktíva a najmä jeho hodnotu alebo kritickosť pre organizáciu. Inventár nemá byť len zoznam zariadení, ale má obsahovať informácie potrebné na určenie hodnoty aktíva a jeho prepojení, aby organizácia vedela určiť, čo by znamenala jeho strata alebo nefunkčnosť.[24] Už aj právna úprava upravuje minimálne obsahové náležitosti evidencie aktív. Evidencia aktív musí obsahovať najmä identifikáciu a evidenciu a) primárnych aktív, b) podporných aktív, c) vlastníkov aktív, d) zodpovedných osôb za identifikáciu a evidenciu aktív, a jej súčasťou je aj označenie bezpečnostných funkcií podporných aktív alebo odkazy na príslušnú časť bezpečnostnej dokumentácie týchto funkcií.[25]

Pri inventári aktív je dôležité vyjasniť pojem „vlastník aktíva". V bezpečnostnom riadení vlastník neznamená právneho vlastníka v zmysle vlastníckeho práva. Ide o osobu alebo rolu, ktorá nesie zodpovednosť za to, že aktívum má účel, je primerane spravované, rozvíjané a chránené. Vlastník aktíva rozhoduje o požiadavkách, spolupracuje na hodnotení rizík a na výbere opatrení.

Napokon, pri aktívach je kľúčové pracovať s väzbami a závislosťami. Typickým príkladom je dodávateľ, bez ktorého organizácia nevie obnoviť prevádzku po incidente. Preto má inventár a identifikácia aktív zmysel len vtedy, ak zachytáva aj prepojenia. Metodiky na riadenie aktív a rizík výslovne zdôrazňujú evidovanie väzieb medzi primárnymi aktívami a následne identifikáciu podporných aktív v kategóriách technika, komunikácie, softvér, objekty, ľudia, dodávatelia a externé služby.

1.3 Hrozby

Kybernetická hrozba je v európskom aj slovenskom práve chápaná veľmi široko, nakoľko ide o každú potenciálnu okolnosť, udalosť alebo činnosť, ktorá by mohla poškodiť, narušiť alebo inak negatívne ovplyvniť siete a informačné systémy, užívateľov takýchto systémov a iné osoby.[26] Táto definícia je zámerne technologicky neutrálna a neobsahuje vinníka ani konkrétnu techniku útoku, ale pracuje s potenciálom negatívneho dopadu. V praxi to znamená, že hrozbou môže byť rovnako úmyselný útok (napr. vydieranie, sociálne

[24] NBÚ: Správa aktív. 7 februára 2024, dostupné na https://www.sk-cert.sk/sk/rady-a-navody/ransomware/pred-incidentom/sprava-aktiv/index.html.
[25] § 6 ods. 4 a 5 vyhlášky NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach.
[26] Čl. 2 bod 8 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 (Akt o kybernetickej bezpečnosti) – definícia pojmu „kybernetická hrozba".

inžinierstvo), neúmyselná ľudská chyba (napr. neschválená konfigurácia či aktualizácia), zlyhanie technológie (napr. porucha úložiska) aj udalosť prostredia (napr. poškodenie nosičov údajov, alebo IT zariadení prírodnými hrozbami). Pre organizáciu je podstatné, že hrozba vždy mieri na aktíva, pričom môže ohroziť ich dôvernosť, integritu, dostupnosť, prípadne aj kontinuitu služby, bezpečnosť ľudí či reputáciu. Z hľadiska riadenia rizík je dôležité rozlišovať medzi hrozbou a dopadom. Hrozba je zdroj možného problému; dopad je to, čo sa reálne nastane, ak sa hrozba naplní. Rovnaká hrozba pritom môže mať úplne rozdielny dopad podľa toho, ktoré aktívum zasiahne. Napríklad výpadok elektriny môže byť „len" nepríjemnosť pre kancelárske PC, ale kritický incident pre OT prvky alebo pre službu, ktorá má zmluvne garantovanú dostupnosť. Organizácia nemusí vedieť predvídať všetko, ale mala by vedieť predvídať typové hrozby, ktoré sú pre jej aktíva rozumne očakávateľné, a primerane im prispôsobiť opatrenia.

Aby identifikácia hrozieb nebola náhodná a subjektívna, prax aj regulácia tlačia organizácie k systematickému prístupu. Jedným z nástrojov je katalóg hrozieb, teda prakticky zoznam dôvodne očakávateľných hrozieb, ktorý pomáha pokryť typové scenáre a nevynechať niečo len preto, že konkrétny tím nemá skúsenosť s určitým typom útoku alebo zlyhania.[27] Katalóg sa následne „premieta" na konkrétne aktíva a služby. Pre každé aktívum sa uvažuje, ktoré hrozby sú relevantné, aké zraniteľnosti by mohli hrozbu umožniť, aká je pravdepodobnosť a aký dopad by nastal. Užitočné je tiež myslieť na hrozby ako na scenáre, nie ako na izolované položky. V reálnom svete bývajú hrozby reťazené. Napríklad sociálne inžinierstvo môže viesť k získaniu prístupu, ten k nasadeniu malvéru, následne k exfiltrácii dát alebo k vydieraniu, a popritom sa spustí aj incident s dostupnosťou. Pri tvorbe katalógu sa organizácie typicky neopierajú o jediný (univerzálny) zoznam, ale vychádzajú z verejných zdrojov a prispôsobujú ich kontextu vlastnej prevádzky. ENISA napríklad pravidelne publikuje prehľad hrozieb (Threat Landscape) ako prehľad hlavných trendov a typových hrozieb v EÚ, ktorý môže slúžiť ako východisko pre jednotlivé subjekty, vrátane sektorovo špecifických hrozieb.[28] Kľúčové je však doplnenie o vlastnú skúsenosť a dôkazy, ako sú incidenty z minulosti, výsledky auditov, penetračných testov, skenov zraniteľností, výstupy monitoringu, zmenové konania v IT a tiež upozornenia od tretích strán (dodávatelia, CSIRT, komunity).

[27] NBÚ: Verejný katalóg hrozieb (metodické usmernenie k tvorbe a používaniu katalógu hrozieb), Dostupné na: https://www.nbu.gov.sk/katalog-hrozieb-na-stiahnutie/.
[28] ENISA: ENISA Threat Landscape 2025. Dostupné na: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.

Podľa ENISA boli medzi najčastejšie cielene zasiahnuté sektory v EÚ verejná správa, doprava, digitálna infraštruktúra a služby, financie a výroba; zároveň sa uvádza, že kľúčové subjekty tvorili približne 53,7 % zaznamenaných incidentov. Osobitne vyčnieva verejná správa ako najviac cielený sektor (približne 38,2 %), pričom prevažovali nízko-dopadové DDoS kampane (uvádza sa až 94,8 %), no ransomvér mal výrazný dopad najmä na úrovni samospráv. To je typický príklad, prečo pri hodnotení hrozieb nestačí počítať iba počet incidentov, ale treba pracovať aj s dopadom: dva incidenty môžu byť štatisticky „len 2 %", ale právne a prevádzkovo môžu byť existenčné, ak vedú k prerušeniu služby alebo k dlhodobej nedostupnosti.[29] V rovnakom prehľade ENISA poukazuje aj na stabilnú prítomnosť štátom podporovaných aktivít voči členským štátom EÚ (najmä kyberšpionáž zameraná na verejnú správu) a na rastúce zásahy typu FIMI (Foreign Information Manipulation and Interference), ktoré čoraz častejšie cielia na publikum v EÚ. Zároveň sa uvádza, že objem incidentov v EÚ výrazne spôsobuje hacktivizmus, typicky cez DDoS kampane, pričom len malá časť viedla k reálnemu prerušeniu služby (približne 2 %).

APT (Advanced Persistent Threat) je označenie pre dlhodobú, cielenú a typicky dobre financovanú útočnú aktivitu, ktorá sa vyznačuje „perzistenciou", teda snahou udržať si prístup do prostredia obete čo najdlhšie, často za účelom špionáže, prípravy sabotáže, alebo strategického získavania informácií. Podľa NIST ide o aktéra so sofistikovanou úrovňou odborných znalostí a značnými zdrojmi, ktorý mu umožňuje prostredníctvom viacerých rôznych útočných vektorov (napr. kybernetických, fyzických a klamlivých) vytvárať príležitosti na dosiahnutie svojich cieľov, ktorými je zvyčajne etablovať sa a rozširovať svoju prítomnosť v rámci IT infraštruktúry organizácií za účelom neustáleho získavania informácií a/alebo podkopávania či bránenia kritickým aspektom misie, programu alebo organizácie, alebo sa dostať do pozície, aby tak urobil v budúcnosti.[30] ENISA pracuje s pojmom „state-nexus" a uvádza ako príklady aktívnych skupín v EÚ napr. APT28, APT29 či Sandworm, pričom zdôrazňuje ich zameranie najmä na verejnú správu, obranu a telekomunikácie. Označenie *state-nexus* (napojenie na štát) znamená, že existujú dôvodné indície, že útok je priamo riadený štátnym aktérom alebo aspoň štátom podporovaný či tolerovaný (napr.

[29] ENISA Threat Landscape 2025 Booklet. Dostupné na: https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025%20Booklet.pdf.
[30] NIST: Definícia APT. Dostupné na: https://csrc.nist.gov/glossary/term/advanced_persistent_threat.

financovaním, zadávaním úloh, poskytovaním infraštruktúry alebo tým, že útočníci pôsobia bez postihu na území daného štátu).

Označenia typu APT28/APT29/Sandworm sú pracovné názvy používané bezpečnostnou komunitou (rôzni výrobcovia ich vedia volať aj inak) a pripísanie štátnym štruktúram je spravidla otázkou atribúcie, teda vyhodnotenia indícií.

APT28 (Fancy Bear) je pomenovanie používané pre dlhodobo pôsobiaceho aktéra spájaného s ruskou vojenskou spravodajskou službou GRU, konkrétne s jej jednotkou 26165. Typicky ide o kybernetickú špionáž a operácie „hack-and-leak" (preniknutie a selektívne zverejnenie alebo manipulácia informácií), často proti štátnym inštitúciám, obrannému sektoru, politickým subjektom či médiám.[31]

APT29 (Cozy Bear) sa najčastejšie opisuje ako špionážny aktér spájaný s ruskou civilnou spravodajskou službou SVR. V praxi sa tento názov používa pre kampane, ktoré sú skôr tiché, dlhodobé a zamerané na získavanie prístupu k citlivým informáciám (napr. štátna správa, diplomacia, výskum). Vlády USA a Spojeného kráľovstva jej pripísali kompromitáciu SolarWinds.[32]

APT44 (Sandworm) sa spája s ruskou GRU jednotkou 74455 a je známy tým, že popri špionáži robí aj deštruktívne a rušivé operácie, najmä voči kritickej infraštruktúre a Ukrajine (napr. útoky na energetiku). Jednotke 74455 sa pripisujú aj operácie ako Industroyer a NotPetya.[33]

DDoS (Distributed Denial of Service) je útok na dostupnosť, ktorého cieľom je zahltiť systém alebo sieť tak, aby neboli schopné poskytovať službu legitímnym používateľom. Distribuovaný (Distributed) znamená, že útok prichádza z veľkého množstva zdrojov (často kompromitovaných zariadení tzv. botov), čo komplikuje obranu aj atribúciu. DDoS je typický príklad hrozby s vysokou frekvenciou a často relatívne nízkym dopadom na údaje (nejde primárne o získanie údajov), no s potenciálne vysokým dopadom na dostupnosť a kontinuitu služieb, zmluvné záväzky a reputáciu.

[31] Viac informácií je dostupných na https://attack.mitre.org/groups/G0007/ a tiež Policy paper Profile: GRU cyber and hybrid threat operations, https://www.gov.uk/government/publications/profile-gru-cyber-and-hybrid-threat-operations/profile-gru-cyber-and-hybrid-threat-operations.

[32] Viac informácií je dostupných na https://attack.mitre.org/groups/G0016/.

[33] Policy paper Profile: GRU cyber and hybrid threat operations. Dostupné na: https://www.gov.uk/government/publications/profile-gru-cyber-and-hybrid-threat-operations/profile-gru-cyber-and-hybrid-threat-operations.

Hacktivizmus je ideologicky motivovaná kybernetická aktivita, ktorej cieľom je politický alebo spoločenský efekt (tlak, demonštrácia, narušenie symbolického cieľa), nie priamo finančný zisk. Prakticky sa hacktivizmus často prejavuje práve DDoS útokmi alebo zverejňovaním získaných dát, pričom jeho „úspech" sa meria mediálnym dosahom, nie technickou sofistikovanosťou.

Ransomvér je druh útoku, pri ktorom útočníci vyvíjajú a/alebo používajú škodlivý softvér (malvér), na zamedzenie prístupu k údajom, systémom alebo sieťam a požadujú zaň výkupné. Medzi bežné metódy útoku patrí šifrovanie údajov, exfiltrácia údajov a narušenie prevádzky obete. Útoky často zahŕňajú viac ako jednu metódu a môžu zahŕňať hrozbu zverejnenia údajov poškodeného.[34]

Útočníci sa často zameriavajú na právnické osoby s vysokou hodnotou alebo právnické osoby, o ktorých si myslia, že je pravdepodobnejšie, že zaplatia výkupné, aby obnovili obchodné operácie alebo sa vyhli kontrole. Selektívne sa zameriavajú aj na právnické osoby pôsobiace v dodávateľských reťazcoch typu just-in-time, u ktorých je pravdepodobnejšie, že budú mať vyššie náklady na výpadok, ako aj na kritickú infraštruktúru alebo na tie, ktoré majú citlivé alebo cenné informácie. Útočníci môžu vyhodnotiť, že tieto právnické osoby majú v porovnaní s ostatnými väčšiu tendenciu platiť výkupné.

Ransomvér ako služba (RaaS) označuje protiprávny obchodný model, v rámci ktorého útočníci poskytujú balíky ransomvérového softvéru na Dark webe alebo externe zabezpečujú prvky ransomvérových útokov vrátane distribúcie škodlivého softvéru, počiatočnej kompromitácie siete obete, exfiltrácie údajov alebo vyjednávania o výkupnom pre pridružené spoločnosti výmenou za poplatok a/alebo percento z výkupného. Páchatelia si môžu zakúpiť aj odcudzené údaje (credentials) na prístup k systémom poškodeného a ich zneužitie, čo umožní distribúciu ransomvéru, a môžu tiež získať spravodajské informácie týkajúce sa konkrétnych odvetví v konkrétnych jurisdikciách, aby sa mohli zamerať na svoje ciele a maximalizovať účinnosť svojho útoku. Model RaaS znížil náklady a potrebné technické znalosti na vykonávanie útokov, čím sa znížili bariéry vstupu a umožnilo sa menej sofistikovanejším zločincom vykonávať ransomvérové útoky.

[34] Financial Action Task Force (FATF) Report: Countering Ransomware Financing. Marec 2023. online. dostupné na: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Countering-Ransomware-Financing.pdf.coredownload.pdf.

V rámci postupu útočníkov po úspešnom prieniku do systému a siete obete sa vyvinulo niekoľko spôsobov či úrovní vydierania tejto obete.

Dvojité vydieranie (*double-extortion*) označuje postup, pri ktorom útočníci pred zašifrovaním údajov obete exfiltrujú údaje a potom hrozia zverejnením odcudzených údajov, ak nebudú splnené požiadavky na výkupné. Táto hrozba zverejnenia dopĺňa hrozbu týkajúcu sa napadnutého systému. Táto taktika môže na poškodených vyvinúť ďalší tlak, aby zaplatili požiadavky na výkupné, aj keď sa im podarí obnoviť prevádzku.

Trojité vydieranie (*triple-extortion*) sa vzťahuje na postup, pri ktorom útočníci požadujú peniaze nielen od poškodeného, ktorý bol prvým cieľom, ale aj od poškodených, ktorí by mohli byť ovplyvnená zverejnením údajov pôvodného (cieľového) poškodeného, ako sú chránené zdravotné informácie, osobné údaje, údaje k účtu a duševné vlastníctvo.

Viacnásobné vydieranie (*multiple-extortion*) sa vzťahuje na postupy, ktoré zahŕňajú viac ako dva spôsoby vydierania. Vychádza z dvojitého vydierania pomocou šifrovania a exfiltrácie, ale zahŕňa aj ďalšie nátlakové taktiky, ako je distribuované odmietnutie služby (DDoS), kontaktovanie zákazníkov poškodených a narušenie ich infraštruktúry.

Čoraz viac prípadov, kde za ransomvérovým útokom je primárny dôvod nenápadná exfiltrácia dát. V týchto prípadoch je požiadavka na výkupné často úplne nepodstatná. Takéto krytie ransomvérom je využívané štátnymi hráčmi resp. skupinami sponzorovaným štátmi, či zločineckými skupinami zameranými na priemyselnú špionáž.[35]

1.4 Zraniteľnosti

Zraniteľnosť je správanie alebo súbor podmienok prítomných v systéme, produkte, komponente alebo službe, ktoré porušujú implicitné alebo explicitné bezpečnostné politiky. Technická norma STN EN ISO/IEC 27000 definuje zraniteľnosť ako slabinu aktíva alebo opatrenia, ktorú môže využiť jedna alebo viaceré hrozby.[36] Smernica NIS2 definuje zraniteľnosť ako slabinu, náchylnosť alebo chybu produktov alebo služieb IKT, ktorú môže využiť kybernetická hrozba.[37] Podobne ZoKB podobne definuje zraniteľnosť ako akýkoľvek

[35] CONNOLLY L.Y., WALL, D.S., LANG M., ODDSON, B., An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability, *Journal of Cybersecurity*, Volume 6, Issue 1, 2020, tyaa023. online. dostupné na: https://doi.org/10.1093/cybsec/tyaa023.

[36] STN EN ISO/IEC 27000 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník (ISO/IEC 27000: 2018) článok 3 bod 3.77.

[37] Smernica NIS2, článok 6 bod 15.

nežiaduci stav alebo chybu technického prostriedku alebo programového prostriedku, alebo nedostatok procesu vrátane nesprávnej bezpečnostnej konfigurácie, ktorá môže byť zneužitá kybernetickou hrozbou.[38] Pojem zraniteľnosť pritom nie je iba chyba v zdrojovom kóde počítačového programu. V praxi sem patria aj zlé konfigurácie (napr. zbytočne otvorené porty, prednastavené heslá), chýbajúce bezpečnostné aktualizácie, nesprávne nastavené práva, ale aj chýbajúce alebo nesprávne implementované bezpečnostné opatrenia (napr. neexistujúce riadenie záplat, nesprávne nastavená politika hesiel, nestatočne vynucované plnenie politík).

Zraniteľnosť sama osebe ešte nie je incident. Zraniteľnosť je potenciál, kdežto incident je uskutočnenie (materializácia) rizika, typicky vtedy, keď hrozba zraniteľnosť skutočne zneužije a spôsobí negatívny následok. Preto je potrebné odlišovať zneužiteľnosť a dopad. Zneužiteľnosť odpovedá na otázku „ako ľahko sa dá slabina zneužiť" (vyžaduje útočník prístup do siete? potrebuje autentifikáciu? existuje verejne dostupný exploit?), kým dopad odpovedá na otázku „čo sa stane, keď sa zneužije" (únik dát, zastavenie výroby, kompromitácia účtov, výpadok služby). Nie každá zraniteľnosť vedie k povinnosti oznamovania incidentu, k nároku na náhradu škody alebo k porušeniu zmluvy, ale môže zakladať povinnosť prijať primerané preventívne opatrenia (napr. aplikovanie záplaty, mitigácie, obmedzenie prístupov, dočasné vypnutie funkcie). Na úrovni regulácie produktov je zaujímavé, že Akt o kybernetickej odolnosti (CRA) používa pojem „aktívne zneužívaná zraniteľnosť", teda zraniteľnosť, v prípade ktorej existuje spoľahlivý dôkaz, že škodlivý subjekt ju zneužil v systéme bez povolenia vlastníka systému.[39] Výrobcovia budú od 11. septembra 2026 povinní prostredníctvom jednotnej oznamovacej platformy informovať jednotku pre riešenie počítačových bezpečnostných incidentov (ďalej len „CSIRT") určenú za koordinátora, ako aj agentúru ENISA o aktívne zneužívaných zraniteľnostiach.

V praxi sa organizácie pri identifikácii zraniteľností neopierajú o jednu databázu, ale o viac zdrojov. V globálnom meradle je základom identifikátor (Common Vulnerabilities and Exposures, CVE), štandardizované označovanie zraniteľností prevádzkované organizáciou MITRE. Na rýchle porovnávanie závažnosti sa používa skórovací systém (Common Vulnerability Scoring System, CVSS), ktoré je síce technické, ale má jasnú právne použiteľnú logiku, rozkladá zraniteľnosť na parametre súvisiace so spôsobom útoku a s dopadom, a

[38] § 3 ods. 1 písm. q) ZoKB.
[39] Článok 3 ods. 42 CRA.

výsledkom je porovnateľné číslo/slovný rating. V posledných rokoch je pre užitočný aj katalóg známych zneužívaných zraniteľností (Known Exploited Vulnerabilities, KEV) od americkej CISA, ktorý obsahuje už reálne zneužívané zraniteľnosti. Európskou odpoveďou na fragmentáciu údajov je Európska databáza zraniteľností (European Vulnerability Database, EUVD), ktorá má ambíciu poskytovať agregovať informácie o zraniteľnostiach z viacerých zdrojov, vrátane CSIRT komunít, a podporovať rýchlu orientáciu v tom, čo je relevantné pre európsky trh a regulované subjekty. EUVD nie je len ďalšia databáza, ale súčasť širšej európskej infraštruktúry kybernetickej bezpečnosti, pričom pomáha prepojiť technickú realitu (zraniteľnosti) s požiadavkami regulácie (oznamovacie povinnosti podľa NIS2/ZoKB, povinnosti výrobcu podľa CRA). Ako ilustráciu možno vnímať aj to, že EUVD používa vlastné identifikátory (EUVD-...), napr. záznam označený EUVD-2026-3550, ktoré slúžia na jednotné odkazovanie v rámci databázy a jej väzieb na ďalšie zdroje. Aby sa predišlo duplicite úsilia a podporilo sa vzájomné dopĺňanie, ENISA úzko spolupracuje s MITRE a európskymi, ako aj mimoeurópskymi prevádzkovateľmi systému CVE. V tejto súvislosti ENISA ponúka služby registrácie zraniteľností, keďže sa stala autoritou pre prideľovanie číslovania CVE (CVE Numbering Authority, CNA) so zameraním na zraniteľnosti v IT produktoch objavené alebo nahlásené európskym tímami CSIRT na účely koordinovaného zverejňovania.

1.5 Riziko a riadenie rizík

Bezpečnosť aktív stojí na tom, že organizácia udržiava riziko na prijateľnej úrovni. Nejde o nulové riziko, ale o riadené riziko, to znamená, že identifikované riziká sa priebežne znižujú, menia alebo prijímajú tak, aby negatívne prejavy hrozieb neohrozili ciele organizácie a fungovanie jej služieb. Zmyslom riadenia rizík je mať preukázateľný proces, ktorý určuje, čo je pre organizáciu dôležité, čo to ohrozuje, aké sú možné následky a aké opatrenia sa zavedú. Riziko sa vo všeobecnosti chápe ako vplyv neistoty na ciele.[40] V kybernetickej bezpečnosti sa riziko viaže na možné budúce straty spôsobené narušením dôvernosti, integrity, dostupnosti alebo sledovateľnosti (traceability) informačných aktív organizácie. Takéto straty môžu byť priame finančné (napr. výpadok, náklady na obnovu, sankcie) aj nepriame (napr. reputačné škody, strata dôvery, odchod zákazníkov). Výraz „kybernetické bezpečnostné riziko" sa v

[40] NBÚ: Metodika analýzy rizík kybernetickej bezpečnosti, verzia 2.0, 2025, Dostupné na: https://www.nbu.gov.sk/data/att/3446.pdf str. 4.

praxi používa aj ako ekvivalent „IT rizika", ak je zrejmé, že ide o riziká viazané na siete a informačné systémy. Riadenie rizík je cyklický proces, ktorý sa opakuje a aktualizuje. Základný model vychádza z prístupov technickej normy ISO/IEC 27005 a v praxi sa opisuje piatimi nadväzujúcimi krokmi: stanovenie kontextu, posúdenie rizík (v tomto texte označované aj ako „analýza rizika"), ošetrovanie rizík, komunikácia o rizikách a monitorovanie s preskúmaním.[41] Cyklickosť je dôležitá, pretože sa mení technológia, dodávatelia, hrozby, biznis aj spôsob používania systémov; rizikový obraz sa preto prirodzene posúva.

Stanovenie kontextu rizika je prvý krok, ktorý určuje hranice a pravidlá celej analýzy. Organizácia v ňom nastaví rozsah (ktoré služby, systémy, lokality, procesy a dodávateľské väzby sú v analýze), určí kritériá rizika (čo je ešte prijateľné, čo už nie) a pomenuje vnútorné a vonkajšie parametre, ktoré treba zohľadniť (napr. regulačné požiadavky, zmluvné záväzky, tolerancia výpadku, požiadavky zákazníkov). Do kontextu patrí identifikácia aktív a ich zodpovednosti, zraniteľnosti, potenciálne hrozby, odhad následkov, odhad pravdepodobností a prehľad existujúcich opatrení.

Analýza rizika sa dá robiť rôznymi prístupmi podľa toho, z čoho organizácia vychádza a aké informácie má k dispozícii. Prístup orientovaný na hrozby začína identifikáciou zdrojov hrozieb a udalostí, rozvíja scenáre (ako by k škodlivej udalosti mohlo dôjsť) a následne hľadá zraniteľnosti, ktoré sú v danom scenári relevantné. Prístup orientovaný na aktíva a dopady začína tým, čo je kritické pre činnosť organizácie (služby, dáta, systémy), a následne hodnotí dôsledky narušenia a hľadá zraniteľnosti, ktoré môžu viesť k závažným dopadom. Prístup orientovaný na zraniteľnosti vychádza zo známych slabín alebo predispozičných podmienok (napr. neaktualizované systémy, chybné konfigurácie, zistenia skenovania), identifikuje ich zneužiteľnosť a potom dopĺňa, aké hrozby a scenáre sú na ne naviazané. V praxi sa tieto prístupy často kombinujú: organizácia môže mať zároveň katalóg hrozieb, inventár aktív a pravidelné výstupy zo skenovania zraniteľností. Výsledok analýzy rizika treba vyjadriť spôsobom, ktorý umožní rozhodovanie. Na to sa používajú tri základné metódy hodnotenia rizika: kvalitatívna, kvantitatívna a semikvantitatívna. Kvalitatívna metóda pracuje so slovnými opisnými škálami (napr. nízke–stredné–vysoké), je rýchla a vhodná pri nižšej vyspelosti riadenia rizík, no nesie vyššiu mieru subjektivity. Kvantitatívna metóda sa snaží

[41] Tamže. str. 9.

vyjadriť riziko číselne a opiera sa o dáta a výpočty, umožňuje finančné modelovanie, ale je náročná na dostupnosť kvalitných údajov. Semikvantitatívna metóda kombinuje slovné hodnotenia s číselnými stupnicami tak, aby bola výsledná škála interpretovateľná, porovnateľná a použiteľná v tímovej práci; zároveň však stále zachováva určitú mieru subjektivity.

Ošetrovanie rizika je fáza, v ktorej sa rozhodne, čo sa s rizikom urobí. Bežne ide o voľbu medzi znížením rizika zavedením opatrení, vyhnutím sa riziku zmenou procesu alebo architektúry, prenesením rizika (typicky zmluvne alebo poistením, vždy len v určitom rozsahu) a prijatím rizika, ak spĺňa kritériá prijateľnosti. Riadenie rizík tu musí zostať preukázateľné, a teda ku každému významnému riziku má byť jasné, kto je zaň zodpovedný, aké opatrenia sa prijali, v akom termíne a aký zvyškový (reziduálny) rizikový stav ostáva.

Komunikácia o rizikách a monitorovanie s preskúmaním sú prvky, ktoré z procesu robia riadenie, nie jednorazové cvičenie. Komunikácia zabezpečuje, že rozhodnutia o rizikách sú zrozumiteľné naprieč organizáciou a že sa vedia premietnuť do rozpočtu, priorít a zodpovedností. Monitorovanie a preskúmanie zasa znamená, že riziká a opatrenia sa priebežne revidujú podľa zmien v prostredí: zmeny systémov, nové zraniteľnosti, incidenty, zmeny dodávateľov, výsledky auditov a testovania, alebo zmeny v kritickosti služieb. V praxi sa tak riadenie rizík stáva kontinuálnym mechanizmom, ktorý prepája aktíva, hrozby, zraniteľnosti a bezpečnostné opatrenia do jedného rozhodovacieho rámca.

Analýza rizík po transpozícii smernice NIS2 do ZoKB získala kľúčové postavenie vo väzbe na rozsah a spôsob prijímania bezpečnostných opatrení. Každý prevádzkovateľ základnej služby je povinný na základe analýzy rizík ošetrovať tie riziká, ktoré sú nad úrovňou vopred definovaného akceptovaného rizika. Platí, že prevádzkovateľ základnej služby je povinný v závislosti od vykonanej analýzy rizík prijať, dodržiavať a vykonávať všeobecné bezpečnostné opatrenia[42] a bezpečnostné opatrenia sú realizované na základe vykonanej analýzy rizík.[43] Príloha č. 1 k vyhláške č. 227/2025 Z. z. definuje katalóg bezpečnostných opatrení, z ktorých si môže prevádzkovateľ základnej služby po analýze rizík vybrať, či sú pre neho relevantné alebo nie.

[42] §19 ods. 1 ZoKB.
[43] § 20 ods. 1 ZoKB.

1.6 Bezpečnostné opatrenia

Cieľom každej organizácie je minimalizácia rizík. Opatrenia, ktoré upravujú riziko označujeme ako **bezpečnostné opatrenia**. Tie môžu zahŕňať *„akýkoľvek proces, politiku, zariadenie, prax alebo iné akcie, ktoré menia bezpečnostné riziko."*[44] Podľa § 20 ods. 1 ZoKB sa bezpečnostnými opatreniami rozumejú úlohy, procesy, role a technológie v organizačnej, personálnej, fyzickej a technologickej oblasti, ktorých cieľom je dosiahnutie, zaručenie a udržanie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov a operačných technológií.

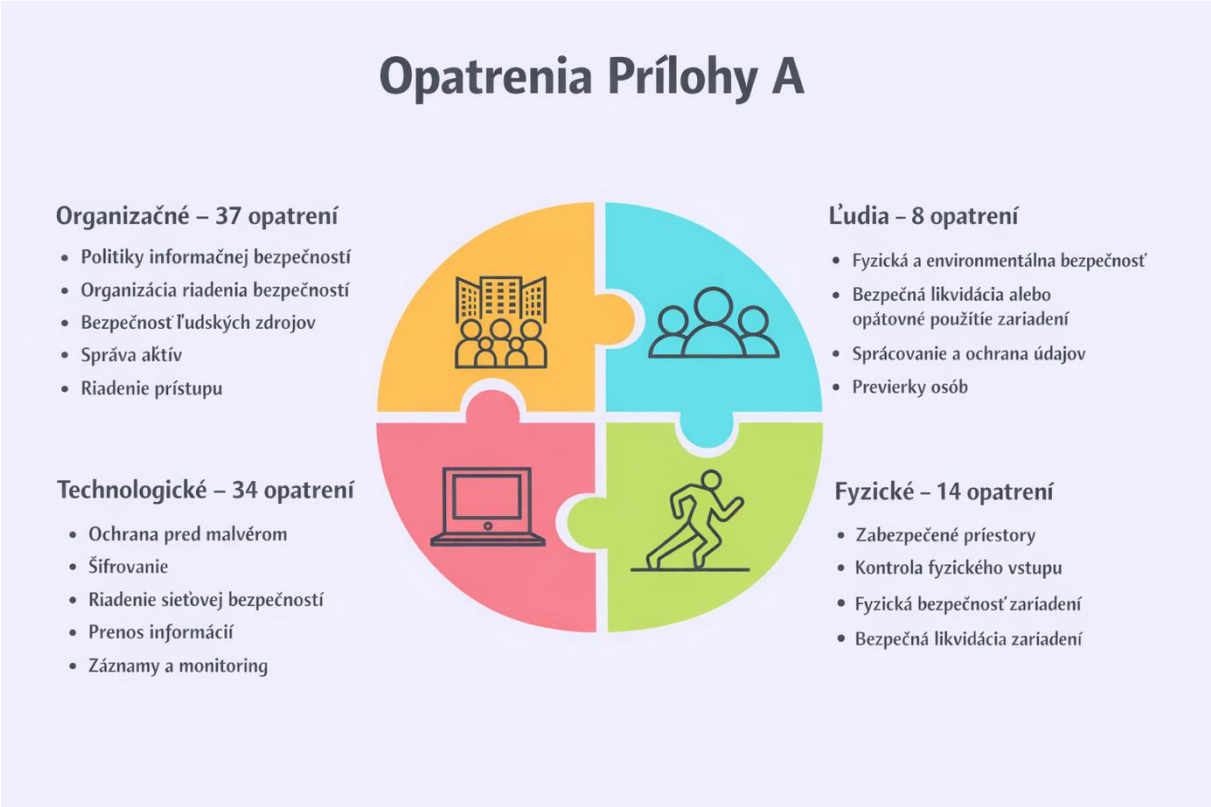
Príloha A normy STN EN ISO/IEC 27001: 2023 obsahuje 4 tematické kategórie opatrení (controls) pre informačnú bezpečnosť, ktoré nahradili predchádzajúce oblasti, a poskytuje zoznam referenčných cieľov a opatrení, ktoré organizácie zvažujú pri implementácii systému riadenia informačnej bezpečnosti (ISMS) na zvládanie rizík, pričom ISO 27002 poskytuje detailné usmernenia k ich implementácii.

Hlavné tematické kategórie opatrení v norme STN EN ISO/IEC 27001: 2023 sú:

1. Osoby (People Controls): Opatrenia zamerané na ľudský faktor a povedomie o bezpečnosti.
2. Fyzické (Physical Controls): Zabezpečenie fyzických priestorov a zariadení.
3. Technologické (Technological Controls): Zabezpečenie systémov, aplikácií a sietí.
4. Organizačné (Organizational Controls): Politiky, procesy a riadenie bezpečnosti v rámci organizácie.

Norma ISO 27001 obsahuje normatívnu Prílohu A s kontrolnými cieľmi a opatreniami, ktoré sú záväzné v kontexte implementácie ISMS. STN EN ISO/IEC 27002: 2023 je samostatná norma slúžiaca ako usmernenie (guideline) pre implementáciu týchto opatrené, ponúkajúca detailné návody a rady pre manažérov informačnej bezpečnosti, aby sa zabezpečilo komplexné pokrytie rizík. V novej verzii došlo k zlúčeniu predchádzajúcich 14 oblastí do 4 spomínaných tematických skupín, čo zjednodušuje implementáciu.

[44] International Organization for Standardization, International Electrotechnical Commission. ISO/IEC 27000: 2018 - Information technology—Security techniques—Information security management systems—Overview and vocabulary.



Obrázok č. 2: Opatrenia Prílohy A STN EN ISO/IEC 27001: 2023.[45]

Bezpečnostné opatrenia v prílohe č. 1 k vyhláške č. 227/2025 Z. z. vychádzajú z normy STN EN ISO/IEC 27001: 2023, resp. z jej prílohy A. Zároveň však európska a slovenská právna úprava vytvára rôzne kategórie bezpečnostných opatrení, ktoré môžeme rozdeliť do troch základných skupín, a to minimálne, všeobecné a sektorové.

Minimálne bezpečnostné opatrenia sú bezpečnostné opatrenia podľa § 20 ods. 4 podľa ktorého bezpečnostné opatrenia musia zahŕňať najmenej:

a) určenie manažéra kybernetickej bezpečnosti, ktorý je pri návrhu, prijímaní a presadzovaní bezpečnostných opatrení nezávislý od štruktúry riadenia prevádzky a vývoja služieb informačných technológií a ktorý spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti,

b) detekciu kybernetických bezpečnostných incidentov,

c) evidenciu kybernetických bezpečnostných incidentov,

d) postupy riešenia a riešenie kybernetických bezpečnostných incidentov,

e) určenie kontaktnej osoby pre prijímanie a evidenciu hlásení,

[45] Vygenerované nástrojom UI (ChatGPT).

f) pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálneho systému včasného varovania,

g) určenie a pridelenie úloh, rolí a zodpovednosti podľa podmienok prevádzkovateľa základnej služby a zabezpečenie primeraného vzdelávania a preškoľovania pre všetky zavedené roly,

h) určenie konkrétnej osoby alebo konkrétnych osôb zodpovedných za schvaľovanie bezpečnostných opatrení, dohľad, kontrolu a audit, zabezpečenie primeranosti zdrojov na riadenie kybernetickej bezpečnosti a za vzdelávanie,

i) vzdelávanie a budovanie bezpečnostného povedomia v oblasti kybernetickej bezpečnosti.

Všeobecné bezpečnostné opatrenia pre oblasti kybernetickej bezpečnosti podľa § 20 ods. 2 ZoKB sa prijímajú aspoň pre

a) organizáciu a riadenie informačnej bezpečnosti a kybernetickej bezpečnosti,

b) správu zraniteľností a kybernetických hrozieb,

c) správu aktív a riadenie kybernetických hrozieb a rizík,

d) riadenie udalostí a kybernetických bezpečnostných incidentov,

e) riadenie kontinuity činností, zálohovanie, obnovu systémov po havárii a krízové riadenie,

f) bezpečnosť pri nadobúdaní, vývoji a údržbe siete, informačných systémov, aplikácií a konfigurácií,

g) postupy posudzovania účinnosti opatrení, riadenie súladu a kontrolné činnosti,

h) kryptografické opatrenia a zásady používania kryptografie,

i) bezpečnosť a spôsobilosti ľudských zdrojov,

j) správu identít a prístupov,

k) bezpečnosť pri prevádzke sietí a informačných systémov,

l) ochranu proti škodlivému kódu a nežiaducemu obsahu,

m) systémovú bezpečnosť, sieťovú bezpečnosť a komunikačnú bezpečnosť,

n) monitorovanie, zaznamenávanie a hlásenie udalostí,

o) fyzickú bezpečnosť, bezpečnosť prostredia a správu koncových zariadení,

p) ochranu záznamov, súkromia a označovanie informácií,

q) dodávateľský reťazec,

r) obstarávanie a využívanie certifikovaných produktov IKT, služieb IKT a procesov IKT.

Vyššie uvedený rozsah bezpečnostných opatrení je ďalej detailne vymedzený v prílohe č. 1 k vyhláške č. 227/2025 a diferencuje sa podľa toho, či ide o prevádzkovateľa

základnej služby podľa § 17 ZoKB alebo prevádzkovateľa kritickej základnej služby podľa § 18 ZoKB, a taktiež sa rozlišuje, či ide o informačné a komunikačné technológie (IKT) alebo ide o operačné technológie (OT). Bezpečnostné opatrenia sa následne prijímajú a realizujú v rozsahu a spôsobom podľa tejto vyhlášky, a na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu.

Stratégia kybernetickej bezpečnosti je kľúčovým dokumentom prevádzkovateľa základnej služby, ktorá určuje jej dlhodobé smerovanie a najmä záväzok vedenia prevádzkovateľa základnej služby k podpore kybernetickej bezpečnosti. Bezpečnostné politiky sa schvaľujú pre jednotlivé oblasti relevantné pre daného prevádzkovateľa základnej služby. Bezpečnostné politiky by mali definovať základný rámec postupov, zodpovedností a princípov, uplatňovaných pre jednotlivé oblasti u prevádzkovateľa základnej služby. Obsahom dokumentácie je aj analýza rizík a najmä vyjadrenie úrovne akceptovateľného rizika, ktoré sa prevádzkovateľ základnej služby rozhodol prijať. Poznanie zvyškového rizika je zásadné pre prevádzkovateľa základnej služby z dôvodu, aby prevádzkovateľ základnej služby vedel určiť, či a v akej miere prijaté a aplikované bezpečnostné opatrenia znížili pôvodné riziko a teda či boli efektívne vynaložené zdroje na ošetrenie rizík. Stratégia kybernetickej bezpečnosti, ako aj bezpečnostné politiky majú byť nielen schválené, ale majú podliehať aj pravidelnému preskúmavaniu a revízii, čím sa má docieliť aktuálnosť bezpečnostnej dokumentácie.

Súčasťou bezpečnostnej dokumentácie, ako centrálneho zdroja informácií, je aj zadokumentovanie všetkých bezpečnostných opatrení, ktoré boli u prevádzkovateľa základnej služby prijaté na ošetrenie rizika, rovnako ako uvedenie dôvodu, prečo niektoré opatrenia neboli prijaté. Uvedenie dôvodu pre neprijatie bezpečnostných opatrení je kľúčové na účel vykonania kontroly alebo vykonania auditu, aby bolo zrejmé, že prevádzkovateľ základnej služby neopomenul na existenciu daného bezpečnostného opatrenia, ale tieto bezpečnostné opatrenia prehodnotil a rozhodol sa ich neprijať. Pod neprijatím opatrenia sa rozumie aj iný spôsob pokrytia rizika ako napríklad prenesenie rizika na tretiu stranu alebo skončenie vykonávania danej činnosti. Súčasťou zadokumentovania rozsahu a spôsobu aplikovaných bezpečnostných opatrení má byť uvedená aj infraštruktúra, architektúra a topológia prostredia organizácie, majúceho vplyv na kybernetickú bezpečnosť. Bezpečnostná dokumentácia obsahuje aj poslednú záverečnú správu o výsledkoch auditu kybernetickej bezpečnosti, ktorý dáva komplexný obraz o úrovni zabezpečenie kybernetickej

bezpečnosti u prevádzkovateľa základnej služby a tiež poukazuje na potrebu zlepšovania prijatých bezpečnostných opatrení.

V prípade, ak existujú iné dokumenty, ktorých obsahom je zabezpečiť bezpečnosť a ochranu sietí a informačných systémov, informácií alebo údajov, ktorými je prevádzkovateľ základnej služby povinný disponovať a ktoré môžu ovplyvniť stratégiu kybernetickej bezpečnosti prevádzkovateľa základnej služby alebo iným spôsobom vplývajú na kybernetickú bezpečnosť prevádzkovateľa základnej služby majú byť tiež súčasťou bezpečnostnej dokumentácie (napríklad dokumentácia pri posudzovaní vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov).

Schválením bezpečnostnej dokumentácie a najmú Stratégie kybernetickej bezpečnosti sa štatutárny orgán zaväzuje k podpore a budovaniu kybernetickej bezpečnosti vo svojej organizácií.

Cieľom právnej úpravy je, aby prevádzkovateľ základnej služby prijímal všetky bezpečnostné opatrenia. Na základe výstupov analýzy rizík si však môže zhodnotiť z hľadiska rizík a efektívnosti opatrení, prečo dané opatrenie neprijal. Predmetom auditu kybernetickej bezpečnosti je potom aj overenie potreby prijať bezpečnostné opatrenia, ktoré sa prevádzkovateľ základnej služby rozhodol v zmysle postupu ktorý vyhláška umožňuje, neprijať.

Príloha č. 1 k vyhláške definuje katalóg bezpečnostných opatrení, z ktorých si môže prevádzkovateľ základnej služby po analýze rizík vybrať, či sú pre neho relevantné alebo nie. V prípade, ak sa prevádzkovateľ nachádza v sektore, ktorý prijal svoju vlastnú reguláciu bezpečnostných opatrení (tzv. sektorové bezpečnostné opatrenia), tak obsah bezpečnostných opatrení je definovaný touto reguláciou a prevádzkovateľ základnej služby nie je povinný prijímať opatrenia podľa tejto vyhlášky (okrem bezpečnostných opatrení podľa § 20 ods. 4 ZoKB), ak osobitný predpis neustanovuje inak. Prevádzkovateľ základnej služby pri určovaní rozsahu prijímaných bezpečnostných opatrení vychádza z identifikácie aktív a následnej analýzy a hodnotenia rizík, pričom uplatňuje bezpečnostné opatrenia podľa toho, či ide o informačné a komunikačné technológie alebo operačné technológie a zároveň si ich vyberá podľa toho, či ide o prevádzkovateľa základnej služby alebo prevádzkovateľa kritickej základnej služby.

Príkladom **sektorových bezpečnostných opatrení,** ktoré vyplývajú z osobitných právnych predpisov, sú napríklad Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554

o digitálnej prevádzkovej odolnosti finančného sektora (DORA), zákon č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe v znení neskorších predpisov (ZoITVS), vyhláška MIRRI, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy,[46] vyhláška Úradu jadrového dozoru Slovenskej republiky č. 430/2011 Z. z. o požiadavkách na jadrovú bezpečnosť.

1.7 Overovanie úrovne kybernetickej bezpečnosti

Overovanie úrovne kybernetickej bezpečnosti má všeobecný účel, a to získať objektívnu informáciu o stave ochrany aktív. Ide najmä o zhodnotenie súladu aktuálneho stavu bezpečnosti so stanovenými bezpečnostnými cieľmi a o posúdenie, či prijaté opatrenia zodpovedajú určenému rozsahu opatrení a či sú implementované opatrenia účinné. Overovanie zároveň umožňuje posúdiť bezpečnostnú architektúru (security by design), bezpečnosť aplikácií a nastavení (security by default), vyspelosť procesu riadenia bezpečnosti, identifikovať zraniteľnosti a hrozby, stanoviť úrovne rizík a atestovať spôsobilosti a súlad v oblasti kybernetickej bezpečnosti. V procese overovania úrovne bezpečnosti sa overované entity a prvky všeobecne označujú ako „objekty posúdenia" (assessment objects). Subjekt sa môže uistiť o požadovanej úrovni kybernetickej bezpečnosti štyrmi základnými prístupmi: *posúdením, testovaním, auditom* alebo *certifikáciou*.

Posudzovanie bezpečnosti je dokazovanie, že sa splnili určené požiadavky týkajúce sa objektu posudzovania. Typicky sa realizuje prostredníctvom analýzy rizík, rozdielovej analýzy, analýzy súladu, analýzy funkčných dopadov (Business Impact Analysis, BIA), porovnávania v rámci odvetvia (benchmarking) alebo prieskumu. Primárnym účelom posudzovania je poskytnúť ucelenú informáciu o stave kybernetickej bezpečnosti a rizikách kybernetickej bezpečnosti formou technickej správy a použiť konsolidované výstupy na sledovanie trendu napr. kľúčové ukazovatele výkonnosti (Key Performance Indicators - KPI). Pre posudzovanie je typické, že môže byť vykonané vlastným hodnotením.

Testovanie bezpečnosti je proces, v ktorom je jeden alebo viac objektov posudzovania vystavených podľa opakovateľného postupu určitým podmienkam s cieľom porovnať ich

[46] K januáru 2026 v legislatívnom procese.

aktuálne a očakávané charakteristiky. Typické metódy zahŕňajú detekciu zraniteľností a skenovanie zraniteľností, penetračné testovanie, revíziu softvérového kódu (code review), integračné testovanie a výkonnostné testovanie (performance test). Primárnym účelom testovania je získanie informácií o charakteristikách objektov v kontexte kybernetickej bezpečnosti. Pre testovanie je typická požiadavka na vysokú mieru zručnosti.

Audit bezpečnosti je systematický, nezávislý a zdokumentovaný proces získavania záznamov, konštatovaní faktov alebo iných dôležitých informácií a ich objektívneho posudzovania s cieľom určiť rozsah, v akom sa splnili určené požiadavky. Typické metódy zahŕňajú auditné rozhovory a dotazníky, porovnávanie deklarovaného a skutkového stavu, preskúmanie zdokumentovaných informácií a vzorkovanie, ktoré sa vykonáva vtedy, ak nie je praktické alebo efektívne preverenie všetkých dostupných informácií v priebehu auditu. Primárnym účelom auditu je získanie informácie o nezhodách a rizikách formou konsolidovanej správy a iniciácia návrhov na zmenu existujúcich alebo implementáciu ďalších bezpečnostných opatrení. Pre audit je typická požiadavka na nestrannosť.

Certifikácia bezpečnosti (posudzovanie zhody) je atestácia nezávislým akreditovaným orgánom posudzovania zhody týkajúca sa charakteristík objektu posudzovania. Typický proces zahŕňa štyri kroky: žiadosť o posúdenie zhody, vyhodnotenie (overenie, že objekt spĺňa kvalifikačné kritériá), atestáciu (rozhodnutie o splnení kvalifikačných kritérií) a dohľad (priebežné posudzovanie, že objekt naďalej spĺňa kritériá). Primárnym účelom certifikácie je deklarácia primeranej úrovne kybernetickej bezpečnosti výrobkov, služieb a procesov a posilnenie transparentnosti posudzovania a dôvery v bezpečnosť výrobkov, služieb a procesov. Pre certifikáciu je typická požiadavka na akreditáciu a dohľad.

Proces akreditácie pre posudzovanie zhody pracuje s pojmami, ktoré sú štandardizované technickými normami. Akreditačný orgán je autoritatívny orgán, ktorý vykonáva akreditáciu; v Slovenskej republike je vnútroštátnym akreditačným orgánom Slovenská národná akreditačná služba (SNAS). Certifikačný orgán je orgán vykonávajúci posudzovanie zhody treťou stranou podľa certifikačnej schémy. Akreditácia je atestácia treťou stranou týkajúca sa orgánu posudzovania zhody, ktorá slúži ako oficiálny dôkaz kompetentnosti plniť špecifické úlohy posudzovania zhody. Certifikácia je atestácia treťou stranou týkajúca sa produktov, procesov, systémov alebo osôb. Certifikačná schéma je systém certifikácie, ktorý sa vzťahuje na určené produkty, na ktoré sa aplikujú rovnaké určené

požiadavky, osobitné pravidlá a postupy. Vlastník schémy je osoba alebo organizácia zodpovedná za rozvoj a udržiavanie konkrétnej certifikačnej schémy. Certifikačné schémy obsahujú dva kľúčové prvky: kritériá stanovujúce konkrétne certifikačné požiadavky na posúdenie (špecifikáciu, podľa ktorej sa posudzuje zhoda) a metodiku posudzovania, ktorú aplikuje certifikačný orgán pri vykonávaní posúdenia zhody.

V praxi sa objekty posudzovania zhody v oblasti bezpečnosti typicky triedia podľa toho, či sa posudzujú *osoby, systémy manažérstva* alebo *produkty*. Pre osoby sa používajú schémy nadväzujúce na ISO/IEC 17024, pre systémy manažérstva (napr. ISMS, ITSM, BCM) schémy nadväzujúce na ISO/IEC 17021 a pre produkty schémy nadväzujúce na ISO/IEC 17065. Medzi príklady patria audítori kybernetickej bezpečnosti, manažéri kybernetickej bezpečnosti, výrobky, procesy a služby.

Právnym základom certifikácie kybernetickej bezpečnosti v EÚ je nariadenie CSA. Toto nariadenie pracuje s úrovňami záruky (stupňami dôveryhodnosti) pre výrobok, proces alebo službu: *základná, pokročilá* a *vysoká*.

Základná úroveň znamená, že sa preukáže splnenie stanovených bezpečnostných požiadaviek a prítomnosť požadovaných bezpečnostných funkcií; hodnotenie sa vykonáva na úrovni známych základných rizík a hodnotiace činnosti zahŕňajú aspoň preskúmanie technickej dokumentácie, pričom môže byť umožnené vlastné posúdenie (self-assessment).

Pokročilá úroveň smeruje k rizikám známych útokov a incidentov vykonávaných subjektmi s obmedzenými zručnosťami a zdrojmi; hodnotiace činnosti zahŕňajú aspoň vylúčenie verejne známych zraniteľností a test, ktorý preukazuje, že výrobky, procesy alebo služby IKT správne plnia potrebné bezpečnostné funkcie.

Vysoká úroveň sa viaže na riziká najpokročilejších kybernetických útokov vykonávaných subjektmi so značnými zručnosťami a zdrojmi; hodnotiace činnosti zahŕňajú vylúčenie verejne známych zraniteľností, preukázanie, že výrobky, procesy alebo služby IKT správne plnia najpokročilejšie potrebné bezpečnostné funkcie, a posúdenie odolnosti proti zručným útočníkom prostredníctvom penetračného testovania.

1.8 Technická normalizácia

Predpisy z oblasti kybernetickej bezpečnosti, napríklad smernica NIS2, nariadenie CRA[47] či nariadenie AIA[48], považujú technické normy a certifikáciu za jeden z najdôležitejších prvkov pre preukazovaní súladu s požiadavkami kybernetickej bezpečnosti.

Technická normalizácia je proces vedúci k zjednoteniu podľa jednotných a presne daných noriem (štandardov, z angl. *standards*). Technická normalizácia sa môže vzťahovať na produkty, služby, procesy, materiály, subjekty a systémy manažérstva, čím poukazuje na určitú úroveň kvality, bezpečnosti a spoľahlivosti daného produktu, služieb subjektov či systémov.

Technická norma je súbor pravidiel, usmernení, technických špecifikácií alebo výsledkov činností, ktoré odzrkadľujú aktuálny stav vedy a techniky, ktorý je výsledkom konsenzu (dohody) zainteresovaných strán a podlieha systematickým previerkam jej aktuálnosti (spravidla každých päť rokov).[49] Technické normy sú teda kodifikovanou najlepšou praxou (z angl. *best practice*), teda dokumentom, ktorý obsahuje všeobecne uznávané technické riešenia, ktoré zároveň efektívne ošetrujú riziká.[50] Tieto typické charakteristiky technickej normy ju odlišujú nielen obsahom, ale aj procesom tvorby od legislatívneho procesu tvorby právnych predpisov. Od všeobecne záväzných právnych predpisov, nie je možné efektívne očakávať špecifické technické detaily – to je úlohou technických noriem.[51] Vzťah právneho predpisu a technickej normy je potrebné vnímať citlivo. Právne predpisy väčšinou v dostatočnom detaile nepopisujú požiadavky kladené na každý produkt, proces alebo službu. Potrebnú úroveň detailu obsahujú technické normy a právne predpisy by nemali nahrádzať úpravu technických noriem a upravovať podrobnosti, ktoré prináležia technickým normám. Príkladom prerastania úpravy právneho predpisu do

[47] Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 o horizontálnych požiadavkách na kybernetickú bezpečnosť výrobkov s digitálnymi prvkami (Akt o kybernetickej odolnosti).

[48] Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii), najmä recitál 117, 121, článok 40.

[49] Zo slovenskej definície technickej normy podľa § 3 ods. 1 zákon č. 60/2018 Z. z. o technickej normalizácii v znení neskorších predpisov (ďalej len „*zákon o technickej normalizácii*").

[50] Kompetenčné a certifikačné centrum kybernetickej bezpečnosti: *Technické normy v kyberbezpečnosti.* Dostupné na: https://cybercompetence.sk/technicke-normy-v-kyberbezpecnosti/.

[51] MAKATURA, I.: *Technická normalizácia v informačnej a kybernetickej bezpečnosti*. In: Bezpečnosť v praxi [online]. Žilina: Poradca podnikateľa, 2024. ISSN 2729-885X. Dostupné na: https://www.bezpecnostvpraxi.sk/odborny-clanok/technicka-normalizacia-v-informacnej-a-kybernetickej-bezpecnosti.htm.

detailov doposiaľ typických pre technické normy, je Delegované nariadenie Komisie (EÚ) 2023/1717 z 27. júna 2023, ktorým sa mení smernica Európskeho parlamentu a Rady 2014/53/EÚ, pokiaľ ide o technické špecifikácie nabíjacieho portu a komunikačného protokolu nabíjania pre všetky kategórie alebo triedy rádiových zariadení, ktoré možno nabíjať cez kábel.[52]

Normy vo všeobecnosti nie sú záväzné a ich dodržanie môže upraviť ako povinnosť iba všeobecne záväzný právny predpis. V Slovenskej republike zákon o technickej normalizácií umožňuje, aby bola STN *záväzná, hoci len nepriamo*.[53] Záväzné použitie STN si môžu taktiež dohodnúť zmluvné strany v ich zmluvnom vzťahu (napr. v dohodách o úrovni služieb SLA). Pre porovnanie, európske normy ISO/IEC sú bežne priamo citované v nariadeniach a smerniciach EÚ.[54]

Medzinárodné normy sú prijímané do sústavy slovenských technických noriem na základe podnetov odbornej verejnosti, resp. odborových združení, podnikateľských subjektov, či orgánov štátnej správy. Medzinárodnými normalizačnými orgánmi sú ISO (*International Organization for Standardization*) Medzinárodná organizácia pre normalizáciu a IEC (*International Electrotechnical Commission*) Medzinárodná elektrotechnická komisia. V kybernetickej bezpečnosti je najznámejšou rodinou noriem súbor ISO/IEC 27000, ktorý poskytuje terminológiu aj metodiky pre riadenie bezpečnosti informácií. Pre prax je kľúčová najmä ISO/IEC 27001:2022, ktorá stanovuje požiadavky na systém riadenia bezpečnosti informácií (ISMS). Dôležité je pochopiť, že 27001 nie je zoznam technických nastavení", ale systém manažérstva, ktorý kladie dôraz na procesy, roly a zodpovednosti, riadenie rizík, evidenciu, kontrolu dodávateľov, auditovateľnosť a kontinuálne zlepšovanie. Práve preto sa naň v praxi často nepriamo nadväzuje aj v regulácii. Popri tom má v prostredí priemyselných riadiacich systémov (OT/IACS) zásadný význam norma IEC 62443. Na rozdiel od ISO/IEC 27001 (organizácia a jej riadenie bezpečnosti), IEC 62443 rieši bezpečnosť priemyselných systémov z pohľadu prevádzkovateľa, integrátora aj výrobcu, typicky s dôrazom na segmentáciu, bezpečný návrh a prevádzku v prostredí, kde je dostupnosť a bezpečná prevádzka fyzického procesu kritická. V praxi sa normy často kombinujú.

[52] MAKATURA, I.: *Technická normalizácia v informačnej a kybernetickej bezpečnosti*.
[53] Tamže, porov. § 12 ods. 2 zákona o normalizácii.
[54] Tamže.

Európske normy (EN) sa preberajú do sústavy slovenských technických noriem najneskôr do 6 mesiacov od ich sprístupnenia európskymi normalizačnými organizáciami. Európskymi normalizačnými organizácie sú tri a zodpovedajú za tvorbu dobrovoľných technických noriem na európskej úrovni. Prvou, je CEN (franc. *Comité Européen de Normalisation*, angl. *European Commitee for Standardization*) Európsky výbor pre normalizáciu), druhou je CENELEC (franc. *Comité Européen de Normalisation Électrotechniqu*, angl. *European Commitee for Electrotechnical Standardization*) Európsky výbor pre normalizáciu v elektrotechnike) a poslednou je ETSI (*European Telecommunications Standards Institute*) Európsky inštitút pre telekomunikačné normy.

Rovnako ako v ISO/IEC, sa aj CEN/CENELEC opiera o štruktúru technických komisií.[55] Slovenská republika ako člen CEN a CENELEC, má povinnosť prijať všetky európske normy do sústavy STN a zrušiť pôvodné slovenské technické normy, ktoré sú s nimi v rozpore.

Harmonizované normy sú špecifický most medzi právom a technikou. Európske normy, ktoré sa stávajú harmonizovanými vtedy, keď ich európske normalizačné organizácie oficiálne predložia Európskej Komisii a Európska Komisia ich vyhlási v Úradnom vestníku Európskej únie (Official Journal of the European Union OJ EC), typ L, najmä preto, aby so zreteľom na právne dôsledky bol stanovený dátum, od ktorého možno zhodu s európskou legislatívou predpokladať a aby všetky hospodárske subjekty v EÚ mali rovnakú východiskovú pozíciu pri využívaní harmonizovaných noriem. Právna domnienka súladu je dôvod, prečo harmonizované normy v praxi fungujú ako preferovaný spôsob, ako preukázať súlad, bez toho, aby právny predpis musel do detailu opisovať technické riešenia. Zároveň platí, že používanie harmonizovaných noriem spravidla nie je formálne povinné; výrobca môže zvoliť aj iné technické riešenie, len potom musí vedieť rovnocenne preukázať splnenie právnych požiadaviek.

Práve účinok harmonizovaných noriem vpodobe prezumpcie súladu, vedie v literatúre k popisu javu ako „juridifikácia" technických noriem, normy sa postupne stávajú neoddeliteľnou súčasťou toho, ako v praxi čítame a aplikujeme právo. Harmonizované normy sa stávajú *de facto* záväznými.[56] Rozhodnutie Súdneho dvora EÚ vo veci

[55] Zoznam technických komisií. Dostupné na: https://standards.cencenelec.eu/dyn/www/f?p=CEN:6.

[56] Rozsudok Súdneho dvora (štvrtá komora) z 12. júla 2012. v prípade C-171/11 Fra.bo SpA proti Deutsche Vereinigung des Gas- und Wasserfaches eV (DVGW) – Technisch-Wissenschaftlicher Verein.

Public.Resource.Org[57], ako aj stanovisko generálneho advokáta v tejto veci, vyvoláva otázky týkajúce sa demokratických procesov v normalizačných organizáciách. Vývoj technických noriem vstúpil do štádia, ktoré akademici označujú ako „juridifikácia"[58], keď sa normy, aj keď nie sú záväzné, považujú za súčasť práva EÚ. [59]

V rozsudku Fra.bo Súdny dvor EÚ v podstate uznal, že napriek tomu, že normalizačné a certifikačné orgány sú súkromnoprávnymi subjektmi, môžu vykonávať verejnoprávne právomoci a že aj keď sú vnútroštátne technické normy dobrovoľné (keďže hospodárske subjekty majú aspoň teoreticky alternatívne prostriedky na preukázanie súladu so základnými požiadavkami príslušných sekundárnych právnych predpisov), *de facto* môžu mať záväzné účinky.[60] Súdny dvor v kľúčovom rozsudku James Elliott rozhodol, že harmonizované normy sú vzhľadom na svoje právne účinky súčasťou práva Únie, a Súdny dvor má právo ich vykladať nakoľko majú povahu opatrení vykonávajúcich právny akt Únie. [61] Harmonizované normy však nie sú len prosté vykonávacie opatrenia pochádzajúce od európskych normalizačných organizácií, ale majú sa považovať za prijaté Komisiou, alebo, v každom prípade, že Komisia je zodpovedná za prijatie týchto noriem v spojení s normalizačnými organizáciami.[62]

Presné vymedzenie základných požiadaviek na normu zo strany Komisie je veľmi dôležité, aby sa zabránilo nesprávnemu výkladu zo strany európskych normalizačných organizácií, pričom úroveň podrobnosti a špecifickosť požiadaviek nie je v nariadení č.

---

[57] Rozsudok Súdneho dvora (veľká komora) z 5. marca 2024 v prípade C-588/21 *Public.Resource.Org, Inc. and Right to Know CLG proti Európska komisia*, bod 73.

[58] SCHAPEL, Harm: 'The New Approach to the New Approach: The Juridification of Harmonised Standards in EU Law.' (2013) Maastricht Journal of European and Comparative Law, 20 (4): 521–33 Dostupné na: https://doi.org/10.1177/1023263X1302000404.; VAN GESTEL, Rob a MICKLITZ Hans-W.: "European Integration through Standardisation: How Judicial Review Is Breaking Down the Club House of Private Standardisation Bodies" [2013] *Common Market Law Review* 145-182 Dostupné na: https://doi.org/10.54648/cola2013007; ELIANTONIO Mariolina a COLOMBO Carlo, "Harmonized Technical Standards as Part of EU Law: Juridification with a Number of Unresolved Legitimacy Concerns?" [2017] *Maastricht Journal of European and Comparative Law*, 323-340 [13.9.2024]. Dostupné na: https://doi.org/10.1177/1023263X17709753.

[59] TOVO, Carlo: 'Judicial Review of Harmonised Standards: Changing the Paradigms of Legality and Legitimacy of Private Rulemaking Under EU Law.' (2018) Common Market Law Review, 55 (4). Dostupné na: https://doi.org/10.54648/cola2018096 ; VOLPATO, Annalisa: 'The Legal Effects of Harmonised Standards in EU law,' (2023) REALaw.blog, Dostupné na:https://realaw.blog/?p=2879.

[60] Rozsudok Súdneho dvora (štvrtá komora) z 12. júla 2012. v prípade C-171/11 Fra.bo SpA proti Deutsche Vereinigung des Gas- und Wasserfaches eV (DVGW) – Technisch-Wissenschaftlicher Verein. Body 27 až 32.

[61] Rozsudok Súdneho dvora (tretia komora) z 27. októbra 2016 v prípade C-613/14 James Elliott Construction Limited/Irish Asphalt Limited, body 34, 40.

[62] Rovnako, návrhy Generálnej advokátky Laila Medina z 22. júna 2023 vo veci C-588/21P Public.Resource.Org, Inc., Right to Know CLG proti Európskej komisii.

1025/2012 nijako záväzne špecifikovaná. Komisia aj Európsky parlament vyjadrujú obavy z udeľovania nadmerných oprávnení európskym normalizačným organizáciám prostredníctvom žiadostí o vypracovanie noriem a zdôrazňujú, že normalizačné organizácie by sa mali zamerať výlučne na definovanie technických metód na dosiahnutie legislatívnych cieľov a zdržať sa zasahovania do akejkoľvek politickej diskreácie. Samotná Komisia by mala postupovať mimoriadne opatrne, aby preukázala nevyhnutnosť vypracovania noriem.[63] Z oznámenia Komisie ďalej vyplýva, že normy sa viac ako kedykoľvek predtým nemusia týkať len technických prvkov, ale musia zahŕňať aj základné demokratické hodnoty a záujmy EÚ, ako aj ekologické a sociálne zásady. Práve normy pre kybernetickú bezpečnosť alebo odolnosť kritickej infraštruktúry v tomto smere majú strategický rozmer.[64]

Komisia tiež pripúšťa, že je potrebné presunúť ešte väčšiu kontrolu nad harmonizovanými normami z európskych normalizačných organizácií na Komisiu, keď uvádza, že s cieľom zabezpečiť zohľadnenie verejného záujmu by Komisia mala byť splnomocnená priamo vypracovať - prostredníctvom vykonávacích aktov - *spoločné špecifikácie* (technické dokumenty alternatívne k harmonizovaným normám vypracovaným normalizačnými organizáciami).[65]

Vzhľadom na úlohu harmonizovaných noriem v harmonizačných právnych predpisoch EÚ by spoločná špecifikácia mala byť výnimočným náhradným riešením, ktoré uľahčí povinnosť povinných osôb dodržiavať regulačné požiadavky, ak žiadosť o normalizáciu neprijala žiadna z európskych normalizačných organizácií, alebo ak príslušné harmonizované normy primerane neriešia obavy týkajúce sa základných práv, alebo ak harmonizované normy nie sú v súlade so žiadosťou, alebo ak dôjde k oneskoreniu prijatia vhodnej harmonizovanej normy.[66]

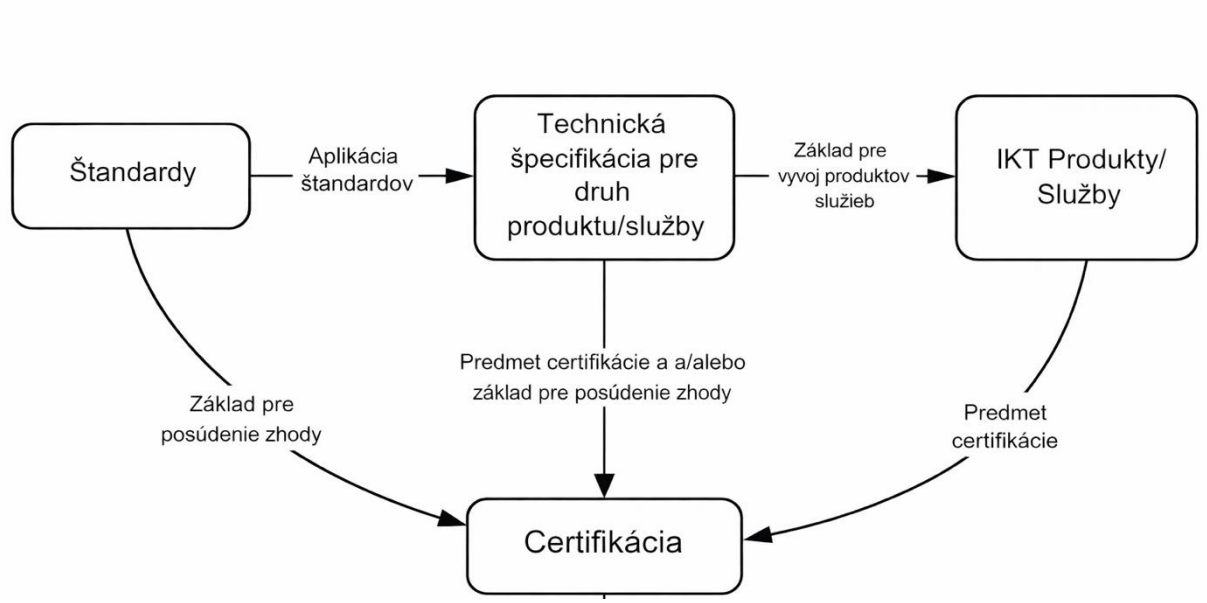
Nariadenie AIA potvrdzuje tento posun tým, že poveruje Komisiu vypracovaním spoločných špecifikácií v prípadoch, keď harmonizované normy buď neexistujú, sú nedostatočné, alebo primerane neriešia obavy týkajúce sa základných práv.[67] Rovnako tak možno poukázať aj na požiadavky kybernetickej bezpečnosti digitálnych produktov, kde CRA

[63] ELIANTONIO, Mariolina a VOLPATO, Annalisa, 'The European System of Harmonised Standards. Legal Opinion for ECOS' (March 11, 2022). Dostupné na: http://dx.doi.org/10.2139/ssrn.4055292.
[64] Oznámenie Komisie z 2 Februára 2022 (COM(2022) 31 final) 'Stratégia EÚ v oblasti normalizácie', s. 4 a 5 Dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:52022DC0031.
[65] Tamže.
[66] Recitál č. 121 AIA.
[67] Porov. článok 41 ods. 1 AIA.

tiež vychádza z možnosti Komisie prijať spoločné špecifikácie na dosiahnutie súladu so základnými požiadavkami uvedenými v prílohe I pre produkty s digitálnymi prvkami, len vtedy, ak sú určité splnené podmienky.[68] Pričom CRA označuje prijatie spoločných špecifikácií Komisiou, ako „výnimočné núdzové" riešenie na uľahčenie povinnosti výrobcu dosiahnuť súlad so základnými požiadavkami, keď je normalizačný proces zablokovaný alebo keď pri zavádzaní vhodných harmonizovaných noriem dochádza k oneskoreniam.[69]

Nakoniec, harmonizované normy treba chápať aj v prepojení na posudzovanie zhody a certifikáciu. Nariadenie CSA od roku 2019 vytvorilo európsky rámec certifikácie kybernetickej bezpečnosti pre produkty IKT, služby IKT a procesy IKT. Jadrom tohto rámca je myšlienka, že dôvera v bezpečný produkt nemá stáť na marketingu, ale na overiteľnom posúdení podľa vopred stanovených pravidiel. ENISA v tomto systéme pripravuje návrhy (kandidátske) certifikačné schémy. Certifikačná schéma je v praxi „recept", ktorý určuje, čo sa posudzuje, ako sa to posudzuje a aké dôkazy sa považujú za dostatočné. Technické normy a technické špecifikácie sú v CSA kľúčové preto, že prekladajú všeobecné právne ciele do konkrétnych, merateľných a auditovateľných požiadaviek. CSA zdôrazňuje potrebu opierať certifikačné schémy o medzinárodné alebo európske normy. Z praktického hľadiska je dôležité, že CSA výslovne počíta s tým, že certifikát alebo EÚ vyhlásenie o zhode bude odkazovať na použité technické špecifikácie, normy a príslušné postupy hodnotenia.

[68] Článok 27 ods. 2 CRA.
[69] Recitál č. 83 CRA.



Obrázok č. 3: Vzťah medzi štandardmi, technickou špecifikáciou, IKT produktmi/službami a certifikáciou.[70]

[70] Adaptované z ENISA: Standardisation in support of the Cybersecurity Certification. December 2019, dostupné na: https://www.enisa.europa.eu/publications/recommendations-for-european-standardisation-in-relation-to-csa-i Vygenerované nástrojom UI (ChatGPT).

2. KYBERNETICKÁ BEZPEČNOSŤ A JEJ MIESTO V SYSTÉME OCHRANY ZÁKLADNÝCH ĽUDSKÝCH PRÁV A SLOBÔD

Základné ľudské práva a slobody predstavujú jeden z pilierov právnych štátov a moderných demokracií. Svoje nezastupiteľné miesto si našli hlavne po druhej svetovej vojne v medzinárodnoprávnych dokumentoch a národných ústavných normách. Výnimkou nie je ani Európska únia, kde je Charta základných práv Európskej únie spolu so zakladajúcimi zmluvami súčasťou primárneho práva Európskej únie. V tejto časti učebnice sa nebudeme venovať historicko-právnemu vývoju základných práv a slobôd a do detailov ich systémového nastavenia.[71] Taktiež sa nebudeme zameriavať na detailnú analýzu jednotlivých práv a slobôd. Naopak, pozornosť čitateľov chceme upriamiť na tie základné ľudské práva a slobody, ktoré s otázkou kybernetickej bezpečnosti priamo alebo nepriamo súvisia. Cieľom je tak poskytnúť ľudsko-právny kontext kybernetickej bezpečnosti. Vzhľadom na nadnárodný charakter danej témy sa budeme venovať predovšetkým právnej úprave na úrovni EÚ s presahom do slovenského právneho systému.

So vzrastajúcou prítomnosťou online pribúdajú možnosti, ktoré môžeme vykonávať prostredníctvom internetu. Ide napríklad o voľbu v parlamentných voľbách kompletne online, takýto systém funguje v Estónsku od roku 2005, pričom oprávneným voličom postačuje mať pripojenie na internet a občiansky preukaz, ktorým sa identifikujú.[72] Vykonávanie aktívneho volebného práva z pohodlia domova bolo v minulosti nemysliteľným krokom, ale v súčasnosti vzrastá nielen ponuka služieb e-governmentu, ale aj rôznych služieb pre osobnú potrebu. Na príklade digitálnych parlamentných volieb si vieme demonštrovať ako jedna má vplyv na viacero ľudských práv. Aby vôbec digitálne parlamentné voľby bolo možné vykonávať, museli vytvoriť software, ktorý takúto voľbu technicky umožní. Ak štát nemá k dispozícii vlastný

[71] Odkazujeme na príslušnú literatúru napr. SVÁK, J.: Ochrana ľudských práv (v troch zväzkoch). Žilina: Eurokódex, 2011 alebo FRIDRICH, B. a kol.: Ústavné garancie ľudských práv. Bratislava: Právnická fakulta UK, 2013 alebo SVÁK, J. – GRUNWALD, T.: Nadnárodné systémy ochrany ľudských práv, I. zväzok Štruktúra systémov a ochrana politických práv. Bratislava: Wolters Kluwer, 2019; SVÁK, J.: Nadnárodné systémy ochrany ľudských práv. II. Zväzok. Ochrana fyzickej integrity človeka. Bratislav: Wolters Kluwer, 2020; SVÁK, J.: Nadnárodné systémy ochrany ľudských práv. III. zväzok. Ochrana súkromia a majetku. Bratislava: Wolters Kluwer, 2021.

[72] Valimised. Internet voting in Estonia. Oktober 2025, [online] [26.02.2026]. Dostupné na: https://www.valimised. ee/en/internet-voting/more-about-i-voting/introduction-i-voting.

software, musí zväčša prostredníctvom verejného obstarávania vysúťažiť, kto mu daný software dodá. Tu svoju rolu zohráva právo podnikať, ktoré umožňuje súkromným entitám ponúknuť štátu svoj software. Štát musí na druhej strane dbať o to, že verejné obstarávanie softwaru bude transparentné a občania sa o celom procese budú môcť informovať, čo súvisí nielen s právom na dobrú správu vecí verejných, ale aj s právom na informácie. Právo na súkromie a právo na ochranu osobných údajov vyžaduje, aby software po odovzdaní hlasu oddelil identitu voliča od jeho hlasovacieho lístka, aby sa nedalo zistiť, koho volič volil. Prirodzene, software, ktorý umožňuje voľbu v parlamentných voľbách cez internet musí byť bezpečný, aby odolával kybernetickým útokom. Bez bezpečného systému nemožno dodržať ani právo na súkromie a právo na ochranu osobných údajov. Existuje však právo na kybernetickú bezpečnosť?

2.1 Právo na (kybernetickú) bezpečnosť?

Máme ako fyzické osoby základné ľudské právo na (kybernetickú) bezpečnosť? Charta ani Ústava Slovenskej republiky podobné právo výslovne neupravuje. To ale hneď automaticky neznamená, že nebudeme vedieť nájsť jeho základ v niektorom z existujúcich základných ľudských práv a slobôd. Zároveň, viaceré nadväzujúce právne akty obsahujú požiadavky dôvernosti či ochrany súkromia.

Aby sme vedeli diskusiu nasmerovať správnym smerom, je potrebné pozrieť sa na to, na základe akého právneho základu EÚ vydala smernicu NIS. Právny základ je ustanovenie primárneho práva, na základe ktorého je následne prijímaná doplňujúca legislatíva. V prípade smernice NIS právny základ tvorí článok 114 Zmluvy o fungovaní EÚ:

> *„Nasledujúce ustanovenia sa použijú na dosiahnutie cieľov uvedených v článku 26, pokiaľ zmluvy neustanovujú inak. Európsky parlament a Rada v súlade s riadnym legislatívnym postupom a po porade s Hospodárskym a sociálnym výborom prijímajú opatrenia na aproximáciu ustanovení zákonov, iných právnych predpisov a správnych opatrení členských štátov, ktoré smerujú k vytváraniu a fungovaniu vnútorného trhu.*"

Kybernetická bezpečnosť je tak vnímaná ako súčasť efektívneho fungovania vnútorného trhu EÚ. Toto konštatovanie je potvrdené aj v samotnej dôvodovej správe ku smernici NIS:

> *„...siete a informačné systémy zohrávajú dôležitú úlohu pri uľahčovaní cezhraničného pohybu tovaru, služieb a osôb. Často sú navzájom prepojené a internet má globálny charakter. Vzhľadom na tento skutočne nadnárodný rozmer, narušenie v jednom členskom štáte môže mať vplyv aj na ďalšie členské štáty a EÚ ako celok. Preto je pre riadne fungovanie vnútorného trhu nevyhnutná odolnosť a stabilita sietí a informačných systémov.*"

Niektorí autori poukazujú na to, že právna úprava kybernetickej bezpečnosti vykazuje určitý stupeň elasticity (prispôsobovania sa aktuálnym hrozbám), čo nevyhnutne vplýva aj na rámec základných práv a slobôd. Všeobecne vo vzťahu ku základným právam a slobodám možno uviesť, že kybernetická bezpečnosť môže vystupovať v troch pozíciách.

V prvom rade spomenieme interpretáciu, ktorá hovorí, že kybernetická bezpečnosť je o ochrane základných ľudských práv a slobôd. To znamená, že právo kybernetickej bezpečnosti priamo základné ľudské práva a slobody chráni. Nasvedčuje tomu napríklad recitál 75 Smernice NIS, ktorý zdôrazňuje potrebu dodržiavania základných práv a zásad uznaných Chartou základných práv Európskej únie, najmä právo na rešpektovanie súkromného života a komunikácie, ochrana osobných údajov, sloboda podnikania, právo vlastniť majetok, právo na účinný prostriedok nápravy pred súdom a právo na vypočutie. Zároveň smernica NIS 2, ktorá nahradila smernicu NIS, je ešte o krok ďalej v tejto téme. Je to z toho dôvodu, že sa priamo odvoláva na definíciu kybernetickej bezpečnosti[73] v zmysle článku 2 bodu 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881, ktoré ochranu jednotlivcov priamo spomína:

> *„činnosti potrebné na ochranu sietí a informačných systémov, **užívateľov takýchto systémov** a iných osôb dotknutých kybernetickými hrozbami.*"

[73] Čl. 6 bod 3 smernice NIS 2.

V smernici NIS 2 recitál 70 v spojitosti s recitálom 143 naďalej akcentuje potrebu dodržiavania základných práv ako základnú hodnotu a rozširuje výpočet základných práv oproti recitálu 75 v predchádzajúcej smernici NIS:

> *„Rozsiahle kybernetické incidenty a krízy na úrovni Únie si z dôvodu vysokého stupňa previazanosti odvetví a členských štátov vyžadujú koordinované opatrenia na zabezpečenie rýchlej a účinnej reakcie. Dostupnosť kyberneticky odolných sietí a informačných systémov a dostupnosť, dôvernosť a integrita údajov sú nevyhnutné pre bezpečnosť Únie a* ***ochranu jej občanov****, podnikov a inštitúcií pred incidentmi a kybernetickými hrozbami, ako aj pre posilnenie dôvery jednotlivcov a organizácií v schopnosť Únie podporovať a chrániť globálny, otvorený, slobodný, stabilný a bezpečný kybernetický priestor* ***založený na ľudských právach****, základných slobodách, demokracii a právnom štáte.*"

> *„V tejto smernici sa rešpektujú základné práva a dodržiavajú zásady uznané v charte, najmä právo na rešpektovanie súkromného života a komunikácií, ochranu osobných údajov, slobodu podnikania, právo vlastniť majetok, právo na účinný prostriedok nápravy a na spravodlivý proces, prezumpcia neviny a právo na obhajobu. Právo na účinný prostriedok nápravy sa vzťahuje aj na príjemcov služieb poskytovaných kľúčovými a dôležitými subjektmi. Táto smernica by sa mala vykonávať v súlade s uvedenými právami a zásadami.*"

Druhou interpretáciou vzťahu kybernetickej bezpečnosti a základných ľudských práv a slobôd je, že kybernetická bezpečnosť musí byť v súlade s ľudsko-právnym štandardom. Napriek tomu, že členské štáty pri ochrane ľudských práv zväčša reflektujú negatívne záväzky (štát nesmie do týchto práv bezbreho zasahovať), v určitých situáciách je nevyhnutná implementácia pozitívneho záväzku dodržiavať určitý štandard. To praktický znamená, že samotná legislatíva a jej uplatňovanie nesmie základným ľudským právam a slobodám odporovať. Ak napríklad prevádzkovateľ monitoruje bezpečnosť sietí, nesmie pri tom príliš invazívnym spôsobom zasahovať do práva na súkromie užívateľov.

Treťou možnosťou je vnímať kybernetickú bezpečnosť úplne oddelene od základných ľudských práv a slobôd.[74] S touto interpretáciou sa ale nestotožňujeme, nakoľko právo kybernetickej bezpečnosti by malo byť vykladané a uplatňované v súlade so základnými právami a slobodami. Uznávame však, že ak vezmeme do úvahy otázku bezpečnostných štandardov v oblasti kybernetickej bezpečnosti, tieto častokrát tvorí samotný trh a nemusia prakticky odzrkadľovať požiadavky základných práv a slobôd. Z dlhodobého hľadiska je ale takýto prístup neudržateľný. Cesta dodržiavania štandardov, ktoré schváli a publikuje EÚ vo svojom vestníku je pre prevádzkovateľov ľahšou, nakoľko nemusia interpretovať požiadavky právneho predpisu, ale „nabehnú" na už presne upravený proces. Na strane druhej, zákonodarca na úrovní EÚ nemá právo tieto štandardy vetovať. Navyše, otvorenou otázkou stále ostáva, či Súdny dvor Európskej únie má kompetenciu štandardy preskúmavať. Ak legislatívne akty Európskej únie odkazujú na konkrétne štandardy, tak sú súčasťou práva Európskej únie[75] a Súdny dvor v tomto prípade má kompetenciu štandardy preskúmať. Ak je odpoveď negatívna, otvára to pandorinu skrinku...[76]

Ak zároveň vezmeme do úvahy, že kybernetická bezpečnosť sa zameriava na ochranu tzv. aktív, je možné konštatovať, že prirodzeným dôsledkom potreby fungovania vnútorného trhu a ochrany aktív bude vnímanie kybernetickej bezpečnosti v kontexte práva na podnikanie resp. práva vlastniť majetok. Toto konštatovanie ale samozrejme neplatí v súvislosti s orgánmi verejnej moci, ktoré musia primeranú bezpečnosť zabezpečiť taktiež, ale s cieľom ochrany aktív, ktoré využívajú na plnenie úloh vo verejnom záujme. Z pohľadu adresátov právnych noriem, ktorým je legislatíva kybernetickej bezpečnosti primárne venovaná tak možno zhrnúť, že z hľadiska základných práv a slobôd je potrebné diskutovať predovšetkým právo vlastniť majetok (vrátane práva na podnikanie a ochrany duševného vlastníctva) a právo na dobrú správu veci verejných.

Každá minca má ale dve strany a nemožno opomenúť ďalší subjekt v rovnici kybernetickej bezpečnosti - fyzické osoby, ktorých informácie častokrát aktíva tvoria. Z ich pohľadu je osobitne dôležité zvýrazniť právo na súkromie a právo na ochranu osobných

[74] Pozri FUSTER, G., JASMONTAITE, L.: Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights. In CHRISTENSEN, M. et al. (eds).: Ethics of Cybersecurity. Springer, 2020, s. 97 - 116.

[75] Rozhodnutie Súdneho dvora Európskej únie, C-185/19 - Public.Resource.Org, Inc. a Right to Know CLG.

[76] Pozri diskusiu v VAELE, M. – BORGESIUS, F.Z.: Demystifying the Draft EU Artificial Intelligence Act. DOI: https://arxiv.org/ct?url=https%3A%2F%2Fdx.doi.org%2F10.9785%2Fcri-2021-220402&v=ec7cae1dm, s. 14 - 15.

údajov. Čiastočne možno hovoriť aj o slobode prejavu v podobe práva na informácie, ktoré sa týkajú bezpečnostných incidentov a právnych povinností informovania o nich. Výber relevantných základných práv a slobôd podporuje aj recitál 75 smernice NIS. Ochranu práva na súkromie a slobody prejavu výslovne spomína aj David Kaye vo svojej správe pre Organizáciu spojených národov.[77] Prečo však právo na súkromie, prípadne právo na ochranu osobných údajov nepostačuje na oblasť kybernetickej bezpečnosti? GDPR sa zaoberá kybernetickými bezpečnostnými incidentmi len vtedy, keď zasiahli osobné údaje jednotlivcov. Osobné údaje nie sú zďaleka všetky citlivé údaje, ktoré môžu byť zasiahnuté, môže ísť o obchodné tajomstvo, know-how alebo iné údaje, ktoré predstavujú určité aktívum. Kybernetické bezpečnostné incidenty nespôsobujú len finančné škody, ale aj psychologické ťažkosti. Psychologické ťažkosti, reputačné riziko ani finančné škody, ktoré v dôsledku kybernetického bezpečnostného incidentu vznikli, nespadajú pod porušenie práva na ochranu osobných údajov. Dôležitosť práva na kybernetickú bezpečnosť podčiarkuje princíp bezpečnosti digitálnych technológiív Európskej deklarácií o digitálnych právach a princípoch.[78]

2.2 Adresáti povinností

Ako postupne vysvetlíme v ďalších častiach tejto učebnice, požiadavky kybernetickej bezpečnosti sa vzťahujú na dva typy subjektov – prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb. Nie je rozhodujúce, či daný subjekt pôsobí ako súkromnoprávna entita alebo orgán verejnej moci. Ak spĺňa kritéria pre prevádzkovateľa základnej služby alebo poskytovateľa digitálnej služby, budú sa na neho vzťahovať požiadavky vyplývajúce z legislatívy. Preto je nevyhnutné tieto požiadavky vnímať dvojakým spôsobom v kontexte základných ľudských práv a slobôd. V prvom rade ako právo vlastniť majetok resp. podnikať pre subjekty pôsobiace v súkromnej sfére. V druhom rade ako zvýraznenie požiadavky dobrej správy veci verejných pre orgány verejnej moci.

[77] KAYE, D.: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression : note / by the Secretary-General. Dostupné na https://digitallibrary.un.org/record/1304394.

[78] Európska komisia. European Declaration on Digital Rights and Principles. December 2022, [online] [26.02.2026]. Dostupné na: https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles.

2.2.1 Právo podnikať a vlastnícke právo

Ako prvé zo základných práv, ktoré explicitne spomína aj samotná Smernica NIS je v kontexte kybernetickej bezpečnosti nutné spomenúť právo podnikať a vlastnícke právo. Sloboda podnikania je zaručená článkom 16 Charty:

> *„Sloboda podnikania sa uznáva v súlade s právom Únie, vnútroštátnymi právnymi predpismi a praxou.*"

Základom tohto práva je rešpektovanie slobody vyvíjať ekonomické aktivity vo vlastnom mene. SDEÚ vo svojej judikatúre taktiež zdôrazňuje, že súčasťou tohto práva je aj ochrana obchodných tajomstiev.[79] Práve ochrana svojho know-how môže byť katalyzátorom pre implementovanie bezpečnostných opatrení.

Sloboda podnikania a jej výkon je úzko previazaná s vlastníckym právom. Ochrana vlastníckeho práva je predmetom článku 17 Charty:

> *„1. Každý má právo vlastniť svoj oprávnene nadobudnutý majetok, užívať ho, nakladať s ním a odkázať ho. Nikoho nemožno zbaviť jeho majetku, s výnimkou verejného záujmu, v prípadoch a za podmienok, ktoré ustanovuje zákon, pričom musí byť včas vyplatená spravodlivá náhrada. Užívanie majetku môže byť upravené zákonom v nevyhnutnej miere v súlade so všeobecným záujmom.*
> *2. Duševné vlastníctvo je chránené.*"

Kým článok 16 Charty chráni proces nadobudnutia majetku, článok 17 Charty chráni už nadobudnutý majetok – vlastnícke právo. Pod pojmom majetok je potrebné rozumieť nielen hnuteľné, ale aj nehnuteľné komodity, ako napríklad duševné vlastníctvo potvrdené druhým odsekom diskutovaného článku. Zároveň daný článok upravuje podmienky pre obmedzenie vlastníckeho práva.

Ak sa nad článkami 16 a 17 Charty zamyslíme vo vzájomnej súvislosti v kontexte kybernetickej bezpečnosti, môžeme sa na to z pohľadu adresáta povinností (podnikateľa)

[79] Rozhodnutie Súdneho dvora Európskej únie, C-1/11 - Interseroh Scrap and Metals Trading.

pozrieť dvojakým spôsobom. Na jednej strane podnikateľ *musí* v zmysle požiadaviek na kybernetickú bezpečnosť svoj majetok chrániť a dodržiavanie týchto pravidiel je v gescií príslušného orgánu. Ak tieto pravidlá nedodrží, môže mu byť uložená pokuta alebo iná sankcia. EÚ resp. štát v tomto prípade vyžaduje minimálny bezpečnostný štandard pre určité subjekty zo súkromného sektora, pričom toto konštatovanie špecificky platí pre kritické služby pre fungovanie hospodárstva alebo štátu ako dopravné služby, finančné služby či energetické podniky.

Na strane druhej by podnikateľ *mal chcieť* minimálne niektoré svoje aktíva chrániť. Informácie o svojich zákazníkoch, dáta odvodené o ich správaní či iné kritické aktíva predstavujú kľúč pre podnikanie a častokrát aj zväčšovanie majetku. Z tohto pohľadu je ochrana majetku nevyhnutnou súčasťou podnikania, pričom jej výkonu svedčia práve bezpečnostné opatrenia, z ktorých viaceré predpisuje európska a národná legislatíva.

2.2.2 Právo na dobrú správu veci verejných

Inou optikou je pohľad orgánov verejnej moci, ktoré majú častokrát k dispozícií veľmi presné databázy informácií o svojich občanoch. Tie sú následné využívané pre plnenie úloh vo verejnom záujme. Cenné informačné aktíva sa tak nenachádzajú iba v rukách súkromných spoločností, ale aj štátu. Vzhľadom na to, že cieľom štátu nie je produkovanie zisku a štát „nie je firma," nemožno v kontexte kybernetickej bezpečnosti hovoriť o vlastníckom práve a slobode podnikania.[80]

Charta v článku 41 obsahuje právo na dobrú správu veci verejných:

> *„1. Každý má právo, aby inštitúcie, orgány, úrady a agentúry Únie vybavovali jeho záležitosti nestranne, spravodlivo a v primeranej lehote.*
>
> *2. Toto právo zahŕňa najmä:*
>
> *a) právo každého na vypočutie pred prijatím akéhokoľvek individuálneho opatrenia, ktoré by sa ho mohlo nepriaznivo dotýkať;*
>
> *b) právo každého na prístup k spisu, ktorý sa ho týka, za predpokladu rešpektovania oprávnených záujmov dôvernosti a služobného a obchodného tajomstva;*

[80] Pre účely tejto state nebudeme bližšie rozoberať polo-štátne verejné podniky, ktoré majú špecifické úlohy a nachádzajú sa na pomedzí súkromného a verejného sektora.

c) povinnosť administratívy odôvodniť svoje rozhodnutia.

3. Každý má právo na náhradu škody spôsobenej inštitúciami alebo zamestnancami Únie pri výkone ich funkcií v súlade so všeobecnými zásadami spoločnými pre právne poriadky členských štátov.

4. Každý sa môže obrátiť na inštitúcie Únie v jednom z jazykov zmlúv a musí dostať odpoveď v rovnakom jazyku."

Z dikcie diskutovaného článku by sa mohlo zdať, že právo na dobrú správu veci verejných je čisto procesným právom a vzťahuje sa len na správne konania, kde účastníkom konania priznáva určité penzum práv. Nie je to však tak. V prvom rade tomu nasvedčuje demonštratívny výpočet jednotlivých práv. V druhom rade, jeho vnímanie a interpretácia v rámci aplikácie sa nevzťahuje len na správne právo procesné, ale toto právo by sa malo uplatňovať v každom segmente pri správe veci verejných.[81] Tomuto prístupu zodpovedá aj prístup k tomuto právu v rámci Európskeho kódexu dobrej správnej praxe (Kódex dobrej správnej praxe), ktorý prijal Európsky parlament v roku 2001. Kódex dobrej správnej praxe sa však vzťahuje iba na úradníkov v rámci inštitúcii EÚ. Môže však slúžiť ako inšpirácia aj pre výkon verejnej správny v jednotlivých členských štátoch, nakoľko zakotvuje princípy dobrej verejnej správy.[82]

„Napriek tomu kódex poslúžil ako inšpirácia pre určité podobné texty v členských štátoch Európskej únie, kandidátskych krajinách a tretích krajinách. Okrem toho sa vo vysvetleniach, ktoré sú súčasťou Charty základných práv, objasňuje, že právo na dobrú správu sa zakladá na judikatúre Súdneho dvora týkajúcej sa dobrej správnej praxe ako všeobecnej zásady práva

EÚ. Takéto všeobecné zásady tiež zaväzujú členské štáty, keď pôsobia v rámci rozsahu práva EÚ."

Článok 21 tohto kódexu výslovne stanovuje povinnosť úradníkov zachovávať ochranu osobných údajov, s ktorými dôjdu do styku s odkazom na nariadenie, ktoré sa na túto oblasť

[81] PEKÁR, B. : Európske správne právo a európsky správny priestor. 1. vydanie. Euroiuris, 2012, s. 64 a ďalšie.
[82] Kódex dobrej správnej praxe, s. 11.

v vzťahuje.[83] Princípy dobrej verejnej správy sú spomenuté v texte recitálu 28 tohto nariadenia v súvislosti s prenosom osobných údajov:

> *„V takýchto prípadoch by prevádzkovateľ mal preukázateľne zvážiť rôzne protichodné záujmy s cieľom posúdiť primeranosť požadovaného prenosu osobných údajov. Tento osobitný účel vo verejnom záujme by sa mohol týkať transparentnosti inštitúcií a orgánov Únie. Inštitúcie a orgány Únie by mali v súlade so zásadou transparentnosti* ***a dobrej správy vecí verejných*** *preukázať takúto nutnosť, keď sami iniciujú prenos.*"

Nakoľko požiadavky bezpečnosti a ochrany údajov spolu súvisia, môžeme konštatovať že požiadavky legislatívy kybernetickej bezpečnosti je možné prepojiť aj s právom na dobrú správu veci verejných. Ak by platil opak, museli by sme uviesť absurdné tvrdenie, že zachovanie bezpečnosti aktív v dispozícií orgánov verejnej moci nie je pozitívnou praxou a dobrou verejnou správou. Opak je pravdou.

2.3 Fyzické (dotknuté) osoby

Ako bolo uvedené vyššie, kybernetická bezpečnosť neovplyvňuje len priamych adresátov noriem v podobe regulovaných subjektov, ale aj iné fyzické osoby. Práve z ich pohľadu je diskusia možno ešte zaujímavejšia, nakoľko ide o otázky, ktoré sa bytostne dotýkajú každého z nás. Vzhľadom na to, že Charta odlišuje medzi právom na súkromie a právom na ochranu osobných údajov, budeme požiadavky na kybernetickú bezpečnosť skúmať v každom z práv osobitne. Výklad doplníme o právo na informácie v súvislosti so slobodou prejavu, ktoré výslovne spomína aj Smernica NIS 2.

2.3.1 Právo na súkromie

Právo na súkromie je predmetom ochrany v článku 7 Charty:

[83] Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES . Ú. v. EÚ L 295, 21.11.2018, s. 39 – 98.

„Každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlia a komunikácie."

Právo na súkromie má pomerne bohatý obsah. Ako už z dikcie ustanovenia článku 7 Charty vyplýva, poskytuje ochranu súkromia v najširšom možnom rozsahu a to v podobe súkromného života, rodinného života, obydlia a zasielaných a prijímaných správ (komunikácia). Legálnu definíciu súkromia v Charte nenachádzame, judikatúra opakovane zdôraznila, že zásahy do práva na súkromie je potrebné skúmať od prípadu k prípadu a jeho definícia by bola v konečnom dôsledku kontraproduktívna a pravdepodobne aj reštriktívna.

Otázky kybernetickej bezpečnosti sa budú dotýkať predovšetkým záujmov súkromného života a komunikácie. Komunikáciu je potrebné vnímať a vykladať aj v kontexte technologického vývoja a zahŕňa ako klasickú listovú komunikáciu, tak aj digitálny prenos informácií prostredníctvom mailov alebo chatovacích aplikácií. Zásadné limity obsahuje právo EÚ práve v rámci prístupu prevádzkovateľov takýchto služieb a obsahu prenášaných správ. Osobitnou kapitolou je zachytávanie údajov v rámci sietí alebo pri poskytovaní služieb na účely bezpečnosti, kde je zo získaných dát možné vyvodiť pomerne presné závery o súkromnom živote jednotlivca.

PRÍKLAD

Z polohy jednotlivca možno vyčítať kde pracuje, kde býva, aké sú jeho obľúbené podniky či jeho vierovyznanie. Lokalizačné údaje môžu napomôcť aj ku zisteniu informácií o zdravotnom stave prostredníctvom návštevy zdravotníckych zariadení či laboratórií na odber biologického materiálu. Z týchto údajov slovami SDEÚ..."*možno vyvodiť presné závery týkajúce sa súkromného života osôb, ktorých údaje boli uchovávané, ako ich každodenné zvyklosti, miesta ich trvalého alebo prechodného pobytu, denné alebo iné presuny, vykonávané činnosti, spoločenské vzťahy týchto osôb a spoločenské kruhy, v ktorých sa pohybujú."*[84]

[84] Rozhodnutie Súdneho dvora Európskej únie, Spojené veci C-293/12 a C-594/12 Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources a i. a Kärntner Landesregierung a i., bod 27.

Špecifickým prípadom sú aj štátne orgány, ktoré častokrát k takýmto údajom majú sprostredkovaný prístup cez telekomunikačných operátorov. Avšak tento prístup podlieha prísnym mantinelom, ktoré nastavila judikatúra. Ku otázkam bezpečnosti v intenciách práva na súkromie sa opakovane vyjadrujú aj súdne inštancie, aj keď nie vždy to robia priamo.

SDEÚ vo veci *Digital Rights Ireland*, skúmal otázku bezpečnosti ako sekundárny cieľ, ktorý mala zabezpečiť smernica o uchovávaní údajov. Táto smernica po teroristických útokoch na európskom kontinente umožňovala orgánom činným v trestnom konaní vyžadovať meta-údaje z telekomunikačnej prevádzky (lokalizačné údaje či prevádzkové údaje, teda nie obsah prenášaných správ) a využiť ich na účely prevencie voči terorizmu. Problémom v tomto prípade bolo, že smernica neustanovovala adekvátnu dobu uchovávania údajov a umožňovala plošný zber údajov účastníkov telekomunikačnej prevádzky bez ohľadu na odôvodnenie obavy z trestne činnosti u konkrétneho jednotlivca. SDEÚ výslovne v bode 40 rozhodnutia uviedol:

> *„Toto uchovávanie údajov nemôže tiež zasiahnuť do podstaty základného práva na ochranu osobných údajov zakotveného v článku 8 Charty, pretože smernica 2006/24 vo svojom článku 7 stanovuje pravidlo* ***týkajúce sa ochrany a bezpečnosti údajov****, podľa ktorého poskytovatelia verejne dostupných elektronických komunikačných služieb alebo verejnej komunikačnej siete bez toho, aby boli dotknuté ustanovenia prijaté na uplatnenie smerníc 95/46 a 2002/58, musia dodržať určité* ***zásady ochrany a bezpečnosti údajov****, podľa ktorých členské štáty dbajú na to, aby sa prijali vhodné technické a organizačné opatrenia proti náhodnému alebo nezákonnému zničeniu, ako aj proti strate či náhodnej zmene údajov.*"

Aspekt bezpečnosti údajov si SDEÚ odvodil od sekundárneho cieľa smernice, ktorá vychádzala a primárne zasahovala do práva na súkromie v zmysle článku 7 Charty. SDEÚ z dôvodov nedostatočnej kvality vyžadovaných bezpečnostných opatrení túto smernicu zrušil pre nesúlad s právom na súkromie. Judikatúra tak pomerne nahlas vyžaduje splnenie minimálneho bezpečnostného štandardu pri zásahoch do súkromia. Predmetnú požiadavku možno zasadiť do širšieho rámca v EÚ a konštatovať, že požiadavky na kybernetickú

bezpečnosť v súvislosti s jednotlivcami možno rámcovať okrem iného aj právom na súkromie.[85]

Túto požiadavku opakovane zvýrazňuje aj Ústavný súd Slovenskej republiky. Naposledy tak urobil pri otázke prístupu Úradom verejného zdravotníctva SR ku údajom o polohe od telekomunikačných operátorov za účelom ochrany života a zdravia pri boji s pandémiou šírenia nebezpečne nákazlivej choroby COVID-19:[86]

> *„Zabezpečenie **mimoriadne vysokej úrovne ochrany a bezpečnosti** pomocou technologických a organizačných opatrení znamená, že čím sú údaje citlivejšie, tým je potrebnejšie trvať na kvalitnejších spôsoboch ochrany údajov proti zneužitiu (napr. formou asymetrického šifrovania, implementovaním certifikácie v oblasti bezpečnosti, obmedzením prístupu k údajom alebo vyškolením zodpovedných osôb). Bezpečnostné záruky pritom musia byť upravené osobitne a zodpovedať najnovším vysokým štandardom používaným v odborných kruhoch (porovnaj rozhodnutie Spolkového ústavného súdu Nemecka Vorratsdatenspeicherung, sp. zn. 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, body 224 a 225).*"

Na vyššie uvedené závery Ústavný súd SR nadviazal aj v prípade, ktorý sa týkal zberu údajov Finančnou správou SR prostredníctvom elektronickej registračnej pokladnice (tzv. eKasa). Aj v tomto prípade Ústavný súd SR judikoval, že pri orgánoch verejnej moci je požiadavka vysokej úrovne bezpečnosti pri spracúvaní údajov jednou z esenciálnych záruk proti zneužitiu. Ako rôzne formy bezpečnostných záruk nález uvádza asymetrické šifrovanie, certifikácia v oblasti bezpečnosti, obmedzenie prístupu k údajom alebo vyškolenie zodpovedných osôb.[87]

V slovenskej republike je situácia ešte špecifickejšia, keďže existuje osobitná právna úprava, ktorá je ekvivalentom legislatívy kybernetickej bezpečnosti a týka sa orgánov verejnej moci. Reč je o zákone č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov, ktorému sa budeme ešte v tejto učebnici

[85] Pozri k tomu diskusiu v LYNSKEY, O.: The Foundations of EU Data Protection Law. Oxford: Oxford University Press, 2015, s. 271 a nasl.
[86] Uznesenie Ústavného súdu SR, sp. zn. PL. ÚS 13/2020, bod. 93.
[87] Nález Ústavného súdu SR, sp. zn. PL. ÚS 25/2019-117, bod 106.

venovať. Požiadavky na bezpečnosť pri orgánoch verejnej moci sú tak do určitej miery zabezpečené práve súladom s týmto zákonom.

Ako uzatvára aj Ústavný súd SR:

> *„Tieto povinnosti sú realizáciou **ústavnej povinnosti štátu aktívne chrániť dôvernosť a integritu informačných systémov, ktoré obsahujú osobné údaje jednotlivca**. Právo na ochranu dôvernosti a integrity informačných systémov predstavuje súčasť ochrany podľa čl. 19 ods. 3 a čl. 22 ústavy (podobne BVerfG, 1 BvR 370/07, 1 BvR 595/07, BVerfG 120). Zároveň sú tieto opatrenia predpokladom akceptovateľného závažného zásahu do práva na ochranu osobných údajov (SDEÚ, Digital Rights Ireland, C-293/12 and C-594/12, ods. 66 – 67).*[88]

2.3.2 Právo na ochranu osobných údajov

Právo na súkromie a právo na ochranu osobných údajov sú práva, ktoré sa či už v praxi alebo odbornej spisbe častokrát zamieňajú prípadne sa s nimi pracuje ako so synonymami. Takýto prístup však nie je správny, nakoľko medzi nimi z hľadiska obsahu existujú určité rozdiely[89] a navyše, Charta základných práv EÚ obe práva upravuje samostatne.

Právo na ochranu osobných údajov je zakotvené v článku 8 Charty, na základe ktorého:

> *„1. Každý má právo na ochranu osobných údajov, ktoré sa ho týkajú*
>
> *2. Tieto údaje musia byť riadne spracované na určené účely na základe súhlasu dotknutej osoby alebo na inom oprávnenom základe ustanovenom zákonom. Každý má právo na prístup k zhromaždeným údajom, ktoré sa ho týkajú, a právo na ich opravu.*
>
> *3. Dodržiavanie týchto pravidiel podlieha kontrole nezávislého orgánu.*"

Tieto požiadavky sú ďalej pretavené v sekundárnom práve EÚ, kde sa konkrétnym inštitútom venujeme v samostatnej kapitole tejto učebnice.

---

[88] Tamže, bod 111.

[89] Bližšie pozri FUSTER, G., HIJMANS, H.: The EU rights to privacy and personal data protection: 20 years in 10 questions. Discussion paper. Dostupné na: https://brusselsprivacyhub.eu/events/20190513.Working_Paper_Gonza%CC%81lez_Fuster_Hijmans.pdf.

Ak však chceme diskutovať normatívny ľudsko-právny rámec práva na ochranu osobných údajov v kontexte kybernetickej bezpečnosti, je nevyhnutné spomenúť niekoľko kľúčových rozhodnutí a názorov SDEÚ, ktoré sa týkajúce cezhraničných prenosov osobných údajov do tretích krajín.

Cezhraničné prenosy osobných údajov do tretích krajín reflektujú situáciu, ak dochádza ku transferu osobných údajov mimo členské štáty Európskej únie a Európskeho hospodárskeho priestoru. V takom prípade musí prevádzkovateľ osobných údajov nájsť vhodný právny titul pre legálne vykonanie takéhoto cezhraničného prenosu.[90] Často využívané tituly predstavujú tzv. rozhodnutia o primeranosti vydané Európskou komisiou (*adequacy decisions*) alebo osobitné medzinárodné zmluvy. Práve v kontexte týchto nástrojov SDEÚ judikoval určité východiská týkajúce sa zabezpečenia dát.

Z hľadiska medzinárodných dohôd a ich prieskumu je zaujímavý prípad, ktorý sa týkal bilaterálnej zmluvy medzi EÚ a Kanadou o výmene údajov v leteckej doprave.[91] Napriek tomu, že SDEÚ bol pomerne kritický pri splnení náležitostí pre cezhraničné prenosy vyplývajúcich z Charty, parametre na bezpečnosť údajov považoval za splnené:

> *„Napokon, na jednej strane pokiaľ článok 9 ods. 2 zamýšľanej dohody, ktorý stanovuje, že Kanada uchováva údaje z PNR „**vo fyzicky bezpečnom prostredí, ktoré je chránené kontrolou prístupu**", znamená, že tieto údaje musia byť uchovávané na území Kanady, a na druhej strane pokiaľ sa článok 16 ods. 6 tejto dohody, podľa ktorého po uplynutí obdobia na uchovávanie údajov z PNR Kanada tieto údaje zlikviduje, má chápať v tom zmysle, že ukladá povinnosť nenávratne tieto údaje zničiť, možno usúdiť, že tieto ustanovenia uvedenej dohody spĺňajú požiadavky jasnosti a presnosti."*[92]

V dvojici rozhodnutí SDEÚ, ktoré sa týkali posúdenia súladu rozhodnutí o primeranosti vydané pre USA luxemburský súd dvakrát rozhodol, že prijaté rozhodnutia

[90] Bližšie pozri kapitolu Cezhraničné prenosy osobných údajov v MESARČÍK, M.: Ochrana osobných údajov. Učebnica. 1. vydanie. Bratislava: C.H. BECK, 2020, s. 133 – 147.
[91] Súdny dvor EÚ, STANOVISKO 1/15 SÚDNEHO DVORA (veľká komora) z 26. júla 2017.
[92] Tamže, bod 210.

o primeranosti nie sú v súlade so štandardom zakotveným v Charte.[93] Vzhľadom na to, že tieto štandardy obsahujú aj požiadavky na bezpečnosť údajov, vrátane prístupu orgánov verejnej moci k nim, takýmto spôsobom sa prejavuje značný extra-teritoriálny vplyv práva na ochranu osobných údajov aj mimo hraníc EÚ. Zároveň, jednotlivé dozorné orgány v členských štátoch EÚ môžu na základe porušenia požiadaviek GDPR vrátane bezpečnosti pozastaviť cezhraničné prenosy z tretích krajín.[94] Tieto požiadavky sa však netýkajú iba rozhodnutí o primeranosti, ale aj ďalších nástrojov pre cezhraničné prenosy. Pri posúdení úrovne tretej krajiny je preto vhodné, že ak prevádzkovateľ identifikuje odstrániteľné nedostatky, jednou z možností je implementácia dodatočných technických bezpečnostných záruk pre spracúvanie a uchovávanie údajov.[95]

Na základe vyššie uvedeného je možné uzavrieť, že EÚ v rámci svojich pravidiel na ochranu osobných údajov pri cezhraničných prenosoch explicitne vyžaduje splnenie určitých záruk, ktoré sa okrem iného týkajú aj bezpečnosti prenášaných dát a ich spracúvania v tretích krajinách.

2.3.3 Právo na informácie

Na prvý pohľad sa možno nejaví, že kybernetická bezpečnosť môže v určitej miere súvisieť aj so slobodou prejavu a právom na informácie, avšak opak je pravdou. Sloboda prejavu a prístup ku informáciám má v európskej právnej kultúre výsostné postavenie limitované inými právami a slobodami. Charta základných práv EÚ dané základné právo upravuje v článku 11:

> *„1. Každý má právo na slobodu prejavu. Toto právo zahŕňa slobodu zastávať názory a **prijímať** a rozširovať **informácie** a myšlienky bez zasahovania orgánov verejnej moci a bez ohľadu na hranice.*
> *2. Rešpektuje sa sloboda a pluralita médií.*"

[93] Pozri Súdny dvor EÚ, C-311/18 Data Protection Commissioner proti Facebook Ireland Ltd, Maximillianovi Schremsov a C-362/14 Maximillian Schrems proti Data Protection Commissioner.
[94] Súdny dvor EÚ, C-311/18 Data Protection Commissioner proti Facebook Ireland Ltd, Maximillianovi Schremsov, body 118 – 120.
[95] EUROPEAN DATA PROTECTION BOARD: Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Version 2.0. Adopted on 18 June 2021, s. 21.

V kontexte kybernetickej bezpečnosti považujeme za nevyhnutné upriamiť pozornosť na aspekt prijímania informácií, predovšetkým zo strany jednotlivcov, či už v podobe občana alebo dotknutej osoby. Máme za to, že jednotlivci musia byť primeraným spôsobom informovaní o súvislostiach týkajúcich sa kybernetickej bezpečnosti. Tieto informačné povinnosti možno na pedagogické účely diferencovať na:

a) informácie týkajúce sa bezpečnostných incidentov; a
b) informácie týkajúce sa kybernetickej bezpečnosti vo všeobecnosti.

V prvom rade majú jednotlivci právo na informácie **týkajúce sa bezpečnostných incidentov**. Táto povinnosť má dve modality. Prvá modalita sa týka poskytnutia informácií o konkrétnom bezpečnostnom incidente konkrétnej množine osôb, ktorej sa incident týka. To znamená, že ak by došlo ku hackerskému útoku na orgán verejnej moci alebo službu, v ktorej sú spracúvané údaje dotknutej osoby, táto osoba má právo vedieť, že sa takýto incident odohral a aké opatrenia napadnutá inštitúcia prijala. Predmetná povinnosť je už dnes bežnou súčasťou právneho rámca a bude predmetom výkladu v ďalších kapitolách. Druhá modalita informačnej povinnosti sa týka poskytnutia všeobecných informácií a štatistických ukazovateľov o útokoch na konkrétnu organizáciu. Užívateľ alebo občan tak má možnosť posúdiť bezpečnosť a schopnosť odolnosti systémov, v ktorých sú jeho osobné údaje uchovávané a spracúvané.

V druhom rade majú jednotlivci právo na informácie týkajúce sa kybernetickej bezpečnosti vo všeobecnosti. Tieto informácie by mali byť predovšetkým zverejnené orgánmi verejnej moci a štátom v podobe strategických dokumentov či správ o kybernetickej bezpečnosti. V podmienkach Slovenskej republiky takéto správy na ročnej báze publikuje Národný bezpečnostný úrad SR.[96]

[96] Pozri napríklad NÁRODNÝ BEZPENOŠTNÝ ÚRAD SR: Správa o kybernetickej bezpečnosti v Slovenskej republike v roku 2023. Dostupné na: https://www.nbu.gov.sk/sprava-o-kybernetickej-bezpecnosti-v-slovenskej-republike-v-roku-2023/.

3. PRÁVNA ÚPRAVA KYBERNETICKEJ BEZPEČNOSTI

Na právnu úpravu kybernetickej bezpečnosti možno vo všeobecnosti nazerať dvoma spôsobmi. V prvom prípade možno právnu úpravu kybernetickej bezpečnosti chápať najmä v kontexte technických a organizačných opatrení, prostredníctvom ktorých dôjde k identifikácii osoby, ktorá spôsobila kybernetický bezpečnostný incident. Na druhej strane existuje prístup k právu kybernetickej bezpečnosti, kedy sa prostredníctvom technických a organizačných opatrení zabezpečuje ochrana prostredia, bez toho, aby bolo potrebné vedieť identifikovať užívateľov či osoby, ktoré spôsobili kybernetický bezpečnostný incident. Zatiaľ, čo prvý prístup je príznačný pre Spojené štáty americké či štáty Južnej Ameriky, neskôr spomínaný prístup je príznačný pre Európu, a teda aj pre Slovenskú republiku.[97]

Právnu úprava kybernetickej bezpečnosti na úrovni EÚ, ako aj Slovenskej republiky možno prirovnať k predpisom protipožiarnej ochrany, ktorých zmyslom je ukladať povinnosti konkrétnym subjektom, tak aby dodržiavali konkrétne bezpečnostné opatrenia a prijali také detekčné a reaktívne mechanizmy, ktoré by kybernetické bezpečnostné incidenty efektívne identifikovali, čo najrýchlejšie vyriešili a negatívne následky kybernetických bezpečnostných incidentov odstránili. Následná identifikácia páchateľov a ich postih je už predmetom iných právnych predpisov.[98]

3.1 Právo kybernetickej bezpečnosti - pojem

V odbornej a vedeckej literatúre možno len zriedkavo nájsť definíciu práva kybernetickej bezpečnosti. Jedným z autorov, ktorý definuje právo kybernetickej bezpečnosti je Jeff Kosseff. Podľa tohto autora predstavuje **právo kybernetickej bezpečnosti**:

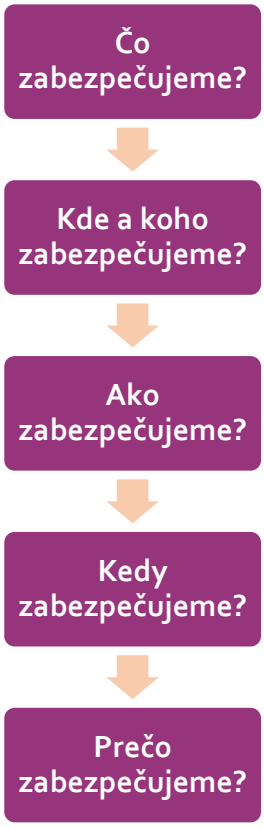
> *„právny rámec, ktorý zabezpečuje dôvernosť, integritu a dostupnosť verejných a súkromných informácií, systémov a sietí prostredníctvom nadčasovej regulácie*

[97] POLČÁK, R.: Kybernetická bezpečnosť. In POLČÁK, R.: a kol. *Právo informačných technológií*. Praha: Wolters Kluwer ČR, 2018, s. 587.
[98] Důvodová zpráva k návrhu zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Dostupné na: https://www.psp.cz/sqw/text/tiskt.sqw?o=7&ct=81&ct1=0.

a stimulov, s cieľom chrániť práva a súkromie jednotlivcov, ekonomické záujmy a národnú bezpečnosť."[99]

Hoci ide o veľmi širokú definíciu, ktorej autor sa zaoberá právom kybernetickej bezpečnosti z pohľadu anglo-amerického právneho systému, pre účely tejto učebnice je dostačujúca a môže tvoriť vhodný základ pre pochopenie práva kybernetickej bezpečnosti.

Predmetná definícia je výsledkom zodpovedania **piatich základných otázok**, ktorými sú:



Čo zabezpečujeme?

Právo kybernetickej bezpečnosti by malo zabezpečiť dôvernosť, integritu a dostupnosť informácií, systémov a sietí. Potreba chrániť nielen informácie a údaje, ale aj systémy a siete je zvýraznená tým, že čoraz viac fyzických zariadení je pripojených do siete internet.[100]

[99] KOSSEFF, J.: *Defining Cybersecurity Law*. *In* Iowa Law Review. 2018, 103: 985, 2018, s. 1010.
[100] Tamže, s. 995-996.

Kde a koho zabezpečujeme?

Je potrebné zodpovedať na otázku, aké druhy informácií, systémov a sietí majú byť chránené právom kybernetickej bezpečnosti. Má byť právna úprava kybernetickej bezpečnosti zameraná skôr na verejný sektor? Alebo by sa mali rovnaké požiadavky aplikovať aj na súkromný sektor? Zákonné požiadavky na kybernetickú bezpečnosť verejnej infraštruktúry sa môžu odlišovať od požiadaviek na kybernetickú bezpečnosť súkromnej infraštruktúry. Avšak tvorcovia legislatívy v oblasti kybernetickej bezpečnosti si musia uvedomiť, že bezpečnosť alebo nedostatočná úroveň bezpečnosti systémov, sietí a informácií súkromného sektora môže ovplyvniť aj siete a systémy vo verejnom sektore.[101]

Ako zabezpečujeme?

Cieľom práva kybernetickej bezpečnosti je zabezpečiť dôvernosť, integritu a dostupnosť verejných a súkromných informácií, systémov a sietí. Avšak ako tento cieľ dosiahnuť? Právo kybernetickej bezpečnosti môže byť regulované právnymi predpismi, ktoré ukladajú povinnosti konkrétnym subjektom v podobe prijatia bezpečnostných opatrení a plnenia iných povinností. V prípade porušenia týchto povinností je týmto subjektom uložená sankcia. Avšak vyššie uvedený cieľ možno dosiahnuť aj inými právnymi predpismi, ktoré budú subjekty motivovať, aby implementovali konkrétne bezpečnostné opatrenia.[102]

PRÍKLAD
Štát môže prijať právnu úpravu, ktorá vytvorí daňové stimuly pre výrobcov robotických doručovacích zariadení, ak ich budú vyrábať pri dodržiavaní konkrétnych bezpečnostných opatrení.

Kedy zabezpečujeme?

Právo kybernetickej bezpečnosti by malo reagovať nielen na už vzniknuté kybernetické bezpečnostné incidenty, ale malo by pôsobiť aj preventívne, tak aby k takýmto incidentom dochádzalo čo najmenej. Taktiež by právna úprava kybernetickej bezpečnosti mala obsahovať inštitúty, ktoré by po vzniknutom kybernetickom bezpečnostnom incidente pomohli danému subjektu, čo najrýchlejšie vyriešiť kybernetický bezpečnostný incident a čo

[101] Tamže, s. 999.
[102] Tamže, s. 1001.

najskôr odstrániť následky kybernetických bezpečnostných incidentov. Takúto právnu úpravu možno označiť za nadčasovú, ktorá reaguje nielen na už vzniknutú situáciu, ale snaží sa jej predchádzať.[103]

Prečo zabezpečujeme?

Právna úprava kybernetickej bezpečnosti by mala v prvom rade zabezpečiť, aby sa predchádzalo vzniku ujmy, resp. zmierňovala sa už vzniknutá ujma, ktorá môže vzniknúť **jednotlivcom** ako následok kybernetického bezpečnostného incidentu.

PRÍKLAD
Kybernetické bezpečnostné incidenty, ktoré môžu mať dopad na fyzické osoby, môžu byť v podobe porušenia ochrany osobných údajov, nemožnosti využívať základné služby ako preprava osôb, obmedzený prístup k pitnej vode, energiám a pod.

Ďalším dôvodom prijatia právnej úpravy kybernetickej bezpečnosti je zabrániť **ekonomickým škodám**, ktoré môžu byť následkom kybernetického bezpečnostného incidentu.

PRÍKLAD
Jeden prieskum uskutočnený v 30 krajinách ukázal, že celkové náklady na nápravu ransomvérového útoku sa výrazne zvýšili, zo 761 106 USD v roku 2020 na 1,85 milióna USD v roku 2021.[104]

V neposlednom rade by malo právo kybernetickej bezpečnosti reflektovať aj **bezpečnosť štátu**. Kybernetické útoky môžu byť namierené aj na kritickú infraštruktúru štátu.

[103] Tamže, s. 1006 -1007.

[104] ENISA: *ENISA threat landscape 2021*. 2021, s. 40. Dostupné na: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

PRÍKLAD

Ako príklad možno uviesť kybernetické útoky na ukrajinské energetické spoločnosti v roku 2016, ktoré spôsobili výpadok elektrickej energie pre vyše 700 000 ľudí na niekoľko hodín.[105]

V súvislosti s právom kybernetickej bezpečnosti taktiež vzniká otázka, či je právo kybernetickej bezpečnosti **samostatným právnym odvetvím** právneho poriadku alebo zmesou právnych predpisov z iných právnych odvetví, ako správne právo, občianske právo, obchodné právo či trestné právo. A je odpoveď na túto otázku vôbec dôležitá? Ottová vymedzuje znaky samostatného právneho odvetvia tak, že (i) upravuje určitú oblasť spoločenského života alebo vzťahov – spoločný predmet, (ii) má špecifickú metódu regulácie a (iii) úlohu jednotiaceho prvku zohrávajú komplexné právne predpisy alebo kódexy. Tretia požiadavka však neplatí absolútne.[106] Vo všeobecnosti možno konštatovať, že právo kybernetickej bezpečnosti všetky tieto znaky napĺňa. Upravuje určitú oblasť spoločenského života alebo vzťahov, ktorých cieľom je zaistenie dôvernosti, integrity a dostupnosti verejných a súkromných informácií, systémov a sietí. Kybernetická bezpečnosť ako normatívny koncept nemá vo fyzickom svete obdobu. Avšak v práve je možné vytvoriť aj nové fenomény, ktoré v reálnom svete nemajú paralelu, pričom právo nemusí brať do úvahy kvalitu reálneho sveta, ale môže vytvoriť aj normatívne koncepty bez ohľadu na skutočnosť. Takýmto príkladom je práve zavedenie pojmu kybernetickej bezpečnosti.[107] Ako budeme vidieť v ďalšej časti učebnice, právo kybernetickej bezpečnosti reguluje spoločenské vzťahy nielen právnymi normami, ale aj inými regulačnými nástrojmi, ako je súťaž, konsenzus (*consensus*), komunikácia či kód. Analýza právnej úpravy kybernetickej bezpečnosti nám ukáže, že na úrovni práva EÚ či vnútroštátneho poriadku Slovenskej republiky sú prijaté komplexné právne predpisy z tejto oblasti a čiastkové problematiky sú upravené špecificky v iných právnych predpisoch.

Avšak z praktického hľadiska dnes nie je dôležité poskytnúť vyčerpávajúcu odpoveď na otázku, či je právo kybernetickej bezpečnosti samostatným právnym odvetvím. Oveľa

[105] WILLIAMS, B. K.: *Cyberattack on Ukrainian power company a 'coordinated effort*'. Dostupné na: https://thehill.com/policy/cybersecurity/265394-cyberattack-on-ukrainian-power-company-a-coordinated-effort.

[106] OTTOVÁ, E.: *Teória práva*. 1. vyd. Bratislava: Heuréka, 2010, s. 228.

[107] POLČÁK, R.: Kybernetická bezpečnosť. In POLČÁK, R. a kol.: *Právo informačných technológií*. Praha: Wolters Kluwer ČR, 2018, s. 587.

dôležitejším aspektom je, aby tvorcovia legislatívy v oblasti kybernetickej bezpečnosti rozumeli na dostačujúcej úrovni technológiám a základom kybernetickej bezpečnosti, tak aby prijímali flexibilnú a nadčasovú právnu úpravu, ktorá bude reagovať na nové kybernetické hrozby. V tejto súvislosti je nevyhnutné, aby pri tvorbe tak dôležitých právnych predpisov, akými právne predpisy z oblasti kybernetickej bezpečnosti sú, tvorcovia legislatívy využili poznatky odborníkov z oblasti informačných a komunikačných technológií či práva. Pochopiteľne by mali na dostačujúcej úrovni rozumieť technológiám a základom kybernetickej bezpečnosti aj orgány aplikácie práva, ktoré v rámci svojej rozhodovacej činnosti môžu rozhodovať o rôznych aspektoch kybernetickej bezpečnosti.

3.2 Regulačné nástroje kybernetickej bezpečnosti

V oblasti kybernetickej bezpečnosti vystupuje mnoho zainteresovaných subjektov. V prvom rade možno uviesť tvorcov pravidiel kybernetickej bezpečnosti, príjemcov týchto pravidiel, či osoby, ktoré je potrebné chrániť pred kybernetickými útokmi, ako aj osoby, ktoré je potrebné informovať o bezpečnostných incidentoch. Čo sa týka technológií, ktoré je potrebné chrániť, pôjde najmä o IKT danej organizácie. Medzi procesy, ktoré zabezpečujú úroveň dostatočnej úrovne kybernetickej bezpečnosti možno zaradiť napr. riadenie aktív a rizík, správu užívateľov a ich rolí, audit kybernetickej bezpečnosti, reakcie na kybernetické útoky a ďalšie. Pre oblasť kybernetickej bezpečnosti je príznačné prijímanie bezpečnostných opatrení, ktoré majú odvrátiť hrozby, resp. zmierniť následky úspešného kybernetického bezpečnostného incidentu. Nemenej dôležitou časťou je detekcia a následná reakcia na úspešné kybernetické incidenty.

Pri pohľade na všetky zainteresované subjekty, ich záujmy v oblasti kybernetickej bezpečnosti, pri pohľade na všetky technológie a jednotlivé procesy, ktoré sa v tejto oblasti zavádzajú, vzniká otázka, či problematika kybernetickej bezpečnosti môže byť vyriešená len prijatím legislatívnych aktov alebo existujú aj iné nelegislatívne regulačné nástroje, prostredníctvom ktorých dochádza k regulácii tejto oblasti.

Yeung a Ranchordás rozlišujú medzi 5 regulačnými nástrojmi. Konkrétne:

- právne normy,
- súťaž,
- konsenzus,

- komunikácia,
- kód,

Prvým nástrojom regulácie sú pochopiteľne **právne normy,**[108] ktoré sú obsiahnuté najmä v legislatívnych aktoch prijatých na úrovni EÚ, ako aj Slovenskej republiky. V prípade kybernetickej bezpečnosti by sme mohli právne normy rozdeliť do troch kategórií, a to na základe toho, akým spôsobom majú regulovať správanie adresátov týchto právnych noriem. Konkrétne ide o:

- právne normy, ktoré určujú, aký **výsledok** má adresát týchto právnych noriem dosiahnuť,
- právne normy, ktoré presne stanovujú, aké **nástroje** má adresát právnych noriem použiť,
- právne normy, ktoré stanovujú, aký **postup** má adresát právnych noriem použiť.[109]

Pri identifikácii týchto druhov právnych noriem je vždy potrebné vychádzať z kontextu, nakoľko sa niektoré druhy môžu prelínať, a to najmä v prípade právnych noriem, ktoré určujú výsledok a právnych noriem, ktoré určujú nástroje.

PRÍKLAD

Ako príklad možno uviesť ustanovenie z návrhu zákona o bezpečnosti a súkromí vo vozidle z roku 2015[110], kde je v právnej norme uvedené: *„Každé motorové vozidlo, ktoré má vstupný bod, musí byť vybavené schopnosťami okamžite detegovať, hlásiť a zastaviť pokusy o zachytenie jazdných údajov alebo o prevzatie kontroly nad vozidlom."*[111]

[108] Reguláciu prostredníctvom príkazov možno označiť za klasickú formu regulácie, resp. „command and control" reguláciu. Je založená na tom, že autoritatívny orgán, typicky štát alebo zákonodarca, stanovuje záväzné pravidlá správania, ktorými určité konanie prikazuje alebo zakazuje. Dodržiavanie týchto pravidiel je zabezpečené právnymi sankciami, ktoré môžu mať občianskoprávnu alebo trestnoprávnu povahu. Výhodou tohto modelu je najmä jasnosť povinností, stabilita regulačného rámca, vyššia miera verejnej kontroly a silná legitimita najmä v krízových situáciách. Zároveň však môže viesť k nadmernému množstvu detailných pravidiel, vyšším administratívnym nákladom, neefektívnosti a obmedzeniu inovácií, keďže tvorba, monitorovanie a vynucovanie pravidiel si vyžadujú značné zdroje. Napriek týmto nedostatkom zostáva tento spôsob regulácie významný, osobitne tam, kde existuje nezávislé súdnictvo, účinné vynucovanie práva a dôvera v princípy právneho štátu. Bližšie pozri YEUNG, K. a RANCHORDÁS, S.: *An introduction to law and regulation. Texts and materials. Second edition.* Cambridge: Cambridge University Press; 2024, s. 169 - 170.

[109] SCHELLEKENS, M. *Car hacking: Navigating the regulatory landscape. In* Computer Law and Security Review. 2015, roč. 32, č. 2, s. 307-315.

[110] Návrh zákona o bezpečnosti a súkromí vo vozidle z roku 2015, ktorý bol prijatý v USA. Dostupné na: https://www.congress.gov/bill/114th-congress/senate-bill/1806/text. Návrh zákona bol v roku 2015 predložený v Senáte USA, no nebol prijatý ako federálny zákon. Avšak slúžil ako základný rámec pre moderné diskusie o kybernetickej bezpečnosti v automobilovom priemysle a ochrane súkromia spotrebiteľov.

[111] § 30129, ods. 4 zákona o bezpečnosti a súkromí vo vozidle z roku 2015.

Predstavuje schopnosť: *„detegovať, hlásiť a zastaviť"* výsledok alebo je možná interpretácia v zmysle, že je potrebné prijať opatrenia, ktoré zabezpečia odhalenie, nahlásenie, zachytenie? Oba výklady sú v tomto prípade akceptovateľné.[112]

Použitie právnych noriem, ktoré **nestanovujú presný špecifický spôsob**, akým sa má dosiahnuť konkrétny výsledok, sú pre oblasť kybernetickej bezpečnosti príznačné. Pravidlá, ktoré nestanovujú konkrétny spôsob splnenia povinnosti, pričom je jej výkon ponechaný na regulovaný subjekt, sa nazývajú performatívne pravidlá.

PRÍKLAD

Smernica NIS v oblasti bezpečnostných požiadaviek stanovovala pre členské štáty povinnosť, aby: *„prevádzkovatelia základných služieb prijali vhodné a primerané technické a organizačné opatrenia na riadenie rizík súvisiacich s bezpečnosťou sietí a informačných systémov, ktoré využívajú vo svojej prevádzke."*[113]

Smernica NIS2 stanovuje povinnosť pre kľúčové a dôležité subjekty prijať: *„vhodné a primerané technické, operačné a organizačné opatrenia na riadenie rizík súvisiacich s bezpečnosťou sietí a informačných systémov, ktoré tieto subjekty využívajú na svoju činnosť alebo na poskytovanie svojich služieb a na prevenciu alebo minimalizáciu vplyvu incidentov na príjemcov ich služieb a na ďalšie služby*."[114]

V zmysle nariadenia eIDAS[115] majú kvalifikovaní a nekvalifikovaní poskytovatelia dôveryhodných služieb prijať: *„vhodné technické a organizačné opatrenia na riadenie rizík ohrozujúcich bezpečnosť dôveryhodných služieb, ktoré poskytujú*."[116]

Ako môžeme vidieť z vyššie uvedených príkladov, výpočet konkrétnych opatrení, ktoré majú byť realizované, chýba. Je na členských štátoch, aké bezpečnostné požiadavky

[112] Uvedený príklad vychádza z príkladu uvedeného v SCHELLEKENS, M. *Car hacking: Navigating the regulatory landscape. In* Computer Law and Security Review. 2015, roč. 32, č. 2, s. 311.
[113] Smernica NIS. čl. 14.
[114] Smernica NIS 2, čl. 21 ods. 1.
[115] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES.
[116] Nariadenie eIDAS, čl. 19 ods. 1.

budú od konkrétnych subjektov vyžadovať, avšak tieto požiadavky musia dosiahnuť stanovený cieľ.

PRÍKLAD

Ďalším príkladom, kedy sa nestanovuje presný špecifický spôsob, akým sa má dosiahnuť konkrétny výsledok, je ustanovenie návrhu zákona o bezpečnosti a súkromí vo vozidle z roku 2015, v ktorom je uvedené, že: *„všetky údaje o jazde zozbierané elektronickými systémami zabudovanými do motorových vozidiel musia byť primerane zabezpečené, aby sa zabránilo neoprávnenému prístupu:*

„(A) počas uchovávania takýchto údajov na palube vozidla;

„(B) počas prenosu takýchto údajov z vozidla na iné miesto; a

„(C) pri akomkoľvek následnom uchovávaní alebo používaní mimo vozidla."[117]

V prípade právnych noriem, ktoré sú zamerané na konkrétne **nástroje**, ktoré má adresát právnych noriem použiť, dochádza k povinnosti realizovať konkrétne bezpečnostné opatrenia zo strany subjektov.

PRÍKLAD

Ako príklad možno uviesť predpis OSN č. 155, ktorý uvádza konkrétne opatrenia, ktoré je potrebné realizovať v prípade rôznych hrozieb. Ak sú napr. hrozbou médiá, ktoré sú infikované vírusmi a tieto médiá sú pripojené k vozidlu, tak bezpečnostným opatrením sú bezpečnostné kontroly, ktoré sa budú uplatňovať na externé rozhranie.[118]

Popri právnych normách, ktoré sú zamerané na výsledok a konkrétne nástroje, sú v právnych predpisoch z oblasti kybernetickej bezpečnosti aj právne normy, ktoré stanovujú konkrétne **postupy**, resp. procesné povinnosti.

[117] § 30129, písm. a), ods. 3 Zákona o bezpečnosti a súkromí vo vozidle z roku 2015.

[118] Predpis OSN č. 155 – Jednotné ustanovenia na účely typového schvaľovania vozidiel vzhľadom na kybernetickú bezpečnosť a systém riadenia kybernetickej bezpečnosti [2021/387]. Príloha 5.

PRÍKLAD
Ako príklad možno uviesť predpis OSN č. 155, v zmysle ktorého sa musia dodržiavať najlepšie postupy v oblasti kybernetickej bezpečnosti týkajúce sa vývoja softvéru a hardvéru.[119]

Vyššie uvedený príklad legislatívneho aktu, ktorý nedefinuje, čo možno považovať za najlepšie postupy v oblasti kybernetickej bezpečnosti, nie je nedostatočnou právnou úpravou. Práve naopak. Najlepšie postupy v oblasti kybernetickej bezpečnosti sa môžu s príchodom nových technológií a nových hrozieb meniť. Výhodou takýchto noriem je ich schopnosť promptne reagovať na dynamický charakter hrozieb, ktoré môžu vzniknúť v budúcnosti.

Medzi ďalšie nástroje regulácie možno v zmysle klasifikácie, ktoré použili Yeung a Ranchordás zaradiť súťaž, konsenzus (*consensus*), komunikáciu a kód.[120]

Medzi nástroje **súťaže** možno zaradiť napr. ekonomické nástroje.

PRÍKLAD
Poplatky, dane, dotácie, pokuty a obchodovateľné emisné/vlastnícke práva.[121]

Konsenzus ako regulačný nástroj môže mať formy samoregulácie či rôznych kooperatívnych partnerstiev medzi súkromným a verejným sektorom, ktorých cieľom je regulácia spoločenského správania. Takýto druh regulácie má svoje pozitívne aj negatívne stránky. V prípade kybernetickej bezpečnosti, ktorá sa vyznačuje značným technickým charakterom možno predpokladať, že táto časť priemyslu má viac informačných a odborných kapacít ako štát. Rizikom samoregulácie je, že nie vždy musí dostatočne zachytiť potrebu regulácie konkrétneho správania, resp. nie je tu dostatočný záujem zainteresovaných subjektov o samoreguláciu. Samotná kybernetická bezpečnosť rôznych IKT produktov

[119] Tamže.
[120] YEUNG, K. a RANCHORDÁS, S.: *An introduction to law and regulation. Texts and materials. Second edition.* Cambridge: Cambridge University Press; 2024, s. 171-191.
[121] Tamže, s. 172-173.

nemusí byť vždy prioritou výrobcov. Preto v tejto oblasti nemusí dôjsť k úspešnej samoregulácii.[122]

Ako príklad konsenzu v oblasti kybernetickej bezpečnosti uvádzame technické normy alebo **štandardy,** na ktoré často odkazujú aj legislatívne akty. 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*."[123]

Z hľadiska orgánu, ktorý prijíma konkrétny štandard, možno štandardy rozdeliť na formálne a neformálne. Kým formálne štandardy boli schválené národnými[124], európskymi[125] alebo medzinárodnými štandardizačnými orgánmi[126], neformálne štandardy boli publikované organizáciami pre rozvoj štandardov, ktoré však nie sú uznané za štandardizačné orgány.[127]

PRÍKLAD
V oblasti kybernetickej bezpečnosti bolo prijatých viacero štandardov, či už na národnej, európskej alebo medzinárodnej úrovni. Ide najmä o medzinárodné štandardy prijaté Medzinárodnou organizáciou pre štandardizáciu (ďalej len „ISO"), konkrétne ISO/IEC 27001 Information Security Management, ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls či ISO/IEC 27032:2023 Cybersecurity — Guidelines for Internet security.

[122] Tamže, s. 175. SCHELLEKENS, M. *Car hacking: Navigating the regulatory landscape. In* Computer Law and Security Review. 2015, roč. 32, č. 2, s. 313.
[123] ISO/IEC *Guide 2:2004 Standardization and related activities – General vocabulary,* s. 10.
[124] Zoznam národných štandardizačných orgánov dostupný na: https://standards.cen.eu/dyn/www/f?p=CENWEB:5.
[125] Medzi európske štandardizačné orgány možno zaradiť *European Committee for Standardization* (CEN), *European Committee for Electrotechnical Standardization* (CENEL) a *European Telecommunications Standards Institute* (ETSI).
[126] Medzi medzinárodné štandardizačné orgány možno zaradiť *International Organization for Standardization* (ISO), *International Electrotechnical Commission* (IEC) a *International Telegraph Union* (ITU).
[127] Napr. *American Society for Testing Materials International, Society of Automotive Engineers, Internet Engineering Task Force* a i.

Je však potrebné uviesť, že v prípade medzinárodných štandardov, ako sú ISO štandardy platí, že štáty, ktoré participovali na ich príprave a prijatí, nie sú povinné prijať tieto štandardy ako národné štandardy.

Komunikácia ako regulačný nástroj predstavuje spôsob informovania spotrebiteľov. Môže ísť o povinné informovanie spotrebiteľov o kybernetickej bezpečnosti alebo aj dobrovoľné informovanie.

PRÍKLAD

Príklad, ako informovať napr. vodiča a pasažierov o kybernetickej bezpečnosti jeho vozidla, možno nájsť už v spomínanom návrhu zákona o bezpečnosti a súkromí vo vozidle z roku 2015, v zmysle ktorého musí byť vozidlo vybavené kybernetickým informačným panelom, ktorý: *„prostredníctvom ľahko zrozumiteľnej a štandardizovanej grafiky informuje spotrebiteľov o tom, do akej miery motorové vozidlo chráni kybernetickú bezpečnosť a súkromie majiteľov motorových vozidiel, nájomcov, vodičov a cestujúcich nad rámec minimálnych požiadaviek."*[128]

Funkcie kybernetického bezpečnostného panela v zásade mohla vykonávať palubná doska vozidla (HMI), ktorá bude vodiča a pasažierov informovať o tom, či sú systémy bezpečné.

PRÍKLAD

Ďalším príkladom je akt o kybernetickej bezpečnosti, ktorý zavádza tri úrovne záruky na bezpečnosť produktu IKT, služby IKT a procesu IKT. Konkrétna úroveň záruky je základ pre presvedčenie, že produkt IKT, služba IKT alebo proces IKT spĺňa bezpečnostné požiadavky konkrétneho európskeho systému certifikácie kybernetickej bezpečnosti.

PRÍKLAD

Ďalším spôsobom ako spotrebiteľom ukázať, že konkrétne IKT produkty sú dostatočne zabezpečené, je vyzvať etických hackerov, aby sa pokúsili preniknúť do ich systémov.

Kód - alebo taktiež niekedy nazývaný architektúra - je dôležitou formou regulácie v oblasti kybernetickej bezpečnosti. Dôležitosť kódu ako jednej z modalít regulácie si uvedomoval aj Lessig, ktorý tvrdí, že kód reguluje správanie užívateľov prostredníctvom

[128] § 3 ods. 2 Zákona o bezpečnosti a súkromí vo vozidle z roku 2015.

softvéru a hardvéru. V prípade ak je prístup na webovú stránku podmienený prihlasovacím menom a heslom, pokiaľ nemáte správne heslo, tak sa k obsahu webovej stránky nedostanete.[129]

3.2.1 Regulačný sandbox

Regulačný sandbox v kontexte kybernetickej bezpečnosti predstavuje osobitný regulačný nástroj experimentálnej povahy. Umožňuje kontrolované testovanie nových technológií pod dohľadom príslušného orgánu verejnej moci. Takáto spolupráca medzi súkromným sektorom a verejnou správou predstavuje výhodu pre obe strany. Na jednej strane si súkromná entita vyskúša svoju technológiu bez rizika sankcií a pre verejnú správu regulačný sandbox vytvorí empirické zistenia, na základe ktorých dokáže pristupovať k regulácií. Regulačné sandboxy v súčasnosti už presahujú sektor finančných technológií a sú uplatniteľné aj pre oblasť kybernetickej bezpečnosti, vrátane umelej inteligencie.

Z pohľadu práva kybernetickej bezpečnosti vieme regulačný sandbox definovať ako

1. **časovo ohraničené**
2. **kontrolované testovacie prostredie** pre novú technológiu s potenciálnym dopadom na bezpečnosť sietí a informačných systémov,
3. ktoré je **pod dohľadom príslušného orgánu verejnej moci.**

Adaptívna regulácia v podobe regulačného sandboxu je nevyhnutná v čase, keď sa rapídne rýchlo vyvíjajú nové technológie, nakoľko dokáže rýchlo reagovať na zmeny. Umožňuje testovať nové technológie, znižovať riziká a súčasne vytvárať regulačný rámec založený na reálnych dátach z testovania danej technológie. Tento experimentálny prístup umožňuje zohľadniť aj prvotné reakcie jednotlivcov v reálnom prostredí.

Podľa Európskeho parlamentu má regulačný sandbox dve funkcie:

1. podporuje rozvoj vnútorného trhu
2. pomáha zákonodarcovi formovať právnu úpravu daných technológií.[130]

Regulačný sandbox pozostáva z prípravnej, testovacej a záverečnej fázy. V **prípravnej fáze** príslušný orgán verejnej moci hodnotí, či je záujemca pripravený sa zapojiť

[129] MESARČÍK, M.: *Právo, technológie a informačná spoločnosť. In* HUSOVEC, M., MESARČÍK, M., ANDRAŠKO,J.: Právo informačných a komunikačných technológií 1. Bratislava: TINCT, 2020, s. 20-21.

[130] European Parliamentary Research Service. *Artificial intelligence act and regulatory sandboxes.* Jún 2022, [online] [26.02.2026]. Dostupné na: https://www.europarl.europa.eu/RegData/etudes/BRI E/2022/733544/EPRSBRI(2022)733544EN.pdf.

do regulačného sandboxu na základe predložených dokumentov. Dokumentácia obsahuje podrobný opis novej technológie, jej jedinečnosť, analýzu rizík, ktoré so sebou prináša nová technológia a použitie inovácie na trhu. V rámci dokumentácie záujemca prikladá aj finančný plán, keďže náklady znáša záujemca, pokiaľ nie je určené inak. Ak orgán dohľadu vyhodnotí, že sú splnené všetky požiadavky, tak dohodne so záujemcom stretnuti, na ktorom spoločne naplánujú testovaciu fázu.

V **testovacej fáze** sa realizuje plán testovania, pričom účastník na pravidelnej báze informuje orgán dohľadu o priebehu testovania novej technológie a spolipracuje s ním. Na základe praktických poznatkov si vypracuje mechanizmus na riešenie incidentov. Testovacia fáza trvá podľa dohody medzi účastníkom a orgánom dohľadu, spravidla do dvoch rokov.

V **záverečnej fáze** účastník vypracuje a odovzdá záverečnú správu o testovaní novej technológie v rámci regulačného sandboxu v dohodnutej lehote od ukončenia testovania.[131]

Obrázok č. 4: Prehľad fáz regulačného sandboxu.[132]

V oblasti kybernetickej bezpečnosti význam regulačných sandboxov vzrastá, nakoľko umožňuje identifikovať kybernetické hrozby efektívne pred sprístupnením širokej verejnosti.

[131] Pozri bližšie KOŠŤÁLOVÁ, S.: *Regulatory sandbox ako nástroj pre efektívnu reguláciu automatizovaných vozidiel.* 2025, s. 25. Marec 2025, [online] [26.02.2026]. Dostupné na: https://www.flaw.uniba.sk/fileadmin/praf/Pracoviska/Ustavy/UPITPDV/PST_PI/Regulatory_sandbox_ako_nastroj_pre_efektivnu_regulaciu_AV_Kostalova.pdf

[132] Spracované prostredníctvom Copilot.

Regulačný sandbox týmto spôsobom nebráni rozvoju inovácií, ale napriek tomu nefunguje bez akýchkoľvek hraníc.

PRÍKLAD
Ako príklad v oblasti kybernetickej bezpečnosti je regulačný sandbox britského dozorného orgánu pre ochranu osobných údajov (ICO), ktorý podporuje súkromné entity pri vytváraní produktov a služieb na spracúvanie osobných údajov. Tento regulačný sandbox zahŕňa aj posudzovanie bezpečnosti spracúvania ochrany osobných údajov, implementácie technických a organizačných opatrení, pseudonymizácie, anonymizácie a riadenia kybernetických rizík. Záujemcovia o účasť na regulačnom sandboxe musia preukázať, že ich produkt alebo služba je bezpečná.[133]

Napriek tomu, že v súčasnosti neexistuje regulačný sandbox cielený výlučne na kybernetickú bezpečnosť, väčšina regulačných sandboxov z oblasti ochrany osobných údajov[134] zahŕňajú aj otázky kybernetickej bezpečnosti.

3.3 Princípy právnej úpravy kybernetickej bezpečnosti

Právna úprava kybernetickej bezpečnosti tak na úrovni práva EÚ, ako aj právneho poriadku Slovenskej republiky je založená na nasledujúcich princípoch:[135]

1. princíp technologickej neutrality,
2. princíp ochrany informačného sebaurčenia človeka,
3. princíp ochrany nedistributívnych (verejných) práv,
4. princíp minimalizácie štátneho donútenia,
5. princíp autonómie vôle regulovaných subjektov,

[133] ICO. *Regulatory Sandbox*. [online] [26.02.2026]. Dostupné na: https://ico.org.uk/for-organisations/advice-and-services/regulatory-sandbox/.

[134] Datatilsynet. *Regulatory privacy sandbox*. [online] [26.02.2026]. Dostupné na: https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/; CNIL. *Bac à sable de données personnelles*. Január 2022, [online] [26.02.2026]. Dostupné na: https://www.cnil.fr/fr/bac-sable-donnees-personnelles-la-cnil-lance-un-appel-projets-concernant-les-outils-numeriques; IMY. *Första regulatoriska sandlåda*. Jún 2024, [online] [26.02.2026]. Dostupné na: https://www.imy.se/nyheter/forsta-delrapporten-fran-pilotprojekt-om-ai-regulatorisk-sandlada-publicerad/.

[135] Uvedené princípy sa uplatňujú v českom zákone o kybernetickej bezpečnosti. Zastávame názor, že ich možno do značnej miery aplikovať aj v prípade právnej úpravy kybernetickej bezpečnosti v podmienkach právneho poriadku Slovenskej republiky. Bližšie pozri dôvodová zpráva k návrhu zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Dostupné na: https://www.psp.cz/sqw/text/tiskt.sqw?o=7&ct=81&ct1=0.

6. princíp bdelosti vo vzťahu k ostatným štátom.

Tieto princípy kybernetickej bezpečnosti sú aplikovateľné na právnu úpravu kybernetickej bezpečnosti vo všeobecnosti.

Princíp technologickej neutrality

Princíp technologickej neutrality sa v právnej úprave kybernetickej bezpečnosti prejavuje spôsobom, že vybrané subjekty, ktoré majú povinnosť realizovať konkrétne bezpečnostné opatrenia môžu tieto bezpečnostné opatrenia prijať pri využití rôznych technológií a postupov.[136]

Právna úprava kybernetickej bezpečnosti je neutrálna voči výberu produktov či bezpečnostných riešení od rôznych dodávateľov. Pri uplatňovaní princípu technologickej neutrality sa odlišuje medzi samotným obsahom komunikácie a technológiami, ktoré tento obsah ukladajú či prenášajú. Inými slovami, predmetom úpravy kybernetickej bezpečnosti nie je obsah prenášaných informácií.[137]

PRÍKLAD
Princíp dodržiavania princípu technologickej neutrality je vyjadrený napr. v recitáloch nariadenia o všeobecnej bezpečnosti.[138] Predmetné nariadenie predpokladá, že automatizované vozidlá postupne prevezmú úlohy vodiča. Práve z tohto dôvodu by sa mali na úrovni EÚ prijať harmonizované pravidlá a technické požiadavky na automatizované systémy vozidiel. Pri prijímaní týchto pravidiel má byť dodržaná zásada technologickej neutrality.[139]

[136] Princíp technologickej neutrality sa aplikuje aj v prípade právnej úpravy ochrany osobných údajov. Bližšie pozri: MESARČÍK, M.: *Osobné údaje ako základ pre fungovanie umelej inteligencie. In* MESARČÍK, M. a GYURÁSZ, Z.: Umelá inteligencia a právna úprava zdravotníctva v Slovenskej republike. 1. vydanie. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2020, s. 41.

[137] Důvodová zpráva k návrhu zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Dostupné: https://www.psp.cz/sqw/text/tiskt.sqw?o=7&ct=81&ct1=0.
Pozri POLČÁK, R., HARAŠTA, J. a STUPKA, V.: *Právní problémy kybernetické bezpečnosti.* 1. vyd. Brno : Masarykova univerzita, Právnická fakulta, 2016, s. 18.

[138] Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/2144 o požiadavkách na typové schvaľovanie motorových vozidiel a ich prípojných vozidiel a systémov, komponentov a samostatných technických jednotiek určených pre tieto vozidlá, pokiaľ ide o ich všeobecnú bezpečnosť a ochranu cestujúcich vo vozidle a zraniteľných účastníkov cestnej premávky.

[139] Recitál 23 nariadenia o všeobecnej bezpečnosti.

Princíp ochrany informačného sebaurčenia človeka

Pojem informačného sebaurčenia človeka v sebe zahŕňa katalóg absolútnych informačných práv človeka. Informačné sebaurčenie v sebe pôvodne zahŕňalo len pasívnu zložku, ktorou je ochrana diskrétnej informačnej sféry (ochrana diskrétnych informácií). Príkladmi práv v rámci pasívnej zložky informačného sebaurčenia je ochrana súkromia a ochrana osobných údajov. Informačné sebaurčenie obsahuje aj aktívnu zložku, ktorá predstavuje právo aktívne prijímať, spracovať a komunikovať informácie. Aktívna zložka informačného sebaurčenia vychádza z predpokladu, že človek nemôže žiť plnohodnotný súkromný život bez toho, aby mal možnosť komunikovať s okolitým svetom.[140]

PRÍKLAD

Ochrana osobných údajov je vyjadrená napr. v nariadení o všeobecnej bezpečnosti, v zmysle ktorého: *„každé spracúvanie osobných údajov, ako napríklad informácií o vodičovi spracúvaných v zariadeniach na záznam údajov o udalostiach alebo informácií v systéme varovania vodiča pred ospalosťou a stratou pozornosti alebo v systéme varovania vodiča pred rozptýlením, sa musí vykonávať v súlade s právnymi predpismi Únie o ochrane údajov, a to najmä s nariadením Európskeho parlamentu a Rady (EÚ) 2016/679"*.[141]

Princíp ochrany nedistributívnych (verejných) práv

V prípade princípu ochrany nedistributívnych (verejných) práv[142] ide najmä o ochranu národnej bezpečnosti, ochranu kriticky dôležitých spoločenských či ekonomických činností a špecificky o ochranu bezpečnosti prostredia, v ktorom dochádza k realizácii informačných transakcií. Nedistributívny charakter bezpečnosti sa prejavuje najmä tým, že tento verejný statok nemožno priradiť žiadnemu jednotlivcovi a z jeho existencie nevznikajú subjektom

[140] Dôvodová zpráva k návrhu zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Dostupné na: https://www.psp.cz/sqw/text/tiskt.sqw?o=7&ct=81&ct1=0. Bližšie k problematike informačného sebaurčenia pozri POLČÁK, R.: *Internet a proměny práva*. Praha: Auditorium, 2012, 388 s.

[141] Recitál 14 nariadenia o všeobecnej bezpečnosti.

[142] Vo všeobecnosti platí, že ústavná úprava postavenia jednotlivca v spoločnosti obsahuje ochranu individuálnych práv a slobôd, ako aj ochranu verejných statkov (*public goods*). V prípade verejných statkov (*public goods*), ktorými je napr. národná bezpečnosť, verejný poriadok či životné prostredie platí, že prospech z nich je nedeliteľný a ľudia nemôžu byť z ich užívania vylúčení. Verejný statok nemožno pojmovo, vecne i právne rozložiť na časti a tieto priradiť jednotlivcovi. Na druhej strane, základné práva a slobody ako osobná sloboda, sloboda prejavu, právo združovať sa a pod. možno pojmovo, vecne i právne členiť na časti a tieto priradiť jednotlivcom. Bližšie pozri: odlišné stanovisko Pavla Holländera k nálezu pléna Ústavního soudu zo dňa 3. 4. 1996, Pl.ÚS 32/95, 112/1996 Sb., N 26/5 SbNU 215.

konkrétne práva. Právo k ochrane bezpečnosti prostredia, v ktorom dochádza k realizácii informačných transakcií vykonáva výlučne štát.[143]

Princíp minimalizácie štátneho donútenia

Dodržiavaním princípu minimalizácie štátneho donútenia sa má docieliť, aby v prípade zásahu do ľudských práv a slobôd bol takýto zásah len v nevyhnutnej miere.

PRÍKLAD
V prípade kybernetickej bezpečnosti ide najmä o zásah do vlastníckeho práva subjektov. Správcovia a prevádzkovatelia sietí a informačných systémov budú musieť spĺňať konkrétne bezpečnostné opatrenia.

V prípade jednotlivcov by nemalo nedochádzať k obmedzovaniu ich práv a slobôd, nakoľko právo kybernetickej bezpečnosti nezasahuje do ich súkromia a neukladá im žiadne povinnosti.

PRÍKLAD
V prípade nedostatočnej úrovne kybernetickej bezpečnosti, napr. automatizovaných vozidiel môže dôjsť k narušeniu integrity, dôvernosti údajov či dostupnosti údajov, čo môže viesť k narušeniu súkromia. Ak je následkom úspešného kybernetického útoku narušenie bezpečnej prevádzky vozidla, môže dôjsť aj k ujme na zdraví či k strate na životoch. Taktiež v prípade plne automatizovaných vozidiel, ktoré sa budú rozhodovať namiesto vodiča, vodič stráca autonómiu rozhodovania, čo môže predstavovať zásah do jeho základných ľudských práv.[144]

[143] POLČÁK, R., HARAŠTA, J. a STUPKA, V.: *Právní problémy kybernetické bezpečnosti.* 1. vyd. Brno : Masarykova univerzita, Právnická fakulta, 2016, s. 19. K nedistributívnym právam pozri: POLČÁK, R.: *Internet a proměny práva*. Praha: Auditorium, 2012, 388 s.

[144] Bližšie pozri RADA EURÓPY: *Study on the human rights dimensions of automated data rocessing techniques (in particular algorithms) and possible regulatory implications*. 2017. Dostupné na: https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5. Mohlo by ísť o zásah do osobnej autonómie ako jedného z hlavných princípov práv na súkromie, ktorý je zakotvený v čl. 8 Európskeho dohovoru o ľudských právach a súvisiacej judikatúre Európskeho súdu pre ľudské práva Evans v the United Kingdom App no 6339/05 (7. marec 2006) 46 EHRR 34, para 57.
práva, je ustáleným právom v judikatúre ESĽP.137

Princíp minimalizácie štátneho donútenia sa prejavuje aj tým, že právna úprava kybernetickej bezpečnosti sa nevzťahuje na všetky siete a informačné systémy a ich správcov a prevádzkovateľov, ale len na vybraný okruh.[145]

Princíp autonómie vôle regulovaných subjektov

Pri rozmanitosti informačných systémov a ich správcov nie je vhodné a efektívne stanoviť špecifické povinnosti pre rôzne druhy subjektov. Spôsobilo by to situácie, kedy by niektoré subjekty museli realizovať bezpečnostné opatrenia, ktoré sú vzhľadom na ich informačné systémy príliš rozsiahle a na druhej strane by niektoré subjekty nedokázali splnením zákonných povinností dostatočne ochrániť svoje informačné systémy. Princíp autonómie vôle regulovaných subjektov sa prejavuje tým, že adresátom právnych povinností je ponechaná voľnosť v spôsoboch, akými ich majú naplniť. Regulované subjekty majú voľnosť pri voľbe konkrétnych postupov ako zabezpečiť požadovaná úroveň funkčnosti bezpečnostných opatrení.[146]

Princíp bdelosti vo vzťahu k ostatným štátom

Princíp bdelosti vo vzťahu k ostatným štátom je v medzinárodnom práve verejnom známy ako princíp *due dilligence*. Podľa tohto princípu je suverénny štát v rámci svojej jurisdikcie povinný brániť škodám, ktoré by mohli vzniknúť ostatným štátom alebo medzinárodnému spoločenstvu. V praktickej rovine môže dôjsť k situáciám, kedy sa zneužitím informačnej a komunikačnej infraštruktúry v jurisdikcii jedného štátu spácha kybernetický útok, ktorý má následky v inom štáte. Preto je dôležité, aby aj na národnej úrovni bola zabezpečená dostatočná úroveň kybernetickej bezpečnosti, tak aby informačné systémy neboli zneužívané ku kybernetickým útokom, ktoré smerujú na iné štáty.[147]

---

[145] POLČÁK, R., HARAŠTA, J. a STUPKA, V.: *Právní problémy kybernetické bezpečnosti.* 1. vyd. Brno : Masarykova univerzita, Právnická fakulta, 2016, s. 20 a 23.

[146] POLČÁK, R., HARAŠTA, J. a STUPKA, V.: *Právní problémy kybernetické bezpečnosti.* 1. vyd. Brno : Masarykova univerzita, Právnická fakulta, 2016, s. 24. Důvodová zpráva k návrhu zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Dostupné na: https://www.psp.cz/sqw/text/tiskt.sqw?o=7&ct=81&ct1=0.

[147] POLČÁK, R. , HARAŠTA, J. a STUPKA, V.: *Právní problémy kybernetické bezpečnosti.* 1. vyd. Brno : Masarykova univerzita, Právnická fakulta, 2016, s. 25-26. Důvodová zpráva k návrhu zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Dostupné na: https://www.psp.cz/sqw/text/tiskt.sqw?o=7&ct=81&ct1=0.

PRÍKLAD

Regulácia automatizovaných vozidiel a plne automatizovaných vozidiel sa vyznačuje harmonizáciou, čím sa má zabezpečiť, aby automatizované vozidlá mohli minimálne v rámci EÚ bez akýchkoľvek obmedzení jazdiť po pozemných komunikáciách. Je v záujme každého štátu, v ktorom bolo dané automatizované vozidlo registrované, aby tieto vozidlá spĺňali dostatočnú úroveň kybernetickej bezpečnosti, tak aby nespôsobovali škody v iných štátoch. Pod škodou spôsobenou automatizovaným vozidlom v inom štáte si možno predstaviť škody na majetku, ujmy na zdraví spôsobené narušením bezpečnej prevádzky vozidla, ktorá bola následkom úspešného kybernetického útoku voči automatizovanému vozidlu. Takýto útok mohol byť vykonaný v štáte, kde bolo vozidlo registrované. V prípade ak je automatizované vozidlo infikované a má v systémoch vložený vírus, je takéto automatizované vozidlo hrozbou pre iné vozidlá v inom štáte, účastníkov cestnej premávky, ako aj infraštruktúru (napr. inteligentné dopravné systémy, telekomunikačné siete a pod.).

Ak by sa zneužitím informačnej komunikačnej infraštruktúry v jurisdikcii jedného štátu spáchal kybernetický útok, ktorý má následky v inom štáte, je potrebné ostatné štáty o tom bezodkladne informovať.

PRÍKLAD

Smernica NIS2 obsahuje ustanovenia, na základe ktorých: *„v prípade potreby, a najmä ak sa významný incident týka dvoch alebo viacerých členských štátov, jednotka CSIRT, príslušný orgán alebo jednotné kontaktné miesto bez zbytočného odkladu informuje o významnom incidente ostatné zasiahnuté členské štáty a agentúru ENISA*.“[148]

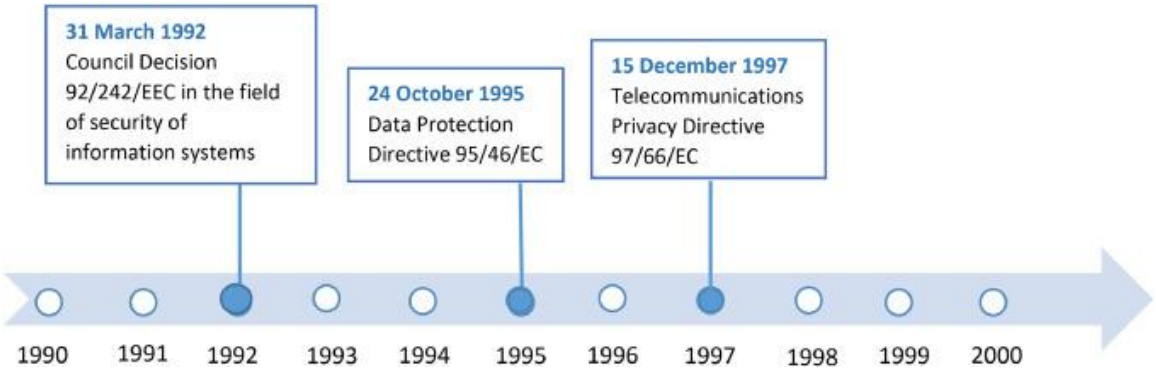
[148] Smernica NIS 2 čl. 23 ods. 6.

4. PRÁVO KYBERNETICKEJ BEZPEČNOSTI NA ÚROVNI PRÁVA EÚ

Začiatky právnej úpravy kybernetickej bezpečnosti na úrovni Európskej únie nemožno spájať až so smernicou NIS z roku 2016, hoci práve táto smernica predstavuje prvý záväzný legislatívny akt EÚ primárne zameraný na dosiahnutie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v EÚ. Už v roku 1992 bolo prijaté rozhodnutie Rady 92/242/EHS z 31. marca 1992 v oblasti bezpečnosti informačných systémov, ktoré možno považovať za prvý právny akt v tejto oblasti. Išlo však o pomerne stručný a koncepčný nástroj, ktorého cieľom bolo vytvoriť akčný plán a poradnú skupinu pre rozvoj strategického rámca bezpečnosti informačných systémov, pričom samotný pojem „bezpečnosť informačných systémov" nebol bližšie vymedzený. Následný vývoj bol spočiatku skôr pozvoľný a fragmentárny. V 90. rokoch sa požiadavky súvisiace s bezpečnosťou informačných systémov objavovali najmä v širšom kontexte ochrany osobných údajov a súkromia v elektronických komunikáciách, najmä v smernici 95/46/ES o ochrane údajov a v smernici 97/66/ES o ochrane súkromia v telekomunikáciách. Až postupný rast závislosti hospodárstva a spoločnosti od digitálnych sietí, ako aj nárast významu kybernetických hrozieb, viedli k tomu, že sa kybernetická bezpečnosť začala vyvíjať ako samostatnejšia oblasť právnej regulácie EÚ. Tento vývoj napokon vyústil do prijatia smernice NIS, ktorá predstavuje základný medzník záväznej právnej úpravy kybernetickej bezpečnosti na úrovni EÚ.[149]

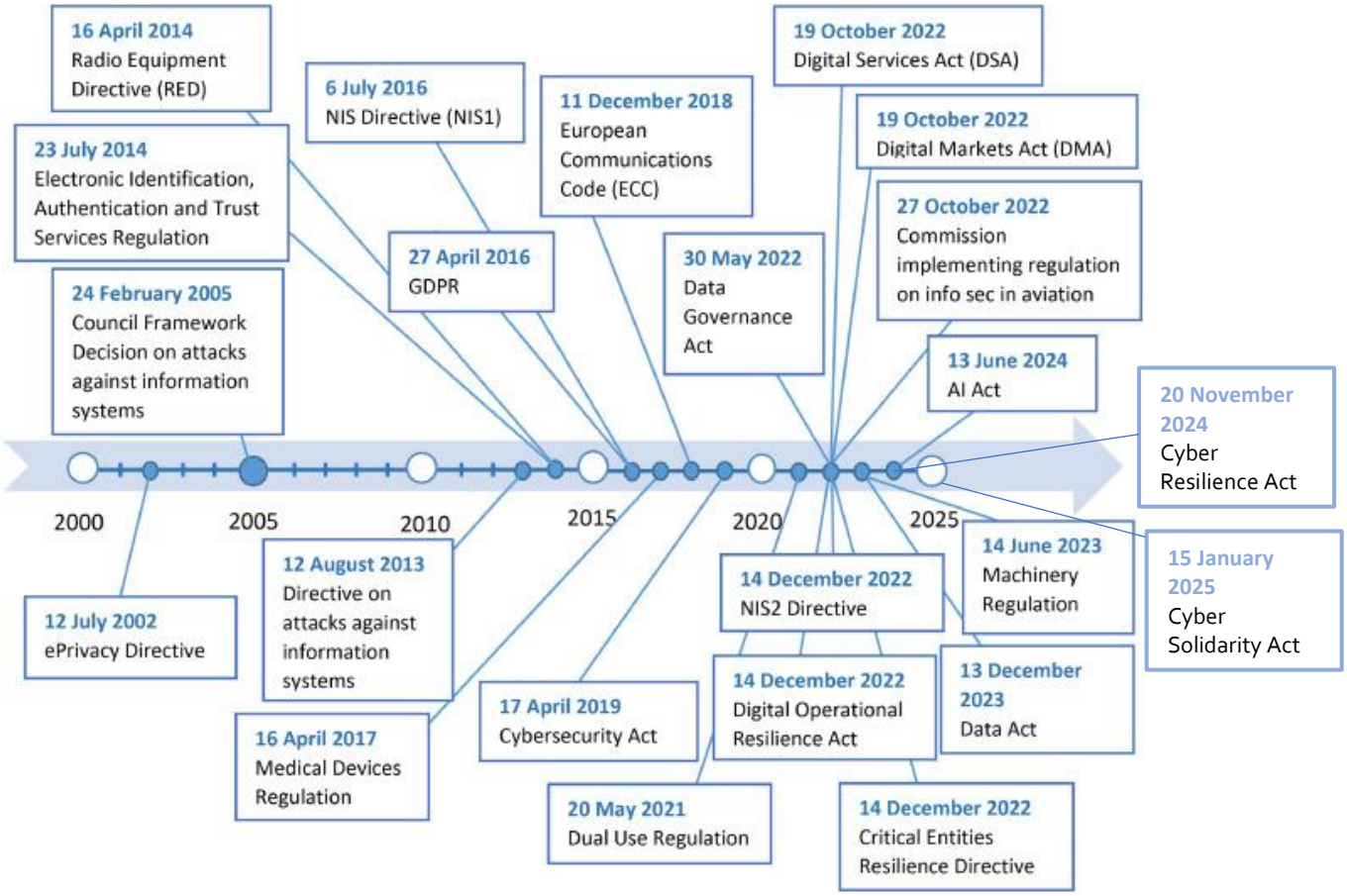
Obrázok nižšie zachytáva počiatočné obdobie právnej regulácie bezpečnosti informačných systémov v EÚ v rokoch 1990 – 2000, ktoré bolo charakteristické len niekoľkými čiastkovými aktmi. Za prvý právny akt v tejto oblasti možno označiť rozhodnutie Rady 92/242/EHS z roku 1992, po ktorom nasledovali najmä predpisy súvisiace s ochranou osobných údajov a súkromia v telekomunikáciách.

[149] BYGRAVE, L.A.: *The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes. In* Computer Law & Security Review, Volume 56, 2025, s. 1 – 4.



Obrázok č. 6: Právna regulácia bezpečnosti informačných systémov v EÚ v rokoch 1990 – 2000.

Obrázok nižšie znázorňuje výrazné zrýchlenie a rozšírenie legislatívnej činnosti EÚ v oblasti kybernetickej bezpečnosti po roku 2000, osobitne od polovice druhého desaťročia 21. storočia. Obrázok poukazuje na prechod od fragmentárnej úpravy k hustejšiemu regulačnému rámcu, ktorý zahŕňa smernicu NIS, GDPR, akt o kybernetickej bezpečnosti, smernica NIS 2, DORA, CER a ďalšie sektorové alebo čiastočne súvisiace právne akty.



Obrázok č. 7: Legislatívne akty v rokoch 1990 – 2025.[151]

[150] Prevzaté s BYGRAVE, L.A.: *The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes. In* Computer Law & Security Review, Volume 56, 2025, s. 3.
[151] Prevzaté s BYGRAVE, L.A.: *The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes. In* Computer Law & Security Review, Volume 56, 2025, s. 3 a doplnené o CRA a CSA.

Aktivity EÚ v oblasti kybernetickej bezpečnosti v súčasnosti smerujú najmä k ochrane jednotného digitálneho trhu a dosiahnutiu vysokej úrovne kybernetickej bezpečnosti v EÚ. Prvým strategickým dokumentom EÚ v oblasti kybernetickej bezpečnosti bola **Stratégia kybernetickej bezpečnosti Európskej únie**[152], ktorá 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 EÚ.[153]

Podľa predmetnej 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."*[154]

Pre účely tejto učebnice sa budeme venovať základným legislatívnym aktom EÚ, ktoré sa primárne venujú otázke kybernetickej bezpečnosti. Týmito legislatívnymi aktami EÚ sú smernica NIS, Smernica NIS 2 a akt o kybernetickej bezpečnosti. V kontexte kybernetickej bezpečnosti sa zameriame aj na RED smernicu, nariadenie CRA a AI Akt.

4.1 Smernica NIS[155]

Za prvý legislatívny akt prijatý európskym zákonodarcom v oblasti kybernetickej bezpečnosti možno považovať smernicu 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**"). Napriek tomu, že smernica NIS

[152] KOMISIA: *Stratégia kybernetickej bezpečnosti Európskej únie*. Brusel: 2013, s. 3.
[153] V decembri 2020 bol predstavený návrh novej stratégie kybernetickej bezpečnosti. Dostupné na: https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade.
[154] Tamže.
[155] Z anglického názvu *Directive on security of network and information systems.*

bola neskôr zrušená smernicou NIS 2, jej význam nemožno vnímať len ako prekonaný historický rámec. Naopak, predstavuje dôležité východisko vývoja európskej regulácie kybernetickej bezpečnosti, a preto považujeme za účelné objasniť jej historickú podstatu, regulačný význam a miesto v ďalšom vývoji právnej úpravy.

Napriek skutočnosti, že ide o legislatívny akt z oblasti kybernetickej bezpečnosti, smernica NIS neupravuje pojem kybernetická 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 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 EÚ ako celok. V tejto súvislosti je bezpečnosť sietí a informačných systémov základným predpokladom hladkého fungovania vnútorného trhu.

Za **sieť a informačný systém** v zmysle smernice NIS možno považovať:

a) elektronickú komunikačnú sieť;[156]
b) každé zariadenie alebo skupinu 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.[157]

[156] V zmysle smernice Európskeho parlamentu a Rady (EÚ) 2018/1972 z 11. decembra 2018, ktorou sa stanovuje európsky kódex elektronických komunikácií (prepracované znenie).
[157] Čl. 4 ods. 1 smernice NIS.

4.1.1 Predmet úpravy a rozsah pôsobnosti

Právna úprava kybernetickej bezpečnosti v smernici NIS nie je priamo orientovaná na ochranu fyzických a právnických osôb a nepriznáva im konkrétne práva v tejto oblasti. Smernica NIS stanovuje **opatrenia na dosiahnutie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov** v rámci EÚ 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 je **všeobecným právnym predpisom** (*lex generalis)* v oblasti kybernetickej bezpečnosti. V prípade, ak sa podľa právneho aktu EÚ špecifického (*lex specialis*) pre určité odvetvie vyžaduje, aby prevádzkovatelia základných služieb alebo poskytovatelia digitálnych služieb buď **zaisťovali bezpečnosť** ich sietí a informačných systémov, alebo aby **oznamovali incidenty**, uplatňujú sa ustanovenia tohto právneho aktu EÚ špecifického pre určité odvetvie. Podmienkou pre uplatnenie špecifického právneho aktu EÚ je, že tieto požiadavky musia mať **aspoň rovnocenný účinok** ako povinnosti stanovené v smernici NIS.[158]

[158] Čl. 1 ods. 7 smernice NIS.

4.1.2 Prevádzkovatelia základných služieb a poskytovatelia digitálnych služieb

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"). Popri týchto subjektoch sú adresátmi právnych noriem obsiahnutých v smernici NIS aj samotné členské štáty, ktoré musia plniť konkrétne povinnosti.

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:

- energetiky,
- dopravy,
- bankovníctva,
- infraštruktúry finančných trhov,
- zdravotníctva,
- dodávky a distribúcie pitnej vody a
- digitálnej infraštruktúry.

Smernica NIS umožňuje 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.

PRÍKLAD
Slovenská republika pridala odvetvie verejná správa či pošta. Niektoré členské štáty pridali odvetvia ako sociálne služby, vzdelávanie, životné prostredie či potraviny.

Zásada minimálnej harmonizácie vo vzťahu k PZS taktiež znamená, že členské štáty môžu uložiť požiadavky na PZS, ktoré sú prísnejšie, než požiadavky stanovené v smernici NIS.[159]

[159] KOMISA: *Správa Komisie Európskemu parlamentu a Rade o posúdení jednotnosti prístupov členských štátov pri identifikácii prevádzkovateľov základných služieb v súlade s článkom 23 ods. 1 smernice 2016/1148/EÚ o bezpečnosti sietí a informačných systémov*, s. 3-4.

4.1.3 Identifikácia prevádzkovateľov základných služieb

Členské štáty sú zodpovedné za identifikáciu subjektov pre každé odvetvie a pododvetvie uvedené v prílohe II. Pre identifikáciu PZS sú stanovené **tri kumulatívne kritériá,** konkrétne:

1. subjekt poskytuje službu, ktorá má zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností;
2. poskytovanie tejto služby je závislé od sietí a informačných systémov a
3. incident by mal závažný rušivý vplyv na poskytovanie uvedenej služby.[160]

Ad 1)

Prvou podmienkou je, aby subjekt poskytoval službu, ktorá má zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností. Pri posudzovaní toho, či subjekt poskytuje služby, ktoré sú pre zachovanie rozhodujúcich spoločenských alebo hospodárskych činností zásadné, stačí preskúmať, či uvedený subjekt poskytuje službu, ktorá je zahrnutá do **zoznamu základných služieb**. Zoznam služieb by mal pre členské štáty slúžiť ako referenčný bod umožňujúci identifikáciu PZS. Jeho účelom je určiť typy základných služieb v ktoromkoľvek danom odvetví uvedenom v smernici NIS.[161]

Hoci smernica NIS bližšie nedefinuje pojem základná služba a nešpecifikuje, čo možno považovať za službu, ktorá má zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností, v kontexte zoznamu jednotlivých odvetví, pododvetví a typov subjektov v týchto odvetviach a pododvetviach podľa prílohy II smernice NIS, ide o také služby, bez ktorých by fungovanie spoločnosti bolo značne obmedzené.

PRÍKLAD
Vhodným príkladom je zoznam základných služieb, ktorý obsahuje česká vyhláška č. 437/2017 o kritériích pro určení provozovatele základní služby.[162] Napr. v sektore energetika, podsektore elektrina sú uvedené tieto služby: výroba elektriny, predaj elektriny, prevádzka prenosovej sústavy, prevádzka distribučnej sústavy.

[160] Čl. 5 ods. 1 a 2 smernice NIS.
[161] Čl. 5 ods. 2 písm. a) a body 19 a 23 preambuly smernice NIS.
[162] Dostupné na: https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=437/2017&typeLaw=zakon&what=Cislo_zakona_smlouvy.

V prípade Slovenskej republiky k dnešnému dňu nebol vytvorený relevantný zoznam základných služieb, ktorý by slúžil ako referenčný bod umožňujúci identifikáciu PZS. Základnú službu možno v niektorých prípadoch vyčítať z uvedeného typu subjektu v danom odvetní a pododvetví.[163]

Ad 2)

Druhou podmienkou je, aby poskytovanie služby, ktorá má zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností bolo závislé od sietí a informačných systémov. [164]

PRÍKLAD

Distribúciu pitnej vody okrem fyzických prvkov ako sú potrubia, čerpadlá a pod. bude zabezpečovať, resp. riadiť konkrétny informačný systém.

Ad 3)

Pre splnenie **tretej podmienky** postačuje, aby mal incident závažný rušivý vplyv na poskytovanie služby, ktorá má zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností.[165] 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) vplyv, 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.

[163] Dostupné na: https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/zakladne-sluzby.htm.
[164] Čl. 5 ods. 2 písm. b) smernice NIS.
[165] Čl. 5 ods. 2 písm. c) smernice NIS.

Podľa potreby môžu členské štáty zohľadniť pri určení či by mal incident závažný rušivý vplyv aj **faktory špecifické** pre jednotlivé odvetvia.[166]

PRÍKLAD
Ako praktický príklad splnenia troch kumulatívnych podmienok by sme mohli uviesť subjekt Železnice Slovenskej republiky, ktoré prevádzkujú železničnú infraštruktúru. Tento subjekt je uvedený ako typ subjektu v odvetví doprava, pododvetví železničná doprava podľa prílohy II smernice NIS. Prevádzka železničnej infraštruktúry predstavuje službu, ktorá má zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností. Táto služba je poskytovaná prostredníctvom sietí a informačných systémov. Aby sme mohli povedať, že incident mal závažný rušivý vplyv na poskytovanie takejto služby, bolo by postačujúce aby bol naplnený aspoň jeden z medziodvetvových faktorov a aspoň jeden zo špecifických faktorov, ak sú pre dané odvetvie prijaté. V prípade ak by incident ochromil železničnú prepravu hoci len na jeden deň, malo by to negatívny dopad na zisky spoločnosti a ovplyvnilo by to aj iné odvetvia.

4.1.4 Povinnosti

PZS sú povinní **prijať vhodné a primerané technické a organizačné opatrenia** na riadenie rizík súvisiacich s bezpečnosťou sietí a informačných systémov, ktoré využívajú vo svojej prevádzke a taktiež sú povinní prijať primerané bezpečnostné opatrenia na zabránenie a minimalizovanie vplyvu incidentov, ktoré ovplyvňujú bezpečnosť sietí a informačných systémov používaných na poskytovanie týchto základných služieb, s cieľom zabezpečiť ich kontinuitu.[167]

Smernica NIS nedefinuje konkrétne druhy technických a organizačných opatrení. Je na členských štátoch, aké bezpečnostné požiadavky budú od konkrétnych subjektov vyžadovať, avšak tieto požiadavky musia dosiahnuť cieľ, ktorým je dostatočná úroveň bezpečnosti sietí a informačných systémov.

Ďalšie povinnosti sa týkajú **oznamovania incidentov**, ktoré majú závažný vplyv na kontinuitu základných služieb, ktoré poskytujú. Smernica NIS definuje **incident** ako:

[166] Čl. 6 ods. 2 smernice NIS.
[167] Čl. 14 ods. 1 a 2 smernice NIS.

„každá udalosť, ktorá má skutočne nepriaznivý vplyv na bezpečnosť sietí a informačných systémov.“[168]

Avšak PZS nie sú povinní hlásiť všetky incidenty, ale len tie, ktoré majú **závažný vplyv na kontinuitu základných služieb,** ktoré poskytujú.[169] S cieľom určiť závažnosť vplyvu incidentu sa zohľadnia najmä tieto parametre:

a) počet používateľov postihnutých narušením základnej služby;
b) dĺžka trvania incidentu;
c) geografické rozšírenie z hľadiska oblasti, ktorú incident postihol.[170]

Smernica NIS nešpecifikuje **lehotu** na oznámenie incidentov, ale len ukladá povinnosť pre PZS, aby **bez zbytočného odkladu** oznamovali príslušnému orgánu alebo jednotke CSIRT incidenty, ktoré majú závažný vplyv na kontinuitu základných služieb, ktoré poskytujú.[171]

Oznámenia o incidentoch, ktoré majú závažný vplyv na kontinuitu základných služieb obsahujú informácie umožňujúce príslušnému orgánu alebo jednotke CSIRT určiť prípadný **cezhraničný vplyv incidentu**. Na základe týchto informácií, ktoré poskytol PZS v oznámení, je príslušný orgán alebo jednotka CSIRT povinná informovať ostatné postihnuté členské štáty, ak má incident závažný vplyv na kontinuitu základných služieb v týchto členských štátoch.[172]

Smernica NIS taktiež upravuje možnosť **informovania verejnosti o incidente**. Príslušný orgán alebo jednotka CSIRT môže informovať o jednotlivých incidentoch verejnosť za splnenia dvoch podmienok. **Prvou** podmienkou je, aby došlo k porade príslušného orgánu alebo jednotky CSIRT s oznamujúcim PZS. Z tejto podmienky vyplýva, že príslušný orgán alebo jednotka CSIRT nemôže informovať o incidente verejnosť, pokiaľ to nebude prekonzultované s PZS, ktorého sa incident týka. **Druhá** kumulatívna podmienka je, aby bola informovanosť verejnosti potrebná na zabránenie incidentu alebo na riešenie prebiehajúceho incidentu.[173]

[168] Čl. 4 bod 7 smernice NIS.
[169] Čl. 14 ods. 3 smernice NIS.
[170] Čl. 14 ods. 3 smernice NIS.
[171] Čl. 14 ods. 3 smernice NIS.
[172] Č. 14 ods. 3 a ods. 5 smernice NIS.
[173] Čl. 14 ods. 6 smernice NIS.

Popri povinnom hlásení kybernetických bezpečnostných incidentoch upravuje smernica NIS aj **dobrovoľné oznamovanie**. Subjekty, ktoré neboli určené ako PZS a nie sú PDS, môžu na dobrovoľnom základe oznamovať incidenty, ktoré majú závažný vplyv na kontinuitu služieb, ktoré poskytujú.[174]

Smernica NIS v súvislosti s **PDS** uplatňuje **princíp maximálnej harmonizácie**, čo znamená, že na rozdiel od úpravy PZS, nesmú členské štáty v prípade PDS prijať prísnejšie pravidlá, ako tie ktoré vyplývajú zo smernice NIS. PDS nepodliehajú procesu identifikácie ako v prípade PZS, nakoľko rozsah pôsobnosti smernice NIS sa vzťahuje na všetkých PDS, ktorí napĺňajú definičné znaky pojmu PDS. PDS je každá právnická osoba, ktorá poskytuje niektorú z týchto digitálnych služieb:

a) online trhovisko,
b) internetový vyhľadávač,
c) služby cloud computingu,

Online trhovisko je definované ako:

„digitálna služba, ktorá umožňuje spotrebiteľom a/alebo obchodníkom v zmysle článku 4 ods. 1 písm. a) a b) smernice Európskeho parlamentu a Rady 2013/11/EÚ (18) uzavierať online kúpne zmluvy alebo zmluvy o službách s obchodníkmi buď na webovom sídle online trhoviska, alebo na webovom sídle obchodníka, ktoré využíva počítačové služby poskytované online trhoviskom."[175]

PRÍKLAD
Online trhovisko predstavuje platformu, ktorá umožňuje kupujúcim (spotrebiteľom aj obchodníkom) a predajcom uskutočňovať predaje tovaru a služieb. Napríklad Amazon alebo eBay.

[174] Čl. 20 ods. 1 smernice NIS.
[175] Čl. 4 bod 17 smernice NIS.

Internetový vyhľadávač je definovaný ako:

„digitálna služba, ktorá umožňuje používateľom vyhľadávať v zásade na všetkých webových sídlach alebo na webových sídlach v konkrétnom jazyku informácie o akejkoľvek téme na základe kľúčového slova, vety alebo iných zadaných údajov, pričom jeho výsledkom sú linky, prostredníctvom ktorých možno nájsť informácie súvisiace s požadovaným obsahom."[176]

PRÍKLAD
Napr. Google alebo Bing. Pojem internetový vyhľadávač nepokrýva online služby, ktoré porovnávajú ceny určitých výrobkov alebo služieb od rozličných obchodníkov a následne presmerujú používateľa na uprednostňovaného obchodníka, aby si kúpil jeho výrobok.[177]

Služba v oblasti **cloud computingu** je definovaná ako:

„digitálna služba, ktorá umožňuje prístup ku škálovateľnému a pružnému súboru počítačových zdrojov, ktoré možno zdieľať."

PRÍKLAD
Ide o rôzne služby, ktoré spočívajú v prenájme výpočtovej a pamäťovej kapacity (infraštruktúra ako služba, IaaS), prenájme hardvérových kapacít a programového vybavenia (platforma ako služba, PaaS) a využívaní aplikačných programov poskytovateľa služby (SaaS).[178]

PDS sú povinní identifikovať riziká súvisiace s bezpečnosťou sietí a informačných systémov, ktoré používajú v kontexte poskytovania svojich služieb a taktiež sú povinní prijať vhodné a primerané technické a organizačné opatrenia na **riadenie** týchto **rizík.** Tieto opatrenia musia s ohľadom na najnovší technický vývoj zabezpečiť takú úroveň bezpečnosti sietí a informačných systémov, ktorá zodpovedá miere daného rizika, a zohľadniť tieto prvky:

- bezpečnosť systémov a zariadení;

[176] Čl. 4 bod 18 smernice NIS.
[177] Recitál 16 smernice NIS.
[178] ANDRAŠKO, J a kol.:. *Zákon o kybernetickej bezpečnosti.* Bratislava : Wolters Kluwer, 2018, s. 109-110.

- riešenie incidentov;
- riadenie kontinuity činnosti;
- monitorovanie, audit a skúšanie;
- súlad s medzinárodnými normami.[179]

Vyššie uvedené bezpečnostné prvky sú bližšie špecifikované vo vykonávacom nariadení Komisie (EÚ) 2018/151.[180] V predmetnom vykonávacom nariadení sú ako používatelia digitálnych služieb uvedené:

> *„fyzické a právnické osoby, ktoré sú zákazníkmi alebo predplatiteľmi na online trhu alebo využívajú služby cloud computingu, alebo ktoré navštívili webové sídlo internetového vyhľadávača na účely vyhľadávania pomocou kľúčových slov.*"

PDS sú povinní prijať bezpečnostné opatrenia na zabránenie a minimalizovanie **vplyvu incidentov** ovplyvňujúcich bezpečnosť ich sietí a informačných systémov na svoje služby, ktoré sa poskytujú v rámci EÚ, s cieľom zabezpečiť kontinuitu týchto služieb. PDS musia bezodkladne oznámiť príslušnému orgánu alebo jednotke CSIRT každý incident, ktorý má závažný vplyv na poskytovanie služby, ktorú poskytujú v rámci EÚ.[181]

Pri určovaní, či je vplyv incidentu závažný, sa zohľadňujú najmä tieto parametre:

a) počet používateľov postihnutých incidentom, najmä používateľov využívajúcich danú službu na účely poskytovania vlastných služieb;
b) dĺžka trvania incidentu;
c) geografické rozšírenie z hľadiska oblasti, ktorú incident postihol;
d) stupeň narušenia fungovania služby;
e) rozsah vplyvu na hospodárske a spoločenské činnosti.

Vyššie uvedené parametre sú bližšie špecifikované vo vykonávacom nariadení Komisie (EÚ) 2018/151.

[179] Čl. 16 ods. 1 smernice NIS.
[180] 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 toho, či má incident závažný vplyv.
[181] Čl. 16 ods. 1-3 smernice NIS.

PRÍKLAD

Vykonávacie nariadenie Komisie (EÚ) 2018/151 v čl. 4 uvádza situácie, kedy možno incident považovať za incident, ktorý má závažný vplyv.

a) *služba poskytovaná poskytovateľom digitálnych služieb bola nedostupná v rozsahu väčšom než 5 000 000 používateľských hodín, pričom pojem používateľská hodina sa týka počtu postihnutých používateľov v Únii počas šesťdesiatich minút;*
b) *incident viedol k strate integrity, pravosti alebo dôvernosti uchovávaných, zasielaných alebo spracovávaných údajov alebo súvisiacich služieb ponúkaných alebo prístupných prostredníctvom siete alebo informačného systému poskytovateľa digitálnych služieb, čo malo vplyv na viac ako 100 000 používateľov v Únii;*
c) *incident viedol k vzniku rizika pre verejný poriadok či verejnú bezpečnosť alebo k strate života;*
d) *incident viedol k vzniku materiálnej škody v prípade aspoň jedného používateľa v Únii, pričom škoda spôsobená tomuto používateľovi presahuje 1 000 000 EUR.*

4.2 Smernica NIS 2

Aplikačná prax, ako aj závery Komisie poukázali na to, že cieľ smernice NIS, a teda dosiahnutie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v rámci EÚ, sa nepodarilo naplniť. Pravidelný prieskum smernice NIS[182] ukázal viaceré nedostatky tejto právnej úpravy a bol zároveň aj základom pre vypracovanie znenia návrhu smernice NIS 2. Z daného posúdenia vyplýva niekoľko oblastí, ktoré ukázali najvyššiu mieru nedostatočnosti. V prvom rade bola konštatovaná nedostatočná prepojenosť požiadaviek smernice NIS pre jednotlivé sektory (odvetvia)[183]. Ako jasný príklad nejednotnosti v oblasti (osobnej) pôsobnosti smernice NIS uvádza Komisia prípad poskytovateľov zdravotnej starostlivosti, ktorí v niektorých členských štátoch EÚ patria do rozsahu implementácie smernice NIS a podliehajú bezpečnostným a organizačným požiadavkám na kybernetickú bezpečnosť a naopak, v niektorých členských štátoch týmto požiadavkám musia prispôsobiť procesy iba

[182] Príloha č. 6, EURÓPSKA KOMISIA. *Commission staff working document impact assessment report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148. Brusel, 16.12.2020 SWD(2020) 345 final.*
[183] V texte učebnice sú pojmy sektor a odvetvie považované za synonymá.

väčšie nemocnice. Podobná situácia nastala aj v prípade železničných prevádzkovateľov. Zatiaľ čo veľký európsky železničný prevádzkovateľ je zahrnutý do rozsahu pôsobnosti smernice NIS v jednom veľkom členskom štáte, na iného veľkého železničného prevádzkovateľa v inom veľkom členskom štáte sa bezpečnostné požiadavky smernice NIS nevzťahujú.[184]

Ďalej bolo konštatované nejasné vymedzenie pôsobnosti smernice a nejasné vymedzenie kompetencií národných dozorných autorít. V tejto súvislosti Komisia kritizovala odlišné kritéria pre identifikáciu poskytovateľov základných služieb naprieč členskými štátmi. Odlišnosť pri ich identifikovaní preto spôsobuje, že rovnaké entity v konkrétnom sektore podliehajú prísnejším opatreniam v jednom členskom štáte EÚ ako v ostatných. Tento prístup má za následok odlišnú implementáciu smernice NIS a fragmentáciu právneho rámca kybernetickej bezpečnosti. Problémom je aj zároveň nedostatočná informovanosť autorít v členských štátoch ohľadne svojich kompetencií voči prevádzkovateľom základných služieb.[185]

Taktiež boli identifikované odlišné bezpečnostné a notifikačné povinnosti naprieč členskými štátmi. Smernica NIS poskytla pomerne veľkú mieru slobody pri určovaní špecifík nahlasovania bezpečnostných incidentov. Členské štáty preto rozdielne pristúpili k otázkam, ktoré bezpečnostné incidenty je potrebné nahlásiť a v akej lehote. Tento prístup má za následok odlišnú implementáciu smernice NIS a fragmentáciu právneho rámca kybernetickej bezpečnosti.[186]

Z vyššie uvedených dôvodov sa pristúpilo k tvorbe nového legislatívneho aktu, ktorý by nahradil smernicu NIS. Návrh smernice NIS 2 bol 10. 11. 2022 schválený Európskym

[184] EURÓPSKA KOMISIA. *Commission staff working document impact assessment report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148. Brusel, 16.12.2020 SWD(2020) 345 final*, s. 11.

[185] Tamže, s. 15. K rovnakému záveru došla Európska Komisia vo svojej Správe o posúdení jednotnosti prístupov členských štátov pri identifikácii prevádzkovateľov základných služieb v súlade s článkom 23 ods. 1 smernice 2016/1148/EÚ o bezpečnosti sietí a informačných systémov. Dostupné na: <https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:52019DC0546>, cit. 2024-09-20.

[186] Tamže. Ako ďalšie oblasti boli identifikované: nedostatočne efektívny dohľad a vymáhanie; neporovnateľné prerozdelenie financií pri otázkach kybernetickej bezpečnosti naprieč členskými štátmi; limitované zdieľanie informácií medzi členskými štátmi.

parlamentom[187] a 28.11.2022 Radou Európskej únie.[188] Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (ďalej len „**smernica NIS 2**") bola 27.12.2022 zverejnená v Úradnom vestníku Európskej únie a dvadsiatym dňom po tomto uverejnení nadobudla účinnosť. Členské štáty boli povinné transponovať smernicu do vnútroštátnych právnych predpisov do 17. 10. 2024.[189]

Cieľom predkladaného príspevku je analyzovať smernicu NIS 2 v kontexte zmien týkajúcich sa osobnej pôsobnosti. Špecificky bude analyzované, akým spôsobom sa nová regulácia vzťahuje na subjekty verejnej správy a subjekty v oblasti vzdelávania. Analýza bude podrobená aj kritickému pohľadu, ktorý by mal reflektovať základnú otázku či je smernica NIS 2 v porovnaní so smernicou NIS lepším harmonizačným právnym nástrojom v kontexte osobnej pôsobnosti. Autori si taktiež kladú za cieľ poukázať na stav transpozície predmetnej smernice vo vybraných členských štátoch EÚ, najmä v kontexte osobnej pôsobnosti. Analýze bude podrobená právna úprava kybernetickej bezpečnosti dvoch štátov, ktoré už transponovali smernicu NIS 2, konkrétne Chorvátsko a Belgicko.

4.2.1 Pôsobnosť smernice NIS 2

Smernica NIS 2 prináša zásadnú zmenu v otázke **rozsahu (osobnej) pôsobnosti**. Identifikácia prevádzkovateľov základnej služby a rozlišovanie medzi prevádzkovateľmi základných služieb a poskytovateľmi digitálnych služieb v zmysle smernice NIS sa ukázalo ako zastarané, pretože neodráža význam odvetví alebo služieb pre spoločenské a hospodárske činnosti na vnútornom trhu.[190]

Subjekty, ktoré patria do rozsahu pôsobnosti smernice NIS 2 sa rozdeľujú do dvoch kategórií:

---

[187] Cybersecurity. Parliament adopts new law to strengthen EU-wide resilience. Dostupné na: <https://www.europarl.europa.eu/news/en/press-room/20221107IPR49608/cybersecurity-parliament-adopts-new-law-to-strengthen-eu-wide-resilience.>, cit. 2024-09-20.

[188] EU decides to strengthen cybersecurity and resilience across the Union: Council adopts new legislation. Dostupné na: <https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/.>, cit. 2024-09-20.

[189] Smernica NIS 2, čl. 41 ods. 1.

[190] Smernica NIS 2, recitál 6. Bližšie k porovnaniu smernice NIS a smernice NIS 2 pozri VANDEZANDE, N. Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. In Computer Law & Security Review, Volume 52, 2024 a SIEVERS, T. Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations. Int. Cybersecur. Law Rev. 2, 2021, s. 223–231.

- **kľúčové subjekty** (*essential entities*) a
- **dôležité subjekty** (*important entities*).

Kľúčové a dôležité subjekty musia byť subjekty typu uvedeného v prílohe I alebo prílohe II. V **prílohe I** s názvom „**Odvetvia s vysokou úrovňou kritickosti**" sú uvedené nasledujúce odvetvia: energetika, doprava, bankovníctvo, infraštruktúry finančných trhov, zdravotníctvo, pitná voda, odpadová voda, digitálna infraštruktúra, riadenie služieb IKT (medzi podnikmi), verejná správa a vesmír.

V **prílohe II** s názvom „**Iné kritické odvetvia**" sú zadefinované nasledujúce odvetvia: poštové a kuriérske služby; odpadové hospodárstvo; výroba a distribúcia chemických látok; výroba, spracovanie a distribúcia potravín; výroba; poskytovatelia digitálnych služieb a výskum.

Na kľúčové aj dôležité subjekty by sa mali vzťahovať rovnaké požiadavky na riadenie rizík a oznamovacie povinnosti. V prípade dohľadu a sankcií sa však na tieto dve kategórie subjektov neuplatňujú rovnaké ustanovenia.

Pravidlo obmedzenia veľkosti

Smernica NIS 2 neukladá členským štátom povinnosť identifikovať subjekty, ktoré spĺňajú kritériá, aby mohli pôsobiť ako prevádzkovatelia základných služieb („proces identifikácie"), tak ako to je upravené v smernici NIS. Namiesto toho sa v smernici NIS 2 stanovilo jednotné kritérium, ktorým sa určia subjekty, ktoré patria do rozsahu pôsobnosti tejto smernice.[191]

Toto kritérium spočíva v uplatňovaní **pravidla obmedzenia veľkosti** (*size-cap rule*), podľa ktorého sa smernica NIS 2 vzťahuje na všetky verejné alebo súkromné subjekty, ktoré sa považujú za **stredné podniky** podľa článku 2 prílohy k odporúčaniu Komisie zo 6. mája 2003 o definícii mikro, malých a stredných podnikov (oznámené pod číslom dokumentu C (2003) 1422) (2003/361/ES) (ďalej len „**odporúčanie Komisie**"), alebo ktoré **presahujú limity pre stredné podniky** stanovené v odseku 1 uvedeného článku a ktoré poskytujú služby alebo vykonávajú svoje činnosti v EÚ.[192] Podniky presahujúce limity pre stredné podniky možno označiť za veľké podniky.

[191] Smernica NIS 2, recitál 7.
[192] Smernica NIS 2, čl. 2 ods. 1 a recitál 7.

Odporúčanie Komisie definuje **stredné podniky** ako podniky, ktoré zamestnávajú menej ako 250 osôb a ktoré majú buď ročný obrat nepresahujúci 50 miliónov eur, alebo ročnú bilančnú sumu neprevyšujúcu 43 miliónov eur. V kontexte ukazovateľov pre ďalšie subjekty (malé podniky, mikropodniky) upravených v odporúčaní Komisie možno konštatovať, že za stredné podniky sa považujú podniky, ktoré zamestnávajú 50 až 249 osôb, s ročným obratom prevyšujúcim 10 miliónov EUR až do 50 miliónov EUR alebo ročnou bilančnou sumou prevyšujúcou 10 miliónov EUR až do 43 miliónov EUR.

Za **veľké podniky** sa považujú podniky, ktoré zamestnávajú 250 a viac osôb a ktoré majú buď ročný obrat prevyšujúci 50 miliónov eur, alebo ročnú bilančnú sumu prevyšujúcu 43 miliónov eur.

V zmysle odporúčania Komisie sa základný **počet pracovníkov** vyjadruje v **ročných pracovných jednotkách**. Osoby, ktoré v rámci podniku alebo v jeho mene pracovali na plný pracovný čas počas celého referenčného roka, sa považujú za jednu jednotku. Pracovníci na kratší pracovný čas, sezónni pracovníci a osoby, ktoré nepracovali celý rok, sa započítavajú ako zlomky jednej jednotky.[193]

Pre úplnosť je potrebné dodať, že v situáciách, ktoré zahŕňajú „partnerské" alebo „prepojené" podniky, sa na výpočet veľkosti musí vykonať pomerná konsolidácia údajov (ročné pracovné jednotky a obrat alebo bilančná suma) príslušného subjektu a iných subjektov.[194]

Výnimka z pravidla obmedzenia veľkosti

Zo všeobecného pravidla obmedzenia veľkosti existujú v zmysle smernice NIS 2 aj **výnimky**.

Určité malé podniky a mikropodniky, ktoré spĺňajú osobitné kritériá, ktoré naznačujú kľúčovú úlohu pre spoločnosť, hospodárstvo alebo pre určité odvetvia alebo druhy služieb, patria do rozsahu pôsobnosti smernice NIS 2.[195] V tejto súvislosti možno konštatovať, že v osobitných prípadoch uvedených v smernici NIS 2 sa bude smernica NIS 2 vzťahovať aj na mikropodniky a malé podniky.

[193] EURÓPSKA KOMISIA. Príručka pre používateľov k definícii MSP. 2019, s. 13. Dostupné na: <https://op.europa.eu/sk/publication-detail/-/publication/79c0ce87-f4dc-11e6-8a35-01aa75ed71a1>, cit. 2024-09-20.
[194] Tamže, s. 18 - 23.
[195] Smernica NIS 2, recitál 7.

Odporúčanie Komisie 2003/361/ES definuje mikropodniky a malé podniky nasledovne:

> *„Mikropodniky sa definujú ako podniky, ktoré zamestnávajú **menej ako 10 osôb** a ktorých ročný obrat alebo ročná bilančná suma nepresahuje **2 milióny eur**.* "
> *„Malé podniky sa definujú ako podniky, ktoré zamestnávajú **menej ako 50 osôb** a ktorých ročný obrat alebo ročná bilančná suma nepresahuje **10 miliónov eur**.* "

Z vyššie uvedených definícií vyplýva, že pre posúdenie veľkosti subjektu v zmysle spomínaného odporúčania musí byť naplnený zamestnanecký, ako aj finančný ukazovateľ (ročný obrat alebo ročná bilančná suma). Avšak v prípade finančných ukazovateľov sa daný subjekt môže rozhodnúť, či bude spĺňať maximálnu hodnotu stanovenú pre obrat alebo maximálnu hodnotu stanovenú pre bilančnú sumu. Subjekt nemusí spĺňať obe požiadavky, pričom jednu z nich môže aj presiahnuť bez toho, aby to malo vplyv na jeho postavenie mikro, malého alebo stredného podniku.[196]

Pre doplnenie je potrebné uviesť, že za podnik sa považuje: *„každý subjekt, ktorý vykonáva hospodársku činnosť, bez ohľadu na jeho právnu formu*".[197] Určujúcim faktorom nie je právna forma ale hospodárska činnosť. V praxi to znamená, že za podnik sa môžu považovať samostatne zárobkovo činné osoby, rodinné firmy, partnerstvá a združenia alebo akékoľvek iné subjekty, ktoré pravidelne vykonávajú hospodársku činnosť. Za hospodársku činnosť sa zvyčajne považuje: *„predaj výrobkov alebo služieb za stanovenú cenu na určitom/priamom trhu*".[198]

---

[196] Národní úřad pro kybernetickou a informační bezpečnost (ďalej len „NÚKIB") uvádza vo svojom factsheetu pre posúdenie veľkosti subjektov nasledujúce príklady:
Príklad č.1: Podnik so 60 ročnými pracovnými jednotkami, ročným obratom 9 miliónov EUR a ročnou bilančnou sumou 9 miliónov EUR. Podnik bude považovaný za stredný, pretože presiahol zamestnanecký strop pre malé podniky.
Príklad č. 2: Podnik so 49 ročnými pracovnými jednotkami, ročným obratom 12 miliónov EUR a ročnou bilančnou sumou 8 miliónov EUR. Podnik bude považovaný za malý. Aj napriek prekročeniu stropu pre ročný obrat sa môže podnik posudzovať podľa ročnej bilančnej sumy, ktorá do stropov pre malé podniky spadá.
Príklad č. 3: Podnik s 8 zamestnancami, ročným obratom 30 miliónov EUR a ročnou bilančnou sumou 15 miliónov EUR. Podnik bude považovaný za stredný, pretože oba finančné ukazovatele presahujú hodnotu 10 miliónov EUR. Dostupné na: <https://portal.nukib.gov.cz/informace/legislativa/zakon-o-kyberneticke-bezpecnosti>, cit. 2024-09-21.

[197] EURÓPSKA KOMISIA. Príručka pre používateľov k definícii MSP. 2019, s. 10 - 11. Dostupné na: <https://op.europa.eu/sk/publication-detail/-/publication/79c0ce87-f4dc-11e6-8a35-01aa75ed71a1>, cit. 2024-09-20.

[198] Tamže, s. 9.

Smernica NIS 2 sa vzťahuje na subjekty, typu uvedeného v prílohe I alebo prílohe II **bez ohľadu na ich veľkosť** keď:[199]

a) služby poskytujú:
   i. poskytovatelia verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb;
   ii. poskytovatelia dôveryhodných služieb;
   iii. registre názvov domén najvyššej úrovne a poskytovatelia služieb systému názvov domén;
b) subjekt je v členskom štáte jediným poskytovateľom služby, ktorá je kľúčovou pre zachovanie kritických spoločenských alebo hospodárskych činností;
c) narušenie služby poskytovanej subjektom by mohlo mať významný vplyv na verejný poriadok, verejnú bezpečnosť alebo verejné zdravie;
d) narušenie služby poskytovanej subjektom by mohlo vyvolať významné systémové riziko, najmä v odvetviach, v ktorých by takéto narušenie mohlo mať cezhraničný vplyv;
e) subjekt je vzhľadom na svoj osobitný význam na vnútroštátnej alebo regionálnej úrovni kritickým pre konkrétne odvetvie alebo typ služby alebo pre iné vzájomne závislé odvetvia v členskom štáte;
f) subjekt je subjektom verejnej správy:
   i. v ústrednej štátnej správe podľa definície členského štátu v súlade s vnútroštátnym právom; alebo
   ii. na regionálnej úrovni podľa definície členského štátu v súlade s vnútroštátnym právom, ktorý po posúdení na základe rizík poskytuje služby, ktorých narušenie by mohlo mať významný vplyv na kritické spoločenské alebo hospodárske činnosti.

Smernica NIS 2 sa taktiež vzťahuje na subjekty identifikované ako **kritické subjekty** podľa smernice Európskeho parlamentu a Rady (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/114/ES (ďalej len „**smernica o odolnosti kritických subjektov**“) bez ohľadu na ich veľkosť a subjekty poskytujúce služby registrácie názvov domén bez ohľadu na ich veľkosť.[200]

Členské štáty môžu ustanoviť, že sa smernica NIS 2 vzťahuje na:[201]

[199] Smernica NIS 2, čl. 2 ods. 2.
[200] Smernica NIS 2, čl. 2 ods. 3 a 4.
[201] Smernica NIS 2, čl. 2 ods. 5.

a) subjekty verejnej správy na **miestnej úrovni**;
b) **vzdelávacie inštitúcie**, najmä tie, v ktorých sa vykonávajú kritické výskumné činnosti.

V kontexte vyššie uvedeného možno konštatovať, že bude závisieť od členského štátu či sa medzi subjekty verejnej správy budú zaradzovať len subjekty verejnej správy v ústrednej štátnej správe a regionálnej úrovni, alebo sa rozsah pôsobnosti rozšíri aj na subjekty verejnej správy na miestnej úrovni a vzdelávacie inštitúcie.

Negatívna pôsobnosť

Smernica NIS 2 sa nevzťahuje na subjekty verejnej správy, ktoré vykonávajú činnosť v oblasti národnej bezpečnosti, verejnej bezpečnosti, obrany alebo presadzovania práva vrátane prevencie, vyšetrovania, odhaľovania a stíhania trestných činov. Avšak, subjekty verejnej správy, ktorých činnosti s uvedenými oblasťami súvisia len okrajovo, by však nemali byť vylúčené z rozsahu pôsobnosti smernice NIS 2.[202]

Členské štáty môžu vyňať konkrétne subjekty, ktoré vykonávajú činnosti v oblastiach národnej bezpečnosti, verejnej bezpečnosti, obrany alebo presadzovania práva vrátane prevencie, vyšetrovania, odhaľovania a stíhania trestných činov, alebo ktoré poskytujú služby výhradne subjektom verejnej správy, ktoré vykonávajú činnosť v oblasti národnej bezpečnosti, verejnej bezpečnosti, obrany alebo presadzovania práva, v súvislosti s danými činnosťami alebo službami z povinností stanovených v článku 21 alebo článku 23 smernice NIS 2.[203]

Smernica NIS 2 sa taktiež nevzťahuje na subjekty, ktoré členské štáty vyňali z rozsahu pôsobnosti nariadenia (EÚ) 2022/2554 (DORA) v súlade s článkom 2 ods. 4 uvedeného nariadenia.[204]

4.2.1.1 Kľúčové a dôležité subjekty

Ako už bolo vyššie spomínané, smernica NIS 2 už nerozlišuje medzi hospodárskymi subjektami prevádzkovateľ základnej služby a poskytovateľa digitálnej služby, tak ako to bolo v prípade smernice NIS ale zavádza nové druhy subjektov, ktorými sú kľúčové subjekty a dôležité subjekty. Za **kľúčové subjekty** sa považujú:[205]

[202] Smernica NIS 2, čl. 2 ods. 7 a recitál 8.
[203] Smernica NIS 2, čl. 2 ods. 8.
[204] Smernica NIS 2, čl. 2 ods. 10.
[205] Smernica NIS 2, čl. 3 ods. 1.

a) subjekty typu uvedeného v prílohe I, ktoré presahujú limity pre stredné podniky stanovené v článku 2 ods. 1 prílohy k odporúčaniu 2003/361/ES;
b) kvalifikovaní poskytovatelia dôveryhodných služieb a registre názvov domén najvyššej úrovne, ako aj poskytovatelia služieb DNS, bez ohľadu na ich veľkosť;
c) poskytovatelia verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb, ktoré sú považované za stredné podniky podľa článku 2 prílohy k odporúčaniu 2003/361/ES;
d) subjekty verejnej správy uvedené v článku 2 ods. 2 písm. f) bode i);
e) akékoľvek iné subjekty typu uvedeného v prílohe I alebo II, ktoré členský štát označil za kľúčové subjekty podľa článku 2 ods. 2 písm. b) až e);
f) subjekty označené ako kritické subjekty podľa smernice (EÚ) 2022/2557 uvedenej v článku 2 ods. 3 tejto smernice;
g) ak tak členský štát ustanoví, subjekty, ktoré daný členský štát označil pred 16. januárom 2023 ako prevádzkovateľov základných služieb v súlade so smernicou (EÚ) 2016/1148 alebo vnútroštátnym právom.

Subjekty typu uvedeného v prílohe I alebo II, ktoré sa nepovažujú za kľúčové subjekty podľa odseku 1 článku 3 smernice NIS 2, sa považujú za **dôležité subjekty**. Patria sem subjekty označené členskými štátmi ako dôležité subjekty podľa článku 2 ods. 2 písm. b) až e) smernice NIS 2.[206]

Do 17. apríla 2025 vypracujú členské štáty **zoznam kľúčových a dôležitých subjektov** ako aj subjektov poskytujúcich služby registrácie názvov domén. Členské štáty tento zoznam pravidelne prehodnocujú a podľa potreby aktualizujú najmenej každé dva roky po uvedenom dátume.[207]

Na účely zostavenia zoznamu kľúčových a dôležitých subjektov členské štáty požadujú od týchto subjektov, aby príslušným orgánom predložili aspoň tieto informácie:[208]

a) názov subjektu;
b) adresu a aktuálne kontaktné údaje vrátane e-mailových adries, IP adries a telefónnych čísel;
c) podľa potreby príslušné odvetvie a pododvetvie uvedené v prílohe I alebo II; a

[206] Smernica NIS 2, čl. 3 ods. 2.
[207] Smernica NIS 2, čl. 3 ods. 3.
[208] Smernica NIS 2, čl. 3 ods. 4.

d) prípadne zoznam členských štátov, v ktorých poskytujú služby patriace do pôsobnosti tejto smernice.

Kľúčové a dôležité subjekty bezodkladne a v každom prípade do dvoch týždňov odo dňa zmeny oznámia akékoľvek zmeny zasielaných údajov zasielaných.[209]

Komisia s pomocou Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA) bez zbytočného odkladu poskytne usmernenia a vzory súvisiace s povinnosťami týkajúcich sa vytvorenia zoznamu, predloženia konkrétnych informácií či oznamovania zmien zasielaných údajov.[210] Predmetné usmernenia a vzory sú obsiahnuté v **Usmernení Komisie k uplatňovaniu článku 3 ods. 4 smernice (EÚ) 2022/2555 (smernica NIS 2).[211]**

Členské štáty môžu zaviesť vnútroštátne mechanizmy, pomocou ktorých by sa kľúčové a dôležité subjekty mohli zaregistrovať samé.[212]

Subjekty verejnej správy a odvetvie „Verejná správa"

V porovnaní so smernicou NIS sa smernica NIS 2 bude vzťahovať aj na konkrétne subjekty v rámci odvetvia **„Verejná spáva"**.

Subjekt verejnej správy je legálne definovaný v článku 6 bod 35 smernice NIS 2. V zmysle smernice NIS 2 je subjekt verejnej správy: *„subjekt, ktorý je ako taký uznaný v členskom štáte v súlade s vnútroštátnym právom, okrem súdnictva, parlamentov a centrálnych bánk, a ktorý spĺňa tieto kritériá:*

a) je zriadený na účely plnenia potrieb všeobecného záujmu a nemá priemyselný ani komerčný charakter;

b) má právnu subjektivitu alebo je zo zákona oprávnený konať v mene iného subjektu s právnou subjektivitou;

c) je financovaný prevažne štátnymi, regionálnymi alebo inými verejnoprávnymi orgánmi, podlieha dohľadu týchto inštitúcií alebo orgánov nad svojím riadením alebo v správnom, riadiacom alebo dozornom orgáne má viac ako polovicu členov menovaných štátnymi alebo regionálnymi orgánmi alebo inými verejnoprávnymi inštitúciami;

[209] Smernica NIS 2, čl. 3 ods. 4.
[210] Smernica NIS 2, čl. 3 ods. 4.
[211] Oznámenie Komisie Usmernenia Komisie k uplatňovaniu článku 3 ods. 4 smernice (EÚ) 2022/2555 (smernica NIS 2) 2023/C 324/02. Dostupné na: <https://eur-lex.europa.eu/legal-content/SK/TXT/?qid=1716636475611&uri=CELEX%3A52023XC0914%2801%29 >, cit. 2024-09-20.
[212] Smernica NIS 2, čl. 3 ods. 4.

d) *má právomoc vydávať fyzickým alebo právnickým osobám správne alebo regulačné rozhodnutia, ktoré majú vplyv na ich práva pri cezhraničnom pohybe osôb, tovarov, služieb alebo kapitálu*;"

V zmysle legálnej definície nemôže ísť o subjekty komerčného alebo priemyselného charakteru, to znamená, že musia plniť úlohy verejného alebo všeobecného záujmu. Zároveň, musia disponovať právnou subjektivitou alternatívne mať zákonom stanovené oprávnenie konať v mene iného subjektu s právnou subjektivitou. Tretia podmienka pre subjekty verejnej správy je ustanovená alternatívne a týka sa financovania štátom alebo dohľadu vykonávaného štátom. Štvrtá podmienka sa týka vydávania správnych alebo regulačných rozhodnutí, ktoré majú vplyv na práva pri cezhraničnom pohybe osôb, tovarov, služieb a kapitálu. Požiadavky vplyvu na práva pri pohybe osôb, tovarov, služieb a kapitálu reflektuje pôsobnosť EÚ v oblasti jednotného vnútorného trhu. Požiadavku pre cezhraničný aspekt je potrebné vnímať v tom kontexte, že ide o pohyb v rámci jednotlivých členských štátoch EÚ. Nasvedčuje tomu aj legálna definícia pojmu „cezhraničné spracúvanie" podľa nariadenia 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), v zmysle ktorého je cezhraničné spracúvanie také „*spracúvanie osobných údajov, ktoré sa uskutočňuje v Únii v kontexte činností prevádzkarní prevádzkovateľa alebo sprostredkovateľa vo viac ako jednom členskom štáte, pričom prevádzkovateľ alebo sprostredkovateľ sú usadení vo viac ako jednom členskom štáte*."[213] Takémuto výkladu nasvedčuje aj recitál 4 smernice NIS 2, v zmysle ktorého: „*Požiadavky na kybernetickú bezpečnosť uložené subjektom poskytujúcim služby alebo vykonávajúcim činnosti, ktoré sú ekonomicky významné, sa v jednotlivých členských štátoch značne líšia, pokiaľ ide o typ požiadaviek, ich úroveň podrobnosti a metódu dohľadu. Uvedené rozdiely spôsobujú dodatočné náklady a subjektom, ktoré ponúkajú tovar alebo služby cezhranične, spôsobujú ťažkosti. Požiadavky jedného členského štátu, ktoré sa líšia od požiadaviek iného členského štátu alebo sú s nimi dokonca v rozpore, môžu takéto cezhraničné činnosti podstatne ovplyvniť*."

V prípade vyššie uvedených kritérií pre pojem subjekt verejnej správy ide o **kumulatívne kritériá**, čo znamená, že musia byť splnené všetky kritériá.

[213] Všeobecné nariadenie o ochrane údajov, čl. 4, bod 23 písm. a).

Taktiež je potrebné dodať, že hoci sa vylučujú z pojmu subjekt verejnej správy subjekty zo súdnictva, parlamentov a centrálnych bánk, nie je vylúčené, aby sa právna úprava vzťahovala napr. na Kanceláriu Národnej rady Slovenskej republiky, Kanceláriu Najvyššieho súdu Slovenskej republiky či Kanceláriu Ústavného súdu Slovenskej republiky.

Ako už bolo objasnené v predchádzajúcich častiach článku, v smernici NIS 2 sa aplikuje pravidlo obmedzenia veľkosti, čo znamená, že smernica sa vzťahuje na verejné alebo súkromné subjekty typu uvedeného v prílohe I alebo II, ktoré sa považujú za stredné podniky alebo presahujú limity pre stredné podniky. V prílohe I sú pre odvetvie „Verejná správa" uvedené nasledujúce typy subjektov:

a) subjekty verejnej správy na úrovni ústrednej štátnej správy, ako ich vymedzuje členský štát v súlade s vnútroštátnym právom,
b) subjekty verejnej správy na regionálnej úrovni, ako ich vymedzuje členský štát v súlade s vnútroštátnym právom.

Pojem ústredná štátna správa sa spomína napr. v Správe o hodnotení vplyvu.[214] Ide napr. o správne orgány štátu (*administrative departments of the state*) a ďalšie ústredné orgány (*central agencies*), ktorých pôsobnosť pokrýva celé ekonomické územie krajiny (*whose responsibilities cover the whole economic territory of a country*).[215]

V prípade ustanovenia čl. 2 ods. 2 smernice NIS 2, ktoré upravuje výnimky z pravidla obmedzenia veľkosti, možno v súvislosti so subjektami verejnej správy na regionálnej úrovni vidieť aj ďalšie požiadavky, ktoré v prílohe I v odvetví „Verejná správa" nie sú pre subjekty verejnej správy na regionálnej úrovni uvedené. V zmysle ustanovenia čl. 2 ods. 2 písm. f) bod ii sa smernice NIS 2 vzťahuje aj na subjekty typu uvedeného v prílohe I alebo II bez ohľadu na ich veľkosť, ak subjekt je subjektom verejnej správy na regionálnej úrovni podľa definície členského štátu v súlade s vnútroštátnym právom, **ktorý po posúdení na základe rizík poskytuje služby, ktorých narušenie by mohlo mať významný vplyv na kritické spoločenské alebo hospodárske činnosti**. V prípade subjektov verejnej správy na regionálnej úrovni uvedených v predmetnom ustanovení sa v porovnaní s typom subjektu v prílohe I v odvetví Verejná správa navyše vyžaduje, aby išlo o subjekt, ktorý po posúdení na

[214] EURÓPSKA KOMISIA. *Commission staff working document impact assessment report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148. Brusel, 16.12.2020 SWD(2020) 345 final.*
[215] Tamže, s. 51.

základe rizík poskytuje služby, ktorých narušenie by mohlo mať významný vplyv na kritické spoločenské alebo hospodárske činnosti.

Subjekty verejnej správy ako kľúčové subjekty a dôležité subjekty

Subjekty verejnej správy môžu byť v zmysle smernice NIS 2 považované za kľúčové subjekty a dôležité subjekty pri aplikácií rôznych ustanovení čl. 3 ods. 1 smernice NIS 2.

V prvom rade v zmysle čl. 3 ods. 1 písm. d) smernice NIS 2 sú za kľúčové subjekty považované subjekty verejnej správy uvedené v článku 2 ods. 2 písm. f) bode i) smernice NIS 2. V prípade predmetného ustanovenia ide o subjekty verejnej správy na úrovni ústrednej štátnej správy podľa definície členského štátu v súlade s vnútroštátnym právom.[216]

V ďalších ustanoveniach čl. 3 ods. 1 smernice NIS 2 sa už priamo neodkazuje na subjekty verejnej správy a mohlo by sa zdať, že len subjekty verejnej správy na úrovni ústrednej štátnej správy by mali byť považované za kľúčové subjekty. Avšak máme za to, že za kľúčové subjekty možno v prípade ďalších ustanovení čl. 3 ods. 1 smernice NIS 2 za určitých podmienok považovať aj subjekty verejnej správy uvedené v článku 2 ods. 2 písm. f) bode ii) smernice NIS 2 (subjekty verejnej správy na regionálnej úrovni), ako aj subjekty verejnej správy uvedené ako typy subjektov v odvetví, resp. pododvetví inom ako je odvetvie „Verejná správa".

Napríklad ak bude subjekt verejnej správy na regionálnej úrovni identifikovaný ako kritický subjekt podľa smernice o odolnosti kritických subjektov, bude takýto subjekt považovaný za kľúčový subjekt. Subjekt verejnej správy môže byť prevádzkovateľom inteligentných dopravných systémov v odvetví „Doprava", pododvetvie „Cestná doprava" podľa prílohy I smernice NIS 2 ak presahuje limity pre stredné podniky. Taktiež platí, že v zmysle čl. 3 ods. 1 písm. g) smernice NIS 2 sa za kľúčové subjekty môžu považovať aj subjekty, ktoré daný členský štát označil pred 16. januárom 2023 ako prevádzkovateľov základných služieb v súlade so smernicou NIS alebo vnútroštátnym právom. Je na rozhodnutí členského štátu EÚ či tieto subjekty bude považovať za kľúčové subjekty. V tejto súvislosti je však otázne či tieto subjekty budú spĺňať konkrétne kritéria a požiadavky v zmysle smernice NIS 2. Máme za to, že prevádzkovatelia základných služieb (identifikovaní pred 16. januárom 2023) by mali byť považovaní za kľúčové subjekty len za podmienky, že spĺňajú požiadavky

[216] Smernica NIS 2, čl. 3 ods. 1 písm. d).

na kľúčové subjekty v zmysle smernice NIS 2 (pravidlo obmedzenia veľkosti, resp. konkrétne výnimky z tohto pravidla, definičné znaky subjektu verejnej správy). V praktickej rovine môže nastať situácia, že medzi subjektami verejnej správy, ktoré boli pred 16. januárom 2023 identifikovaní ako prevádzkovatelia základnej služby môžu byť nie len subjekty verejnej správy na úrovni ústrednej štátnej správy, ale aj subjekty verejnej správy na regionálnej úrovni a subjekty verejnej správy mimo odvetvia „Verejná správa".

V súvislosti s otázkou či subjekty verejnej správy môžu byť považované za dôležité subjekty je potrebné interpretovať ustanovenie čl. 3 ods. 2 smernice NIS 2, podľa ktorého: *„Na účely tejto smernice sa subjekty typu uvedeného v prílohe I alebo II, ktoré sa nepovažujú za kľúčové subjekty podľa odseku 1 tohto článku, považujú za dôležité subjekty. Patria sem subjekty označené členskými štátmi ako dôležité subjekty podľa článku 2 ods. 2 písm. b) až e).*"

Z predmetného ustanovenia vyplýva, že medzi dôležité subjekty možno zaradiť len také subjekty:

- ktorých typ je uvedený v prílohe I alebo II, avšak sa nepovažujú za kľúčové subjekty v zmysle čl. 3 ods. 1 smernice NIS 2 a
- sú označené členskými štátmi ako dôležité subjekty podľa čl. 2 ods. 2 písm. b) až e) smernice NIS 2.[217]

Logicky by sa mohlo zdať, že medzi dôležité subjekty by sme mohli zaradiť subjekty verejnej správy na regionálnej úrovni podľa ustanovenia čl. 2 ods. 2 písm. f), bod ii). Avšak subjekty verejnej správy na regionálnej úrovni nespĺňajú požiadavku na dôležité subjekty, v zmysle ktorej sú označené členskými štátmi ako dôležité subjekty podľa čl. 2 ods. 2 písm. b) až e) smernice NIS 2. Subjekty verejnej správy na regionálnej úrovni sú uvedené v čl. 2 ods. 2 písm. f), bod ii), a teda sú mimo rozmedzia písm. b) až e) spomínaného ustanovenia. Avšak ako bolo konštatované vyššie, subjekty verejnej správy môžu byť aj subjektami v iných odvetviach ako je „Verejná správa" a môže sa na nich vzťahovať smernica NIS 2 aj z iného dôvodu ako len toho, že sú kategóriou subjektu verejnej správy podľa čl. 2 ods. 2 písm. f) smernice NIS 2 v rámci výnimky z pravidla veľkosti.

[217] Zaujímavosťou je, že v prípade českého prekladu predmetného ustanovenia nie sú tieto dve požiadavky. kumulatívne. Ustanovenie čl. 3 ods. 2: *„Pro účely této směrnice se za důležité subjekty považují subjekty druhu uvedeného v příloze I nebo II, které nelze považovat za základní subjekty podle odstavce 1 tohoto článku. Patří k nim i subjekty, jež členské státy označily za důležité podle čl. 2 odst. 2 písm. b) až e).*"

Lex specialis a lex generalis

V oblasti kybernetickej bezpečnosti nie je ničím neobvyklým, že konkrétne subjekty budú regulované aj tzv. sektorovou úpravou. V zmysle smernice NIS 2 ak sa v odvetvových právnych aktoch EÚ vyžaduje, aby kľúčové alebo dôležité subjekty prijali **opatrenia na riadenie kybernetických rizík** alebo aby **nahlasovali významné incidenty**, a ak majú tieto požiadavky aspoň rovnocenný účinok ako povinnosti stanovené v smernici NIS 2, príslušné ustanovenia smernice NIS 2 vrátane ustanovení o dohľade a presadzovaní práva v kapitole VII smernice NIS 2 sa na takéto subjekty nevzťahujú.[218]

Ak sa odvetvové právne akty EÚ nevzťahujú na všetky subjekty v konkrétnom odvetví v pôsobnosti smernice NIS 2, príslušné ustanovenia smernice NIS 2 sa naďalej vzťahujú na subjekty, na ktoré sa odvetvové právne akty EÚ nevzťahujú.[219]

Otázka, či sa požiadavky na opatrenia na riadenie kybernetických rizík alebo požiadavky na nahlasovanie významných incidentov považujú za rovnocenné s povinnosťami ustanovenými v smernici NIS 2, sa posudzuje podľa nasledujúcich pravidiel:

a) Opatrenia na riadenie kybernetických rizík sa považujú za rovnocenné, ak majú prinajmenšom rovnaký účinok ako opatrenia ustanovené v článku 21 ods. 1 a 2 smernice NIS 2.
b) Požiadavky na nahlasovanie významných incidentov sa považujú za rovnocenné, ak odvetvový právny akt EÚ zabezpečuje jednotkám CSIRT, príslušným orgánom alebo jednotným kontaktným miestam podľa smernice NIS 2 okamžitý, a podľa potreby automatický a priamy, prístup k hláseniam o incidentoch a ak tieto požiadavky majú prinajmenšom rovnaký účinok ako požiadavky ustanovené v článku 23 ods. 1 až 6

4.2.2 Opatrenia

V zmysle smernice NIS 2 sú **riadiace orgány** kľúčových a dôležitých subjektov povinné **schváliť opatrenia** na riadenie kybernetických rizík, ktoré tieto subjekty prijali. Taktiež sú povinné **dohliadať** na ich vykonávanie. V prípade ak kľúčové a dôležité subjekty neplnia povinnosti v oblasti opatrení možno vyvodzovať **zodpovednosť** voči riadiacim orgánom týchto subjektov.[220]

[218] Smernica NIS 2, čl. 4 ods. 1.
[219] Smernica NIS 2, čl. 4 ods. 1.
[220] Smernica NIS 2, čl. 20 ods. 1.

Členovia riadiacich orgánov kľúčových a dôležitých subjektov sú povinní **absolvovať odbornú prípravu**. Taktiež majú členovia riadiacich orgánov kľúčových a dôležitých subjektov podporiť tieto subjekty v tom, aby svojim zamestnancom pravidelne poskytovali podobnú odbornú prípravu a ich zamestnanci tak získali dostatočné znalosti a zručnosti a vedeli rozpoznať riziká a posúdiť postupy riadenia kybernetických rizík a ich vplyv na služby poskytované subjektom.[221]

Kľúčové a dôležité subjekty sú povinné prijať:

> „*vhodné a primerané technické, operačné a organizačné opatrenia na riadenie rizík súvisiacich s bezpečnosťou sietí a informačných systémov, ktoré tieto subjekty využívajú na svoju činnosť alebo na poskytovanie svojich služieb a na prevenciu alebo minimalizáciu vplyvu incidentov na príjemcov ich služieb a na ďalšie služby*."[222]

V porovnaní so smernicou NIS upravuje smernica NIS 2 výpočet jednotlivých oblastí bezpečnostných opatrení, ktoré regulované subjekty majú implementovať. Predmetné opatrenia sú v zmysle smernice NIS 2 založené na **prístupe zohľadňujúcom všetky riziká**, ktorého cieľom je chrániť siete a informačné systémy a fyzické prostredie uvedených systémov pred incidentmi, a **zahŕňajú aspoň**:[223]

a) *zásady analýzy rizík a bezpečnosti informačných systémov;*
b) *riešenie incidentov;*
c) *kontinuitu činností, ako je riadenie zálohovania a obnova systému po havárii, a krízové riadenie;*
d) *bezpečnosť dodávateľského reťazca vrátane bezpečnostných aspektov týkajúcich sa vzťahov medzi jednotlivými subjektmi a ich priamymi dodávateľmi alebo poskytovateľmi služieb;*
e) *bezpečnosť pri nadobúdaní, vývoji a údržbe siete a informačných systémov vrátane riešenia zraniteľností a zverejňovania informácií o zraniteľnostiach;*
f) *zásady a postupy posudzovania účinnosti opatrení na riadenie kybernetických rizík;*

[221] Smernica NIS 2, čl. 20 ods. 2.
[222] Smernica NIS 2, čl. 21 ods. 1.
[223] Smernica NIS 2, čl. 21 ods. 2.

g) *základné postupy kybernetickej hygieny a odborná príprava v oblasti kybernetickej bezpečnosti;*

h) *zásady a postupy používania kryptografie, prípadne šifrovania;*

i) *bezpečnosť ľudských zdrojov, zásady kontroly prístupu a správu aktív;*

j) *v prípade potreby používanie riešení viacstupňovej alebo kontinuálnej autentifikácie, zabezpečenej hlasovej, obrazovej a textovej komunikácie a zabezpečených systémov komunikácie v núdzových situáciách v rámci subjektu.*

Na účely stanovenia technických, metodických, ako aj sektorových požiadaviek na opatrenia môže Komisia prijať vykonávacie akty.[224]

Takýmto vykonávacím aktom je **vykonávacie nariadenie Komisie (EÚ) 2024/2690**.[225] Predmetné vykonávacie nariadenie sa vzťahuje len na konkrétne **príslušné subjekty** v zmysle smernice NIS 2, a to konkrétne:

- poskytovateľov služieb DNS,
- správcov názvov TLD,
- poskytovateľov služieb cloud computingu,
- poskytovateľov služieb dátového centra,
- poskytovateľov sietí na sprístupňovanie obsahu,
- poskytovateľov riadených služieb,
- poskytovateľov riadených bezpečnostných služieb,
- poskytovateľov online trhov, internetových vyhľadávačov a platforiem služieb sociálnych sietí a

[224] Smernica NIS 2, čl. 21 ods. 5.

[225] Vykonávacie nariadenie Komisie (EÚ) 2024/2690 zo 17. októbra 2024, ktorým sa stanovujú pravidlá uplatňovania smernice (EÚ) 2022/2555, pokiaľ ide o technické a metodické požiadavky na opatrenia na riadenie kybernetických rizík a o bližšie určenie prípadov, v ktorých sa incident považuje za významný, vo vzťahu k poskytovateľom služieb DNS, správcom názvov TLD, poskytovateľom služieb cloud computingu, poskytovateľom služieb dátového centra, poskytovateľom sietí na sprístupňovanie obsahu, poskytovateľom riadených služieb, poskytovateľom riadených bezpečnostných služieb, poskytovateľom online trhov, internetových vyhľadávačov a platforiem služieb sociálnej siete a poskytovateľom dôveryhodných služieb. ENISA v júni 2025 publikovala Technical Implementation Guidance, ktoré predstavuje nezáväzné technické usmernenie k vykonávaciemu nariadeniu Komisie (EÚ) 2024/2690. Predmetné technické usmernenie konkretizuje technické a metodické požiadavky kybernetického riadenia rizík podľa smernice NIS2 pre príslušné subjekty. Ku každej požiadavke poskytuje odporúčania na implementáciu, príklady dôkazov použiteľných pri preukazovaní zavedenia opatrení a mapovanie na dobrú prax, medzinárodné a európske štandardy a národné rámce. ENISA zároveň zdôrazňuje, že nejde o právne záväzný dokument ani náhradu vnútroštátnych pokynov. Má slúžiť ako praktická pomôcka pre regulované subjekty aj príslušné orgány pri výklade a implementácii požiadaviek smernice NIS2. Dostupné na: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance.

- poskytovateľov dôveryhodných služieb

V súvislosti s opatreniami, ktoré tieto subjekty majú prijať boli v prílohe predmetného vykonávacieho nariadenia definované konkrétne **technické a metodické požiadavky** na opatrenia na riadenie kybernetických rizík uvedené v článku 21 ods. 2 písm. a) až j) smernice NIS 2.

PRÍKLAD

Vykonávacie nariadenie Komisie (EÚ) 2024/2690 – príloha

3. Riešenie incidentov [článok 21 ods. 2 písm. b) smernice (EÚ) 2022/2555]

3.1. Zásady riešenia incidentov

3.1.1. Na účely článku 21 ods. 2 písm. b) smernice (EÚ) 2022/2555 príslušné subjekty stanovia a vykonávajú zásady riešenia incidentov, ktorými sa stanovujú úlohy, povinnosti a postupy na včasné odhaľovanie incidentov, ich analýzu, zamedzenie ich šíreniu alebo reagovanie na ne, zotavenie sa z nich, ich zaznamenávanie a oznamovanie.

3.3. Oznamovanie udalostí

3.3.1. Príslušné subjekty zavedú jednoduchý mechanizmus, ktorý ich zamestnancom, dodávateľom a zákazníkom umožňuje oznamovať podozrivé udalosti.

3.3.2. Príslušné subjekty svojich dodávateľov a zákazníkov v prípade potreby informujú o mechanizme oznamovania udalostí a svojim zamestnancom poskytujú pravidelnú odbornú prípravu týkajúcu sa toho, ako sa mechanizmus používa.

4.2.3 Oznamovacie povinnosti

V rámci analýzy oznamovacích povinností podľa smernice NIS 2 sa zameriame na štyri základné otázky:

- kto je povinný oznamovaciu povinnosť splniť?
- čo je predmetom oznamovania?
- komu sa príslušné informácie oznamujú?
- v akej lehote musí byť oznámenie vykonané?

Osobitnú pozornosť budeme venovať otázke **predmetu oznamovania**, teda tomu, aké skutočnosti majú byť hlásené príslušným orgánom alebo jednotke CSIRT. V tejto súvislosti sa zameriame najmä na oznamovanie:

- incidentov,
- hrozieb,
- udalostí a
- zraniteľností,

keďže práve tieto kategórie predstavujú kľúčové situácie, pri ktorých právna úprava vyžaduje alebo predpokladá určitú formu oznámenia, hlásenia alebo výmeny informácií.

Kľúčové a dôležité subjekty sú povinné bez zbytočného odkladu oznámiť svojej jednotke CSIRT alebo v náležitých prípadoch svojmu príslušnému orgánu každý incident s významným vplyvom na poskytovanie ich služieb (**významný incident**). [226]

Na vznik oznamovacej povinnosti musia byť **kumulatívne splnené tieto požiadavky**:

a) musí ísť o **incident** v zmysle čl. 6 bodu 6 smernice NIS 2,
b) incident musí byť **významný** v zmysle čl. 23 ods. 3 smernice NIS 2.

Ad a)

Definícia pojmu „**incident**" použitá v smernici NIS 2 sa v porovnaní s definíciou použitou v smernici NIS významne mení. Smernica NIS 2 definuje incident ako:

> *„udalosť ohrozujúca dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov*."[227]

Prvá časť definície pojmu „incident" nekonkretizuje, o aké údaje ide. Predmetné údaje je potrebné vykladať v spojení s definíciou pojmu siete a informačné systémy v zmysle čl. 6 bodu 1 smernice NIS 2. V zmysle uvedeného ustanovenia pôjde o údaje, ktoré sú uchovávané, spracúvané, získavané alebo prenášané elektronickou komunikačnou sieťou alebo akýmkoľvek zariadením alebo skupinou vzájomne prepojených alebo súvisiacich zariadení, z ktorých jedno alebo viaceré podľa programu automaticky spracúvajú digitálne údaje na účely

[226] Smernica NIS 2, čl. 23 ods. 1.
[227] Smernica NIS 2, čl. 6 bod 6.

ich prevádzky, používania, ochrany a údržby. Pokiaľ ide o siete a informačné systémy, zohľadňujú sa iba tie siete a informačné systémy, ktoré subjekty využívajú na svoju činnosť alebo na poskytovanie svojich služieb a na prevenciu alebo minimalizáciu vplyvu incidentov na príjemcov ich služieb a na ďalšie služby. K tomuto záveru možno dospieť výkladom čl. 21 ods. 1 smernice NIS 2.

Kľúčové a dôležité subjekty sú v prípade potreby bez zbytočného odkladu povinné oznámiť príjemcom svojich služieb významné incidenty, ktoré by mohli nepriaznivo ovplyvniť poskytovanie daných služieb.[228]

Kľúčové a dôležité subjekty sú ďalej povinné oznámiť okrem iného všetky informácie, ktoré jednotke CSIRT alebo v náležitých prípadoch príslušnému orgánu umožnia určiť akýkoľvek cezhraničný vplyv incidentu.[229]

Ad b)

Podľa druhej požiadavky sa incident musí považovať za **významný**. Podľa čl. 23 ods. 3 smernice NIS 2 sa incident považuje za významný, ak:

a) spôsobil alebo má schopnosť spôsobiť dotknutému subjektu závažné prevádzkové narušenie služieb alebo finančnú stratu;
b) zasiahol alebo má schopnosť zasiahnuť iné fyzické alebo právnické osoby tým, že im spôsobí značnú majetkovú alebo nemajetkovú ujmu.

Uvedené požiadavky nemusia byť splnené kumulatívne. Takýto záver možno odôvodniť recitálom 101 smernice NIS 2, podľa ktorého: „*V tejto súvislosti by táto smernica mala zahŕňať oznamovanie incidentov, pri ktorých by sa na základe prvotného posúdenia vykonaného dotknutým subjektom mohlo predpokladať, že by mohli viesť k vážnemu narušeniu prevádzky služieb alebo finančným stratám uvedeného subjektu alebo by mohli zasiahnuť iné fyzické alebo právnické osoby tým, že by im spôsobili značnú majetkovú alebo nemajetkovú ujmu.*"

Kľúčové a dôležité subjekty sú povinné postúpiť jednotke CSIRT alebo v náležitých prípadoch príslušnému orgánu:

[228] Smernica NIS 2, čl. 23 ods. 1.
[229] Smernica NIS 2, čl. 23 ods. 1.

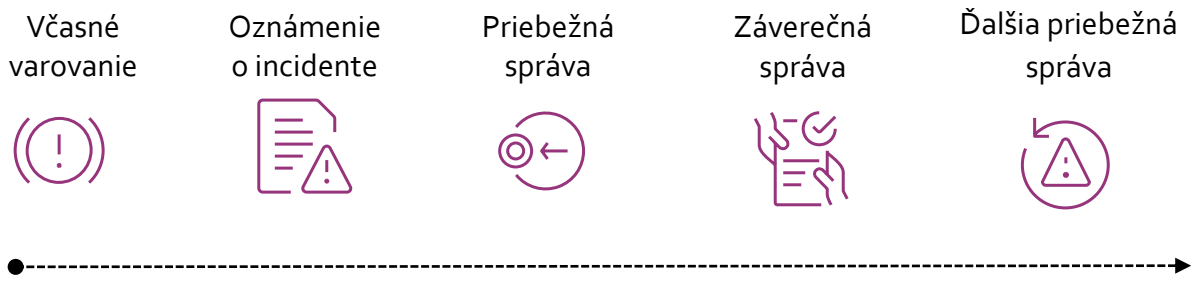
a) bez zbytočného odkladu a v každom prípade do **24 hodín** od zistenia významného incidentu **včasné varovanie,**[230]

b) bez zbytočného odkladu a v každom prípade do **72 hodín** po tom, ako sa dozvedeli o významnom incidente**, oznámenie o incidente,**[231]

c) na žiadosť jednotky CSIRT alebo v náležitých prípadoch príslušného orgánu **priebežnú správu** s relevantnou aktualizáciou daného stavu,[232]

d) najneskôr **jeden mesiac** po postúpení oznámenia o incidente **záverečnú správu**.[233]

V prípade **prebiehajúceho incidentu** v čase predkladania záverečnej správy dotknuté subjekty predložia v uvedenom čase ďalšiu priebežnú správu a záverečnú správu do jedného mesiaca odo dňa, keď incident vyriešili.[234]



Obrázok č. 5: Oznamovacie povinnosti týkajúce sa významného incidentu.

V súvislosti s **cezhraničným vplyvom** významného incidentu platí, že kľúčové a dôležité subjekty oznamujú okrem iného informácie umožňujúce jednotke CSIRT alebo v náležitých prípadoch príslušnému orgánu určiť cezhraničný vplyv incidentu. Ak dotknuté subjekty oznámia príslušnému orgánu významný incident, členský štát zabezpečí, aby uvedený príslušný orgán postúpil toto oznámenie po jeho prijatí jednotke CSIRT.[235]

Komisia môže prijať **vykonávacie akty,** ktorými sa spresnia prípady, v ktorých sa incident považuje za významný.[236] Predmetným vykonávacím aktom je už spomínané **vykonávacie nariadenie Komisie (EÚ) 2024/2690**.

[230] Smernica NIS 2, čl. 23 ods. 4 písm. a).
[231] Smernica NIS 2, čl. 23 ods. 4 písm. b).
[232] Smernica NIS 2, čl. 23 ods. 4 písm. c).
[233] Smernica NIS 2, čl. 23 ods. 4 písm. d).
[234] Smernica NIS 2, čl. 23 ods. 4 písm. e).
[235] Smernica NIS 2, čl. 23 ods. 1.
[236] Smernica NIS 2, čl. 23 ods. 11.

V zmysle predmetného vykonávacieho nariadenia sú uvedené konkrétne **všeobecné kritéria** pre určenie incidentu ako významného v zmysle smernice NIS 2 a **špecifické kritéria** v závislosti od jednotlivých príslušných subjektov.

Vo vzťahu k príslušným subjektom sa incident na účely článku 23 ods. 3 smernice NIS 2 považuje za **významný** vtedy, ak je splnené **aspoň jedno** z týchto (všeobecných) kritérií:[237]

a) *incident príslušnému subjektu spôsobil alebo môže spôsobiť priamu finančnú stratu, ktorá prevyšuje 500 000 EUR alebo 5 % celkového ročného obratu príslušného subjektu za predchádzajúci finančný rok, podľa toho, ktorá suma je nižšia;*
b) *incident spôsobil alebo môže spôsobiť únik obchodných tajomstiev príslušného subjektu, ako sú vymedzené v článku 2 bode 1 smernice (EÚ) 2016/943;*
c) *incident spôsobil alebo môže spôsobiť smrť fyzickej osoby;*
d) *incident spôsobil alebo môže spôsobiť značné poškodenie zdravia fyzickej osoby;*
e) *došlo k úspešnému, domnelo zlomyseľnému a neoprávnenému prístupu do sietí a informačných systémov, ktorý by mohol spôsobiť vážne narušenie prevádzky;*
f) *incident spĺňa kritériá uvedené v článku 4;*
g) *incident spĺňa aspoň jedno z kritérií uvedených v článkoch 5 až 14.*

Taktiež platí, že plánované prerušenia služby a zamýšľané následky činností plánovanej údržby, ktoré vykonávajú príslušné subjekty alebo ktoré sa vykonávajú v ich mene, sa nepovažujú za významné incidenty.[238]

Pri výpočte **počtu používateľov** dotknutých incidentom na účely článku 7 a článkov 9 až 14 vykonávacieho nariadenia Komisie (EÚ) 2024/2690 príslušné subjekty zohľadnia všetky tieto údaje:[239]

a) ***počet zákazníkov**, **ktorí uzatvorili zmluvu** s príslušným subjektom, ktorý im poskytuje prístup k svojim sieťam a informačným systémom alebo k službám poskytovaným alebo prístupným prostredníctvom týchto sietí a informačných systémov;*
b) ***počet fyzických a právnických osôb spojených s komerčnými zákazníkmi**, ktorí používajú siete a informačné systémy alebo služby poskytované alebo prístupné prostredníctvom týchto sietí a informačných systémov.*

[237] Vykonávacie nariadenie Komisie (EÚ) 2024/2690, čl. 3 ods. 1.
[238] Vykonávacie nariadenie Komisie (EÚ) 2024/2690, čl. 3 ods. 2.
[239] Vykonávacie nariadenie Komisie (EÚ) 2024/2690, čl. 3 ods. 3.

Vykonávacie nariadenie Komisie (EÚ) 2024/2690 taktiež upravuje tzv. **opakujúce sa incidenty**. Ide o incidenty, ktoré sa jednotlivo nepovažujú za významný incident v zmysle článku 3 vykonávacieho nariadenia Komisie (EÚ) 2024/2690, ale spoločne sa považujú za jeden významný incident, ak spĺňajú kumulatívne všetky tieto kritériá:[240]

a) *vyskytli sa aspoň dvakrát za šesť mesiacov;*
b) *majú rovnakú zjavnú hlavnú príčinu;*
c) *spoločne spĺňajú kritériá uvedené v článku 3 ods. 1 písm. a).*

Ako bolo uvedené vyššie, v závislosti od jednotlivých príslušných subjektov sú stanovené konkrétne špecifické kritériá pre významný incident.

Smernica NIS 2 taktiež upravuje možnosť **informovania verejnosti** o významnom incidente. Jednotka CSIRT, prípadne príslušný orgán členského štátu a v náležitých prípadoch jednotky CSIRT alebo príslušné orgány ďalších dotknutých členských štátov môžu informovať o významnom incidente verejnosť alebo požiadať o to daný subjekt za splnenia niekoľkých podmienok. V prvom rade musí prebehnúť porada s dotknutým subjektom. Druhou podmienkou je, ak je informovanie verejnosti potrebné na zabránenie významnému incidentu alebo riešenie prebiehajúceho incidentu alebo ak je zverejnenie významného incidentu vo verejnom záujme z iného dôvodu.[241]

V náležitých prípadoch kľúčové a dôležité subjekty bez zbytočného odkladu oznámili príjemcom svojich služieb, ktorí potenciálne čelia **významnej kybernetickej hrozbe**, všetky opatrenia alebo nápravné kroky, ktoré títo príjemcovia môžu v reakcii na danú hrozbu prijať. Subjekty v prípade potreby týchto príjemcov informujú aj o samotnej významnej kybernetickej hrozbe.[242]

Pri definovaní pojmu **kybernetická hrozba** smernica NIS 2 odkazuje na definíciu použitú v čl. 2 bode 8 aktu o kybernetickej bezpečnosti. Podľa tejto predmetnej definície je kybernetická hrozba:

> *„každá potenciálna okolnosť, udalosť alebo činnosť, ktorá by mohla poškodiť, narušiť alebo inak negatívne ovplyvniť siete a informačné systémy, užívateľov takýchto systémov a iné osoby*."

[240] Vykonávacie nariadenie Komisie (EÚ) 2024/2690, čl. 3 ods. 4.
[241] Smernica NIS 2, čl. 23 ods. 7.
[242] Smernica NIS 2, čl. 23 ods. 2.

Významná kybernetická hrozba je definovaná ako:

„kybernetická hrozba, o ktorej možno na základe jej technických charakteristík predpokladať, že má potenciál mať závažný vplyv na sieť a informačné systémy subjektu alebo používateľov služieb subjektu tým, že spôsobí značnú hmotnú alebo nehmotnú ujmu."[243]

Smernica NIS 2 neupravuje iba povinné oznamovanie významných incidentov, ale umožňuje aj **dobrovoľné oznamovanie** relevantných informácií. Ide o mechanizmus, ktorého cieľom je podporiť včasné zdieľanie poznatkov o kybernetických incidentoch, kybernetických hrozbách a udalostiach odvrátených v poslednej chvíli.

Kľúčové a dôležité subjekty môžu jednotkám CSIRT alebo prípadne príslušným orgánom oznamovať **incidenty, kybernetické hrozby, ako aj udalosti odvrátené v poslednej chvíli**.[244] Pojem udalosť odvrátená v poslednej chvíli je definovaná ako:

„udalosť odvrátená v poslednej chvíli" je udalosť, ktorá by mohla ohroziť dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov, ale ktorej vzniku sa úspešne zabránilo alebo ku ktorej nedošlo."[245]

Subjekty, ktoré nie sú kľúčovými subjektami ani dôležitými subjektami môžu jednotkám CSIRT alebo prípadne príslušným orgánom oznamovať významné incidenty, kybernetické hrozby a udalosti odvrátené v poslednej chvíli.[246]

Dobrovoľné oznámenia sa spracúvajú rovnakým postupom ako oznámenia podľa článku 23 smernice NIS 2. Avšak, členské štáty môžu pri spracúvaní oznámení uprednostniť povinné oznámenia pred oznámeniami podanými dobrovoľne.[247]

[243] Smernica NIS 2, čl. 6 bod 11.
[244] Smernica NIS 2, čl. 30 ods. 1 písm. a).
[245] Smernica NIS 2, čl. 6 bod 5.
[246] Smernica NIS 2, čl. 30 ods. 1 písm. b).
[247] Smernica NIS 2, čl. 30 ods. 2.

V súvislosti s oznamovaním zraniteľností platí, že fyzické alebo právnické osoby môžu na požiadanie nahlásiť **zraniteľnosť** jednotke CSIRT určenej za koordinátora anonymne. Zraniteľnosť je definovaná ako:

> *„slabá stránka, náchylnosť alebo chyba produktov IKT alebo služieb IKT, ktorá môže byť zneužitá kybernetickou hrozbou*".[248]

PRÍKLAD

Vykonávacie nariadenie Komisie (EÚ) 2024/2690

Článok 13

Významné incidenty, pokiaľ ide o poskytovateľov platforiem služieb sociálnej siete

V prípade poskytovateľov platforiem služieb sociálnej siete sa incident považuje za významný v zmysle článku 3 ods. 1 písm. g), ak spĺňa **aspoň jedno** z týchto kritérií:

a) platforma služieb sociálnej siete je úplne nedostupná pre viac ako 5 % používateľov tejto platformy služieb sociálnej siete v Únii alebo pre viac ako 1 milión používateľov tejto platformy služieb sociálnej siete v Únii, podľa toho, ktorý údaj je nižší;

b) viac ako 5 % používateľov platformy služieb sociálnej siete v Únii alebo viac ako 1 milión používateľov platformy služieb sociálnej siete v Únii, podľa toho, ktorý údaj je nižší, je dotknutých obmedzenou dostupnosťou tejto platformy služieb sociálnej siete;

c) integrita, dôvernosť alebo pravosť uchovávaných, prenášaných alebo spracúvaných údajov súvisiacich s poskytovaním platformy služieb sociálnej siete je ohrozená v dôsledku domnelo zlomyseľného konania;

d) integrita, dôvernosť alebo pravosť uchovávaných, prenášaných alebo spracúvaných údajov súvisiacich s poskytovaním platformy služieb sociálnej siete je ohrozená s dosahom na viac ako 5 % používateľov tejto platformy služieb sociálnej siete v Únii alebo na viac ako 1 milión používateľov tejto platformy služieb sociálnej siete v Únii, podľa toho, ktorý údaj je nižší.

[248] Smernica NIS 2, čl. 6 bod 15.

4.2.4 Dohľad a presadzovanie práva

Smernica NIS 2 posilňuje právomoci v oblasti dohľadu a opatrení, ktoré pomáhajú zabezpečiť účinné dodržiavanie povinností stanovených v smernici NIS 2. Na tento účel bol stanovený minimálny **zoznam opatrení a prostriedkov dohľadu**, prostredníctvom ktorých môžu príslušné orgány dohliadať na plnenie povinností zo strany kľúčových a dôležitých subjektov.

Smernica NIS 2 rozlišuje **režim dohľadu** medzi kľúčovými a dôležitými subjektmi s cieľom zabezpečiť spravodlivú rovnováhu povinností pre oba typy subjektov aj pre príslušné orgány. V tejto súvislosti podliehajú kľúčové subjekty komplexnému režimu dohľadu ex ante aj ex post, zatiaľ čo dôležité subjekty by mali podliehať ľahšiemu režimu dohľadu, a to iba ex post. Od dôležitých subjektov by sa preto nemalo vyžadovať systematické dokumentovanie súladu s opatreniami na riadenie kybernetických rizík, zatiaľ čo príslušné orgány by mali uplatňovať reaktívny ex post prístup k dohľadu, a teda by nemali mať všeobecnú povinnosť dohliadať na tieto subjekty.

V učebnici objasníme opatrenia dohľadu a presadzovania práva týkajúce sa kľúčových subjektov.[249] Opatrenia dohľadu alebo presadzovania práva uložené **kľúčovým subjektom** v súvislosti s povinnosťami stanovenými v smernici NIS 2 musia byť účinné, primerané a odrádzajúce a zároveň zohľadňovali okolnosti každého jednotlivého prípadu.[250]

Príslušné orgány pri vykonávaní svojich **úloh dohľadu nad kľúčovými subjektmi** majú **právomoc** podrobiť tieto subjekty prinajmenšom:[251]

a) *inšpekciám na mieste a dohľadu na diaľku vrátane náhodných kontrol, ktoré vykonávajú vyškolení odborníci;*
b) *pravidelným a cieleným bezpečnostným auditom, ktoré vykonáva nezávislý orgán alebo príslušný orgán;*
c) *auditom ad hoc, a to v prípadoch odôvodnených významným incidentom alebo porušením tejto smernice kľúčovým subjektom*
d) *bezpečnostným kontrolám podľa objektívnych, nediskriminačných, spravodlivých a transparentných kritérií posudzovania rizík, v prípade potreby v spolupráci s dotknutým subjektom;*

[249] K opatreniam dohľadu a presadzovania práva týkajúce sa dôležitých subjektov pozri čl. 33 smernice NIS 2.
[250] Smernica NIS 2, čl. 32 ods. 1.
[251] Smernica NIS 2, čl. 32 ods. 2.

e) *žiadostiam o informácie potrebné na posúdenie opatrení na riadenie kybernetických rizík, ktoré dotknutý subjekt prijal, vrátane zdokumentovaných politík kybernetickej bezpečnosti, ako aj dodržiavania povinnosti predložiť informácie príslušným orgánom podľa článku 27;*

f) *žiadostiam o prístup k údajom, dokumentom a informáciám potrebným na plnenie ich úloh dohľadu;*

g) *žiadostiam o dôkazy vykonávania politík kybernetickej bezpečnosti, ako sú výsledky bezpečnostných auditov uskutočnených kvalifikovaným audítorom a príslušné podkladové dôkazy.*

Príslušné orgány majú pri vykonávaní svojich **právomocí presadzovania práva** vo vzťahu ku kľúčovým subjektom právomoc prinajmenšom:[252]

a) *vydávať varovania o porušeniach tejto smernice dotknutými subjektmi;*

b) *prijímať záväzné pokyny, a to aj v súvislosti s opatreniami potrebnými na prevenciu alebo nápravu incidentu, ako aj lehotami na vykonávanie takýchto opatrení a podávanie správ o ich vykonávaní, alebo príkaz, ktorým sa od dotknutých subjektov vyžaduje napraviť zistené nedostatky alebo porušenia tejto smernice;*

c) *nariadiť dotknutým subjektom, aby upustili od konania, ktoré porušuje túto smernicu, a takéto konanie neopakovali;*

d) *nariadiť dotknutým subjektom, aby určeným spôsobom a v určenej lehote zosúladili svoje opatrenia na riadenie kybernetických rizík s článkom 21 alebo splnili oznamovacie povinnosti stanovené v článku 23;*

e) *nariadiť dotknutým subjektom, aby informovali fyzické alebo právnické osoby, v súvislosti s ktorými poskytujú služby alebo vykonávajú činnosti, ktoré sú potenciálne zasiahnuté významnou kybernetickou hrozbou, o povahe hrozby, ako aj o akýchkoľvek možných ochranných alebo nápravných opatreniach, ktoré môžu tieto fyzické alebo právnické osoby prijať v reakcii na danú hrozbu;*

f) *nariadiť dotknutým subjektom, aby v primeranej lehote vykonali odporúčania poskytnuté na základe bezpečnostného auditu;*

g) *určiť monitorujúceho úradníka s presne vymedzenými úlohami na určité obdobie, ktorý bude dohliadať na dodržiavanie článkov 21 a 23 dotknutými subjektmi;*

[252] Smernica NIS 2, čl. 32 ods. 4.

h) *nariadiť dotknutým subjektom, aby určeným spôsobom zverejnili aspekty porušovania tejto smernice;*

i) *uložiť správnu pokutu podľa článku 34 alebo požiadať o jej uloženie príslušné orgány, súdy alebo tribunály v súlade s vnútroštátnym právom, a to popri ktoromkoľvek z opatrení uvedených v písmenách a) až h) tohto odseku.*

Ak sa **opatrenia na presadzovanie práva ukážu ako neúčinné**, príslušné orgány majú právomoc stanoviť lehotu, v rámci ktorej je kľúčový subjekt povinný prijať potrebné opatrenia na nápravu nedostatkov alebo splniť požiadavky týchto orgánov. V prípade ak sa požadované opatrenie v stanovenej lehote neprijme, príslušné orgány majú právomoc:[253]

a) ***dočasne pozastaviť certifikáciu alebo povoľovanie*** *alebo požiadať certifikačný alebo povoľujúci subjekt, súd, alebo tribunál v súlade s vnútroštátnym právom, aby dočasne pozastavil certifikáciu alebo povoľovanie časti alebo všetkých relevantných služieb, ktoré kľúčový subjekt poskytuje, alebo činností, ktoré kľúčový subjekt vykonáva;*

b) *od príslušných orgánov, súdov alebo tribunálov v súlade s vnútroštátnym právom požadovať* ***uloženie dočasného zákazu vykonávať riadiace funkcie*** *v tomto kľúčovom subjekte, a to akejkoľvek fyzickej osobe zodpovednej za vykonávanie riadiacich úloh na úrovni výkonného riaditeľa alebo právneho zástupcu v tomto kľúčovom subjekte.*

Dočasné pozastavenia alebo zákazy sa uplatňujú len dovtedy, kým dotknutý subjekt neprijme potrebné opatrenia na nápravu nedostatkov alebo nesplní požiadavky príslušného orgánu, ktorý takéto opatrenia presadzovania práva uložil. Ukladanie takýchto dočasných pozastavení alebo zákazov musí podliehať primeraným procesným zárukám podľa všeobecných zásad práva EÚ a charty vrátane práva na účinný prostriedok nápravy a na spravodlivý proces, prezumpciu neviny a práva na obhajobu. Opatrenia presadzovania práva neuplatňujú na subjekty verejnej správy, na ktoré sa vzťahuje smernica NIS 2.[254]

4.2.5 Správne pokuty ukladané kľúčovým a dôležitým subjektom

Správne pokuty ukladané kľúčovým a dôležitým subjektom v súvislosti s porušeniami smernice NIS 2 musia byť účinné, primerané a odrádzajúce a zároveň zohľadňovali okolnosti každého jednotlivého prípadu.[255]

[253] Smernica NIS 2, čl. 32 ods. 5.
[254] Smernica NIS 2, čl. 32 ods. 5.
[255] Smernica NIS 2, čl. 34 ods. 1.

V prípade porušenia článku 21 (opatrenia na riadenie kybernetických rizík) alebo článku 23 (oznamovacia povinnosť) smernice NIS 2 sa **kľúčovým subjektom** ukladajú správne pokuty v maximálnej výške 10 000 000 EUR alebo v maximálnej výške 2 % celkového celosvetového ročného obratu v predchádzajúcom finančnom roku podniku, ku ktorému kľúčový subjekt patrí, podľa toho, ktorá suma je vyššia.[256]

V prípade porušenia článku 21 (opatrenia na riadenie kybernetických rizík) alebo článku 23 (oznamovacia povinnosť) smernice NIS 2 sa **dôležitým subjektom** ukladajú správne pokuty v maximálnej výške 7 000 000 EUR alebo v maximálnej výške 1,4 % celkového celosvetového ročného obratu v predchádzajúcom finančnom roku podniku, ku ktorému dôležitý subjekt patrí, podľa toho, ktorá suma je vyššia.[257]

4.3 Akt o kybernetickej bezpečnosti[258]

Ďalším legislatívnym aktom z oblasti kybernetickej bezpečnosti prijatým na úrovni EÚ je nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúre Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (ďalej len „**akt o kybernetickej bezpečnosti**").

4.3.1 Predmet úpravy a rozsah pôsobnosti

Akt o kybernetickej bezpečnosti si podobne ako smernica NIS kladie za cieľ zaistiť riadne fungovanie vnútorného trhu, avšak navyše sa usiluje o dosiahnutie vysokej úrovne kybernetickej bezpečnosti, kybernetickej odolnosti a dôvery v rámci EÚ. Na splnenie týchto cieľov sa:

- definovali ciele, úlohy a organizačné aspekty týkajúce sa **agentúry ENISA** (**Agentúra Európskej únie pre kybernetickú bezpečnosť**) a

[256] Smernica NIS 2, čl. 34 ods. 4.
[257] Smernica NIS 2, čl. 34 ods. 5.
[258] K januáru 2026 je v legislatívnom procese návrh nariadenia Európskeho parlamentu a Rady o Agentúre Európskej únie pre kybernetickú bezpečnosť (ENISA), európskom rámci certifikácie kybernetickej bezpečnosti a bezpečnosti dodávateľského reťazca IKT a o zrušení nariadenia (EÚ) 2019/881 (akt o kybernetickej bezpečnosti 2). Dostupné na: https://eur-lex.europa.eu/procedure/EN/2026_11.

- vytvára rámec pre zavádzanie **európskych systémov certifikácie kybernetickej bezpečnosti** na zabezpečenie primeranej úrovne kybernetickej bezpečnosti produktov IKT, služieb IKT a procesov IKT v EÚ.[259]

4.3.2 Agentúra ENISA

Agentúra ENISA je právnou nástupkyňou Agentúry Európskej únie pre sieťovú a informačnú bezpečnosť a sídli v Grécku. Plnením úloh, ktoré agentúre ENISA boli zverené aktom o kybernetickej bezpečnosti, sa má dosiahnuť vysoká spoločná úroveň kybernetickej bezpečnosti v celej EÚ a prispieť k zníženiu fragmentácie vnútorného trhu.[260]

Medzi úlohy Agentúry ENISA patrí napr. pomoc pri tvorbe legislatívnych iniciatív, ktoré sa týkajú kybernetickej bezpečnosti, najmä poskytovaním nezávislých stanovísk a analýz. Taktiež pomáha členským štátom pri konzistentnom vykonávaní politiky a práva EÚ v oblasti kybernetickej bezpečnosti, najmä v súvislosti so smernicou NIS, a to aj vydávaním stanovísk, usmernení, poskytovaním poradenstva a pod.[261]

PRÍKLAD

Agentúra ENISA publikovala stovky analýz, správ, návodov či štúdií z rôznych oblastí kybernetickej bezpečnosti. V súvislosti so smernicou NIS boli publikované napr. správa s názvom *Gaps in NIS standardisation - Recommendations for improving NIS in EU standardisation policy*[262] či *Good practices on interdependencies between OES and DSPs.*[263]

Agentúra ENISA pomáha členským štátom v ich úsilí zlepšovať prevenciu, odhaľovanie a analýzu kybernetických hrozieb a incidentov a schopnosť reagovať na ne tým, že im poskytuje vedomosti a odborné znalosti. Taktiež pravidelne organizuje kybernetickobezpečnostné cvičenia na úrovni EÚ a analyzuje nastupujúce technológie a poskytuje tematicky zamerané posúdenia očakávaných spoločenských, právnych,

[259] Čl. 1 ods. 1 aktu o kybernetickej bezpečnosti.
[260] Čl. 3 ods. 1 aktu o kybernetickej bezpečnosti.
[261] Čl. 5 ods. 2 aktu o kybernetickej bezpečnosti.
[262] Dostupné na: https://www.enisa.europa.eu/publications/gaps-eu-standardisation.
[263] Dostupné na: https://www.enisa.europa.eu/publications/good-practices-on-interdependencies-between-oes-and-dsps.

hospodárskych a regulačných vplyvov technologických inovácií na kybernetickú bezpečnosť.[264]

PRÍKLAD
Agentúra ENISA publikovala v súvislosti s novými technológiami viacero správ. Ako príklady možno uviesť správy s názvom *Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving*[265], *ENISA good practices for security of Smart Cars*[266] či *Securing Machine Learning Algorithms.*[267]

4.3.3 Pojmy kybernetická bezpečnosť a kybernetická hrozba

Akt o kybernetickej bezpečnosti obsahuje **prvú legálnu definíciu pojmu kybernetická bezpečnosť** na úrovni práva EÚ, v zmysle ktorej je kybernetická bezpečnosť definovaná ako:

> *„činnosti potrebné na ochranu sietí a informačných systémov, užívateľov takýchto systémov a iných osôb dotknutých kybernetickými hrozbami.*"[268]

Pri porovnaní pojmu kybernetická bezpečnosť a pojmu bezpečnosť sietí a informačných systémov v zmysle smernice NIS, možno vidieť niekoľko odlišností. Zatiaľ, čo pri pojme bezpečnosť sietí a informačných systémov je hlavným cieľom odolávať konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb, v prípade pojmu kybernetická bezpečnosť je cieľom ochrana sietí a informačných systémov, užívateľov takýchto systémov a iných osôb. Taktiež v prípade definície pojmu kybernetická bezpečnosť možno vidieť, že je potrebné chrániť nielen siete a informačné systémy, ale aj ich **užívateľov a iné osoby**, dotknuté kybernetickými hrozbami. V porovnaní s definíciou bezpečnosti sietí a informačných systémov použitej v smernici NIS ide o výrazný posun, čo do ochrany

[264] Čl. 6, 7, 9 aktu o kybernetickej bezpečnosti.
[265] Dostupné na: https://www.enisa.europa.eu/publications/enisa-jrc-cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving.
[266] Dostupné na: https://www.enisa.europa.eu/publications/smart-cars.
[267] Dostupné na: https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms.
[268] Čl.2 bod 1 aktu o kybernetickej bezpečnosti.

fyzických a právnických osôb pred kybernetickými hrozbami. **Kybernetická hrozba** je definovaná ako:

> *„každá potenciálna okolnosť, udalosť alebo činnosť, ktorá by mohla poškodiť, narušiť alebo inak negatívne ovplyvniť siete a informačné systémy, užívateľov takýchto systémov a iné osoby."*[269]

Z vyššie uvedenej definície vyplýva, že nielen siete a informačné systémy, ale aj užívatelia takýchto systémov a iné osoby môžu byť poškodené, narušené alebo inak negatívne ovplyvnené. Predmetná definícia sa teda týka všetkých osôb, nielen samotných užívateľov konkrétnych systémov.

PRÍKLAD

V praktickej rovine možno demonštrovať negatívny vplyv kybernetickej hrozby na užívateľov konkrétnych sietí a iné osoby na nasledujúcom príklade. Následkom úspešného kybernetického útoku na elektroenergetický podnik, ktorý vyrába elektrickú energiu je prerušenie výroby elektrickej energie. Priamo je zasiahnutý podnik (užívateľ tohto systému), ale aj iné osoby, ako napr. iné elektroenergetické podniky, ktoré distribuujú elektrickú energiu a v konečnom dôsledku aj osoby, ktoré odberajú elektrickú energiu.

Úspešný kybernetický útok na inteligentné dopravné systémy spôsobí ich nefunkčnosť. Primárne budú zasiahnutí prevádzkovatelia takýchto systémov (užívateľ tohto systému), ale aj účastníci cestnej premávky.

V recitáli 3 aktu o kybernetickej bezpečnosti je vyjadrená potreba ochrany fyzických osôb nasledovne:

> *„Rastúca digitalizácia a pripojiteľnosť zvyšujú kybernetickobezpečnostné riziká, takže spoločnosť ako celok sa stáva zraniteľnejšou z hľadiska kybernetických*

[269] Čl. 2 bod 8 aktu o kybernetickej bezpečnosti.

hrozieb a zvyšuje sa nebezpečenstvo, ktorému čelia fyzické osoby, vrátane zraniteľných osôb, ako sú napríklad deti."

Kybernetické hrozby môžu mať negatívny vplyv aj na samotné deti. V súčasnosti možno medzi najčastejšie sa vyskytujúce hrozby pre deti v online prostredí zaradiť kyberšikanu, nevhodný obsah (intímne alebo sexuálne explicitné obrázky či videá), sexting (posielanie sexuálne explicitných správ a intímnych fotiek), sextortion (útočník požaduje výkupné v opačnom prípade zverejní intímne fotografie obete), nadmerné zdieľanie osobných údajov či online predátorstvo.

4.3.4 Európsky systém certifikácie kybernetickej bezpečnosti

Vo všeobecnosti možno povedať, že v rámci procesu **certifikácie** subjekt, ktorý je akreditovaný na to, aby udeľoval certifikáty (certifikačná autorita), posudzuje či výrobok, služba alebo proces spĺňa konkrétne požiadavky (certifikačná schéma). Certifikačnú autoritu možno označiť aj ako subjekt, ktorý posudzuje zhodu. Na takéto hodnotenie potrebuje certifikačný subjekt testovacie laboratórium, v rámci ktorého sú produkty, služby a procesy otestované. Certifikačná autorita má vlastné testovacie laboratórium alebo len spolupracuje na zmluvnom základe s testovacím laboratóriom. V prípade certifikácie pôjde o hodnotenie súladu výrobku, služby či postupu s požiadavkami, ktoré stanovujú právne prepisy či technické normy. Výsledkom certifikácie je vydanie certifikátu, ktorý potvrdzuje, že produkt, služba, proces spĺňa požiadavky konkrétnej úrovne.[270]

PRÍKLAD
Aby mohol výrobca vozidla požiadať o typové schválenie vozidla vzhľadom na kybernetickú bezpečnosť, bude musieť mať platné osvedčenie o zhode systému riadenia kybernetickej bezpečnosti. V tejto súvislosti musí výrobca vozidiel, resp. jeho splnomocnený zástupca podať žiadosť o osvedčenie o zhode systému riadenia kybernetickej bezpečnosti schvaľovaciemu úradu, ktorý bude vykonávať posudzovanie výrobcu a ktorý vydá osvedčenie o zhode systému riadenia kybernetickej bezpečnosti. Výrobca vozidiel musí v rámci procesu udelenia osvedčenia o zhode systému riadenia kybernetickej bezpečnosti

[270] VOSTOUPAL, J.: *Certifikace kyberbezpečnostních technologií*. *In* Revue pro právo a technologie. 2019, č. 20, s. 163-165.

a následného typového schválenia preukázať, že má implementované postupy používané na monitorovanie, odhaľovanie a reagovanie na kybernetické útoky, kybernetické hrozby a zraniteľnosti v rámci typov vozidiel. V prípade ak je posudzovanie úspešné, je výrobcovi udelené osvedčenie s názvom Osvedčenie o zhode systému riadenia kybernetickej bezpečnosti.

Akt o kybernetickej bezpečnosti vytvára **systém certifikácie v oblasti kybernetickej bezpečnosti**, ktorý by mal zabezpečiť dostatočnú úroveň kybernetickej bezpečnosti produktov, postupov a služieb v EÚ. Je potrebné podotknúť, že akt o kybernetickej bezpečnosti nevytvára jednotlivé certifikačné schémy, ale vytvára rámec pre prijímanie európskych certifikačných schém.

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. Predmetné nariadenie ako príklady technológií, pri ktorých je potrebné zabezpečiť vysokú úroveň kybernetickej bezpečnosti uvádza autonómne vozidlá, systémy elektronickej kontroly zdravia alebo priemyselnej automatizácie.

V zmysle aktu o kybernetickej bezpečnosti možno certifikovať produkty IKT (napr. router), služby IKT (napr. autentifikácia klientov online) a procesy IKT (napr. systém riadenia bezpečnosti informácií).

Produkt IKT predstavuje:

„prvok alebo skupina prvkov siete alebo informačného systému."[271]

Služba IKT je definovaná ako:

„služba pozostávajúca úplne alebo prevažne z prenosu, ukladania, získavania alebo spracúvania informácií prostredníctvom sietí a informačných systémov."[272]

Proces IKT predstavuje:

[271] Čl. 2 bod 12 aktu o kybernetickej bezpečnosti.
[272] Čl. 2 bod 13 aktu o kybernetickej bezpečnosti.

„súbor činností vykonávaných pre navrhnutie, vyvinutie, poskytnutie alebo údržbu produktu IKT alebo služby IKT."[273]

Certifikačná autorita čiže orgán posudzovania zhody musí byť v zmysle aktu o kybernetickej bezpečnosti akreditovaný vnútroštátnym akreditačným orgánom, pričom sa akreditácia vydá len vtedy, ak orgán posudzovania zhody spĺňa požiadavky stanovené v prílohe k aktu o kybernetickej bezpečnosti.[274]

Orgán posudzovania zhody musí byť zriadený podľa vnútroštátneho práva a má právnu subjektivitu a taktiež musí byť nezávislý od organizácie alebo produktov IKT, služieb IKT alebo procesov IKT, ktoré posudzuje a musí spĺňať konkrétne požiadavky v zmysle prílohy aktu o kybernetickej bezpečnosti.[275]

Využitie certifikácie kybernetickej bezpečnosti je dobrovoľné, pokiaľ sa to nestanovuje inak v právnych predpisoch EÚ alebo vnútroštátnych právnych predpisoch, ktorými sa stanovujú bezpečnostné požiadavky týkajúce sa 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.[276]

Po úspešnom hodnotení splnenia požiadaviek na produkt IKT, službu IKT alebo proces IKT v procese posudzovania zhody, vydáva orgán posudzovania zhody **európsky certifikát kybernetickej bezpečnosti**. Európsky certifikát kybernetickej bezpečnosti predstavuje potvrdenie, že hodnotenie bolo vykonané správne. Certifikát sám osebe ešte nezaručuje, že certifikované produkty IKT, služby IKT a procesy IKT sú kyberneticky bezpečné.[277] K takémuto záveru možno dospieť najmä s ohľadom na nové hrozby, ktoré v čase posudzovania zhody nemuseli ani existovať. Výsledný certifikát bude uznávaný vo všetkých

[273] Čl. 2 bod 13 aktu o kybernetickej bezpečnosti.
[274] Čl. 60 aktu o kybernetickej bezpečnosti.
[275] Príloha aktu o kybernetickej bezpečnosti.
[276] Recitál 57 aktu o kybernetickej bezpečnosti.
[277] Recitál 77 aktu o kybernetickej bezpečnosti.

členských štátoch, čo uľahčí podnikom cezhraničné obchodovanie a zákazníkom pochopiť bezpečnostné prvky produktu alebo služby.[278]

Európsky systém certifikácie kybernetickej bezpečnosti musí byť navrhnutý tak, aby podľa potreby splnil konkrétne bezpečnostné ciele:[279]

a) chrániť uchovávané, prenášané alebo inak spracúvané údaje pred náhodným či neoprávneným uchovávaním, spracúvaním, prístupom alebo poskytnutím počas celého životného cyklu produktu IKT, služby IKT alebo procesu IKT;

b) chrániť uchovávané, prenášané alebo inak spracúvané údaje pred náhodným či neoprávneným zničením, stratou alebo zmenou alebo nedostatočnou dostupnosťou počas celého životného cyklu produktu IKT, služby IKT alebo procesu IKT;

c) umožňovať oprávneným osobám, programom alebo zariadeniam prístup výlučne k tým údajom, službám alebo funkciám, na ktoré sa vzťahujú ich prístupové práva;

d) identifikovať a dokumentovať známe závislosti a zraniteľnosti;

e) zaznamenávať, ktoré údaje, služby alebo funkcie boli predmetom prístupu, použité alebo inak spracúvané, kedy a kým;

f) umožňovať overenie, ktoré údaje, služby alebo funkcie boli predmetom prístupu, použité alebo inak spracúvané, kedy a kým;

g) overovať, či produkty IKT, služby IKT a procesy IKT neobsahujú známe zraniteľnosti;

h) v prípade fyzického alebo technického incidentu včas obnoviť dostupnosť údajov, služieb a funkcií a prístup k nim;

i) aby produkty IKT, služby IKT a procesy IKT boli bezpečné štandardne a už v štádiu návrhu;

j) aby sa produkty IKT, služby IKT a procesy IKT dodávali alebo poskytovali s aktualizovaným softvérom a hardvérom, ktoré neobsahujú verejne známe zraniteľnosti, a dodávali alebo poskytovali s mechanizmami na bezpečnú aktualizáciu.

[278] Čl. 56 ods. 10 aktu o kybernetickej bezpečnosti.
[279] Čl. 51 aktu o kybernetickej bezpečnosti.

Z vyššie uvedených bezpečnostných cieľov je zrejmé, že cieľom je ochrana dôvernosti, integrity a dostupnosti údajov počas celého životného cyklu produktu IKT, služby IKT alebo procesu IKT.

4.3.5 Úrovne záruky

Akt o kybernetickej bezpečnosti zavádza **tri úrovne záruky**[280] na bezpečnosť produktu IKT, služby IKT a procesu IKT. Konkrétne ide o úroveň záruky **základná, pokročilá a vysoká**. Úroveň záruky odpovedá úrovni rizika spojeného s plánovaným využívaním daného produktu IKT, služby IKT alebo procesu IKT z hľadiska pravdepodobnosti a vplyvu incidentu.[281]

Konkrétna úroveň záruky je základ pre presvedčenie, že produkt IKT, služba IKT alebo proces IKT spĺňa bezpečnostné požiadavky konkrétneho európskeho systému certifikácie kybernetickej bezpečnosti. Každý európsky certifikát kybernetickej bezpečnosti bude uvádzať jednu z troch úrovní záruky.

Základnou úrovňou záruky boli produkty IKT, služby IKT a procesy IKT hodnotené na úrovni určenej na minimalizovanie známych základných rizík incidentov a kybernetických útokov.[282] Inými slovami, produkty IKT, služby IKT a procesy IKT sú schopné odolať základným incidentom a útokom. Hodnotenie zahŕňa aspoň preskúmanie technickej dokumentácie k produktu IKT, službe IKT alebo procesu IKT orgánom posudzovania zhody.[283]

V prípade **pokročilej úrovne záruky** boli produkty IKT, služby IKT a procesy IKT hodnotené na úrovni určenej na minimalizovanie známych kybernetickobezpečnostných rizík a rizík incidentov a kybernetických útokov, ktoré vykonávajú subjekty s obmedzenými zručnosťami a zdrojmi. V rámci hodnotenia sa vykonáva test verejne známych zraniteľností a skúška na preukázanie, že produkty IKT, procesy IKT alebo služby IKT správne plnia potrebné bezpečnostné funkcie.[284]

[280] V slovenskej verzii aktu o kybernetickej bezpečnosti je použitý pojem stupeň dôveryhodnosti. V tomto prípade ide o nesprávny preklad pojmu *assurance level,* ktorý by mal byť preložený ako úroveň záruky.
[281] Čl. 52 aktu o kybernetickej bezpečnosti.
[282] Čl. 52 ods. 5 aktu o kybernetickej bezpečnosti.
[283] Recitál 88 a čl. 52 ods. 5 aktu o kybernetickej bezpečnosti.
[284] Čl. 52 ods. 6 aktu o kybernetickej bezpečnosti.

V prípade **vysokej úrovne záruky** boli pre produkty IKT, služby IKT a procesy IKT, pre ktoré bol vydaný certifikát na tejto úrovni, vykonané hodnotenia na úrovni určenej na minimalizovanie rizika najpokročilejších kybernetických útokov, ktoré vykonávajú subjekty so značnými zručnosťami a zdrojmi. V rámci hodnotenia sa vykonáva test verejne známych zraniteľností, skúška na preukázanie, že produkty IKT, služby IKT alebo procesy IKT správne plnia najpokročilejšie potrebné bezpečnostné funkcie. Taktiež sa vykonáva posúdenie ich odolnosti proti zručným útočníkom prostredníctvom skúšky prieniku.[285]

Akt o kybernetickej bezpečnosti umožňuje za určitých podmienok vykonať aj **vlastné posúdenie zhody**, čo znamená, že sa posudzovanie zhody vykoná na výhradnú zodpovednosť výrobcu alebo poskytovateľa produktov IKT, služieb IKT alebo procesov IKT. V takýchto prípadoch by výrobca alebo poskytovateľ produktov IKT, služieb IKT alebo procesov IKT vykonal všetky kontroly sám s cieľom zabezpečiť zhodu produktov IKT, služieb IKT alebo procesov IKT s európskym systémom certifikácie kybernetickej bezpečnosti. Takéto posúdenie by sa malo aplikovať len v prípade menej zložitých produktov IKT, služieb IKT a procesov IKT, ktoré predstavujú nízke riziko z hľadiska verejného záujmu. Vlastné posúdenie zhody malo byť dovolené len pre produkty IKT, služby IKT alebo procesy IKT, ktoré zodpovedajú úrovni záruky základná.[286]

Orgánmi posudzovania zhody môžu byť verejné aj súkromné subjekty. Avšak v riadne odôvodnených prípadoch sa môže v európskom systéme certifikácie kybernetickej bezpečnosti stanoviť, že európske certifikáty kybernetickej bezpečnosti podľa daného systému má vydávať len verejný subjekt. Takýmto príkladom je situácia, kedy európsky systém certifikácie kybernetickej bezpečnosti vyžaduje úroveň záruky vysoká.[287]

4.4 Kybernetická odolnosť produktov v práve EÚ (RED smernica a nariadenie CRA)

Európska regulácia kybernetickej bezpečnosti sa v posledných rokoch posúva od „čisto" prevádzkových povinností (smernica NIS2) aj k bezpečnosti samotných produktov uvádzaných na trh. Rozlišujeme a) požiadavky na rádiové zariadenia podľa smernice RED (vrátane delegovaného nariadenia k článku 3 ods. 3 smernice), ktorá zavádza kybernetickú

[285] Čl. 52 ods. 7 aktu o kybernetickej bezpečnosti.
[286] Recitál 79 a čl. 53 aktu o kybernetickej bezpečnosti.
[287] Čl. 56 ods. 5 a 6 aktu o kybernetickej bezpečnosti.

bezpečnosť pre bezdrôtovo pripojené produkty od 1. augusta 2025, a b) novú, horizontálnu reguláciu prostredníctvom Nariadenia Európskeho parlamentu a Rady (EÚ) 2024/2847 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami (akt o kybernetickej odolnosti) (Cyber Resilience Act - CRA), ktorý postupne preberá úlohu jednotného produktového rámca pre hardvér aj softvér.

RED a CRA majú spoločné to, že oba právne predpisy vyžadujú označenie CE k preukázaniu zhody výrobku s predpismi EÚ. Označenie CE na výrobku deklaruje, že výrobca splnil všetky relevantné požiadavky. Ak sa na produkt vzťahuje RED alebo neskôr CRA, výrobca musí zabezpečiť zhodu, aby mohol legálne umiestniť značku CE.

4.4.1 Smernica o rádiových zariadeniach (RED)

Smernica Európskeho parlamentu a Rady 2014/53/EÚ o harmonizácii právnych predpisov členských štátov týkajúcich sa sprístupňovania rádiových zariadení na trhu (Radio Equipment Directive - RED) sa vzťahuje na široké spektrum bezdrôtovo pripojených produktov (mobilné telefóny, tablety, IoT, nositeľné zariadenia, prepojené priemyselné zariadenia a pod.). Delegované nariadenie Komisie (EÚ) 2022/30 rozširuje smernicu RED o požiadavky kybernetickej bezpečnosti cez článok 3 ods. 3 písm. d) až f). Zariadenia nemajú poškodzovať sieť ani zneužívať jej zdroje, majú chrániť údaje a súkromie a majú obsahovať prvky prevencie podvodov (napr. ochranu proti manipulácii či klonovaniu).

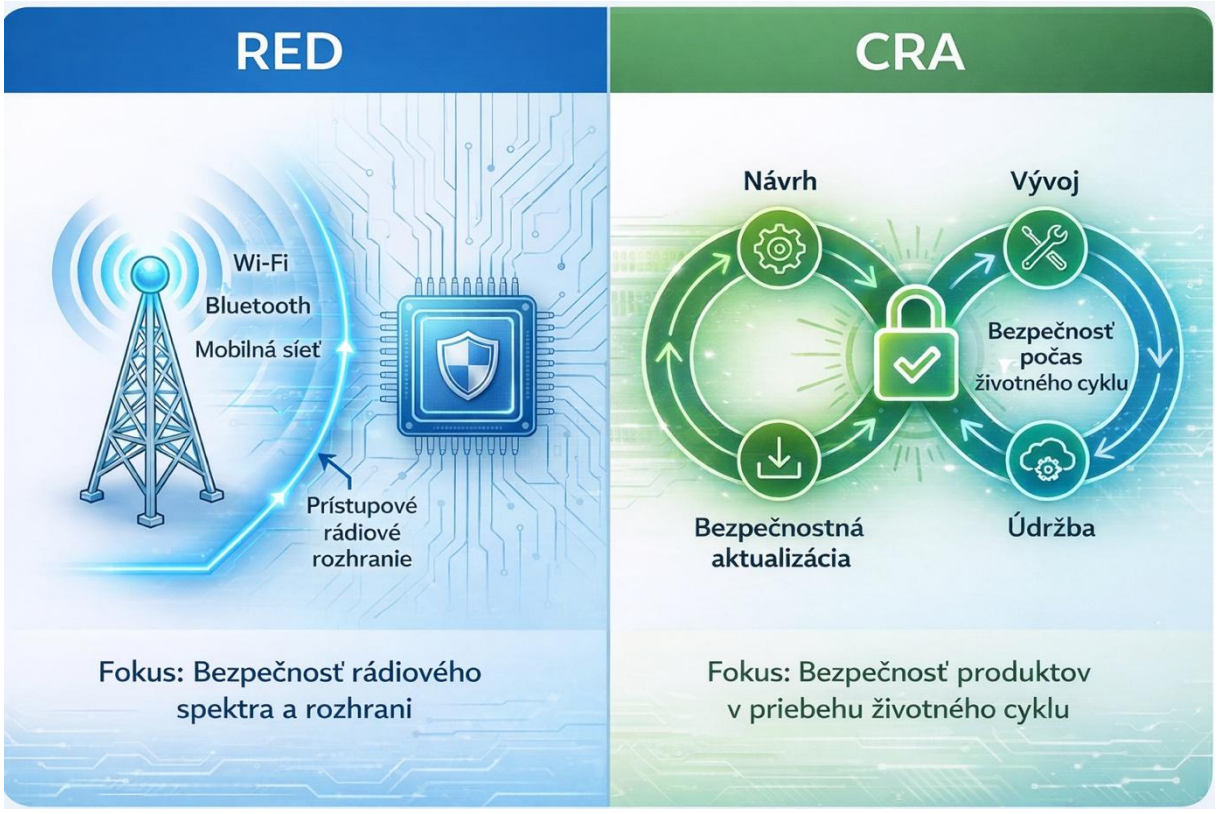
S praktickým dopadom RED úzko súvisí zavedenie harmonizovaných noriem EN 18031, ktoré predstavujú prvé harmonizované technické normy kybernetickej bezpečnosti pre produkty (v tomto prípade rádiové zariadenia). EÚ prijala prvé harmonizované normy kybernetickej bezpečnosti produktov pre RED (EN 18031) cez vykonávacie rozhodnutie Komisie (EÚ) 2025/138. Ide o tri časti:

- EN 18031-1:2024 (rádiové zariadenia pripojené na internet),
- EN 18031-2:2024 (zariadenia spracúvajúce údaje – vrátane kategórií ako starostlivosť o deti, hračky, nositeľné zariadenia),
- EN 18031-3:2024 (zariadenia spracúvajúce virtuálne peniaze/peňažnú hodnotu).

Norma obsahuje 33 požiadaviek rozdelených do 11 skupín (napr. riadenie prístupu, autentifikácia, bezpečné úložisko, bezpečná komunikácia, odolnosť, monitorovanie siete, riadenie prevádzky, dôvernosť kryptografických kľúčov, kryptografia).

Zároveň je dôležité, že podľa vykonávacieho rozhodnutia Komisie (EÚ) 2025/138 nie všetky časti textu EN 18031 vytvárajú predpoklad zhody. Časti označené ako „odôvodnenie" a „usmernenie" (rationale a guidance) sa za takýto základ nepovažujú. Pri ustanoveniach o predvolených heslách sa výslovne uvádza, že výrobca *nemá umožniť* používateľovi režim „bez hesla".

V právnom poriadku Slovenskej republiky je smernica RED transponovaní najmä nariadením vlády SR č. 193/2016 Z. z. o sprístupňovaní rádiových zariadení na trhu, ktoré predstavuje základný vnútroštátny predpis pre uvádzanie rádiových zariadení na trh. Dohľad nad dodržiavaním týchto požiadaviek na vnútornom trhu vykonáva Slovenská obchodná inšpekcia ako všeobecný orgán trhového dozoru, medzi predpismi upravujúcimi jej pôsobnosť je výslovne uvedené aj nariadenie vlády SR č. 193/2016 Z. z.



Obrázok č. 8: Porovnanie smernice RED a nariadenia CRA.[288]

[288] Vygenerované nástrojom UI (ChatGPT).

4.4.2 CRA: Produkty s digitálnymi prvkami

Z hľadiska načasovania je dôležitý vzťah RED a CRA. Delegované nariadenie Komisie (EÚ) 2022/30, ktorým sa dopĺňa smernica RED, pokiaľ ide o uplatňovanie základných požiadaviek kybernetickej bezpečnosti rádiových zariadení uvedených v článku 3 ods. 3 písm. d), e) a f) uvedenej smernice, pokrýva produkty uvádzané na trh od 1. augusta 2025 do 10. decembra 2027. Delegované nariadenie má podľa legislatívneho návrhu[289] Komisie zaniknúť k 11. decembru 2027, nakoľko CRA sa v celom rozsahu začne uplatňovať práve od 11. decembra 2027.

CRA sa však v istých prípadoch vzťahuje na produkty uvedené na trh pred 11. decembrom 2027, a to ak tieto produkty budú po tomto dátume podstatne upravené. Ďalšou výnimkou je povinnosť výrobcov produktov oznamovať aktívne zneužívané zraniteľnosti a závažné incidenty, ktoré majú vplyv na bezpečnosť produktu s digitálnymi prvkami, pre všetky produkty s digitálnymi prvkami, ktoré patria do rozsahu pôsobnosti CRA, vrátane produktov, ktoré boli uvedené na trh pred 11. decembrom 2027 (článok 69(3) CRA).

CRA je priamo aplikovateľné nariadenie, ktoré zavádza horizontálne pravidlá kybernetickej bezpečnosti pre produkty s digitálnymi prvkami (alebo len„ produkty"), ktoré sú sprístupnené na trhu EÚ. Národný bezpečnostný úrad plní úlohy orgánu dohľadu nad trhom pre produkt s digitálnymi prvkami v Slovenskej republike.

Pojem sprístupnenia na trhu je definovaný v článku 3 ods. 22 CRA ako „dodanie produktu s digitálnymi prvkami na distribúciu alebo použitie na trhu Únie v rámci obchodnej činnosti, či už za úhradu alebo bezplatne". V súlade s článkom 3 ods. 21 CRA sa produkt uvádza na trh EÚ pri jeho prvom sprístupnení. Aktuálne vydanie „Modrej príručky o implementácii pravidiel EÚ o produktoch" (ďalej len „Modrá príručka")[290] poskytuje usmernenia uľahčujúce pochopenie pravidiel EÚ o produktoch, ktoré sú v súlade s novým legislatívnym rámcom, ako je napríklad CRA. Pokiaľ ide o „sprístupnenie", koncepcia uvedenia na trh sa vzťahuje na každý jednotlivý výrobok, nie na typ výrobku, a na to, či bol vyrobený ako samostatná jednotka alebo v sérii. Preto sa v prípade každého jednotlivého výrobku môže uvedenie na trh Únie

[289] Návrh nariadenia Komisie o zrušení delegovaného nariadenia RED 2022/30 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=PI_COM%3AC%282026%29778&qid=1771489801670.

[290] Oznámenie Komisie Modrá príručka na vykonávanie právnych predpisov EÚ týkajúcich sa výrobkov 2022 (2022/C 247/01) https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A52022XC0629%2804%29&qid=1658331887710.

uskutočniť len raz v celej EÚ a neuskutočňuje sa v každom členskom štáte jednotlivo. (oddiel 2.3).

V prípade tradičnejších výrobkov, ako je hardvér vo forme strojov alebo rádiových zariadení, je pojem „uvedenie na trh" dobre zavedený a Modrá príručka poskytuje ďalšie usmernenia na objasnenie, kedy sa takéto výrobky považujú za uvedené na trh.

Na rozdiel od hmotných produktov, softvér dodávaný digitálnymi prostriedkami nepodlieha fyzickej výrobe ani obmedzeniam zásob: každé sprístupnenie softvéru na stiahnutie alebo vzdialený prístup vedie k vytvoreniu novej identickej kópie pre používateľa. Pokiaľ táto verzia softvéru nie je upravená spôsobom, ktorý by ovplyvnil súlad s CRA, uvedenie na trh sa považuje za uskutočnené v momente prvej ponuky na distribúciu alebo použitie. Možnosť následného stiahnutia alebo vzdialeného prístupu k tejto verzii softvérového produktu sa preto považuje za prípad, kedy je tento softvérový produkt sprístupnený.

Článok 3 ods. 1 CRA definuje produkt s digitálnymi prvkami ako „softvérový alebo hardvérový produkt a jeho riešenia spracovania údajov na diaľku vrátane softvérových alebo hardvérových komponentov, ktoré sa uvádzajú na trh samostatne". Takéto produkty patria do rozsahu pôsobnosti CRA, ak ich zamýšľaný účel alebo rozumne predvídateľné použitie zahŕňa priame alebo nepriame logické alebo fyzické dátové pripojenie k zariadeniu alebo sieti.

CRA sa preto môže vzťahovať na samostatný softvér, ako napríklad (i) aplikácie a počítačové programy; (ii) hardvér so zabudovaným softvérom (napr. zariadenia internetu vecí); (iii) samostatný hardvér (napr. integrované obvody, základné dosky); a (iv) akúkoľvek kombináciu hardvéru a softvéru dodávaného samostatne, ale určeného na spoločné fungovanie.

To, či softvér tvorí súčasť produktu, by sa nemalo určovať podľa toho, ako alebo kedy je tento softvér dodaný používateľovi, ale podľa toho, či je softvér vzhľadom na zamýšľaný účel produktu a rozumne predvídateľné použitie nevyhnutný na to, aby produkt plnil svoje zamýšľané funkcie. Ak je hardvérové zariadenie navrhnuté tak, aby fungovalo spolu so špecifickým softvérom s cieľom vykonávať svoje funkcie, hardvér a tento softvér spolu tvoria produkt uvedený na trh. Softvér, ktorý je potrebný na prevádzkovanie, konfiguráciu, ovládanie alebo zmysluplné používanie zariadenia, je preto súčasťou produktu, aj keď je

získaný prostredníctvom samostatného kanála (napr. obchodu s aplikáciami, odkazu na stiahnutie alebo iného digitálneho kanála po uvedení hardvéru na trh).

Na druhej strane, ak výrobca poskytuje svojim zákazníkom počítačový kód ako súčasť svojej obchodnej činnosti, tento kód sa považuje za uvedený na trh, bez ohľadu na to, či ide o strojový alebo zdrojový kód.

Produkt tak môže mať mnoho foriem, napríklad:

a) Samostatný softvér, ktorý sa dá stiahnuť a nainštalovať do zariadenia, napr. mobilná aplikácia, ktorú sa dá stiahnuť prostredníctvom obchodu s aplikáciami, alebo program, ktorý sa dá stiahnuť prostredníctvom webovej stránky;
b) Softvér určený na integráciu do elektronického informačného systému, keď sa uvádza na trh samostatne, napr. firmvér alebo softvér určený na vloženie do hardvérových zariadení;
c) Softvér, ktorý sa uvádza na trh spolu s hardvérovým produktom, či už je predinštalovaný na hardvéri alebo nie, napr. ovládače, ktoré sú potrebné na správne fungovanie tlačiarne, operačný systém v notebooku a pod.;
d) Rôzne typy hardvéru, ako napríklad základné komponenty (napr. integrované obvody, základné dosky; senzory); spotrebné zariadenia (napr. smartfóny, notebooky, inteligentné chladničky); zložité zariadenia (napr. priemyselné zariadenia IoT, stroje).

Produkt s digitálnymi prvkami zahŕňa aj svoje riešenia pre diaľkové spracovanie údajov. Ako je uvedené v recitály 12 CRA, webové stránky, ktoré nepodporujú funkčnosť produktu s digitálnymi prvkami, samy osebe nie sú produktmi s digitálnymi prvkami. Webové stránky, ktoré podporujú funkčnosť produktu s digitálnymi prvkami, môžu spadať do rozsahu pôsobnosti CRA, pokiaľ spĺňajú definíciu diaľkového spracovania údajov (článok 3(2) CRA).

Podobne služby, ako napríklad samostatný softvér ako služba (SaaS) alebo iné cloudové riešenia navrhnuté a vyvinuté mimo zodpovednosti výrobcu produktu s digitálnymi prvkami, samy osebe nie sú produktmi s digitálnymi prvkami . Na druhej strane, ak takéto služby spĺňajú definíciu diaľkového spracovania údajov, spadajú do rozsahu pôsobnosti CRA.

CRA výslovne vylučuje zo svojej pôsobnosti produkty s digitálnymi prvkami:

- na ktoré sa vzťahuje nariadenie (EÚ) 2017/745 o zdravotníckych pomôckach a nariadenie (EÚ) 2017/746 o diagnostických zdravotníckych pomôckach in vitro;
- na ktoré sa vzťahuje nariadenie (EÚ) 2019/2144 o požiadavkách na typové schválenie motorových vozidiel a ich prípojných vozidiel a systémov, komponentov a

samostatných technických jednotiek určených pre takéto vozidlá, pokiaľ ide o ich všeobecnú bezpečnosť a ochranu cestujúcich vo vozidle a zraniteľných účastníkov cestnej premávky;

- certifikované v súlade s nariadením (EÚ) 2018/1139 o spoločných pravidlách v oblasti civilného letectva a o zriadení Agentúry Európskej únie pre bezpečnosť letectva;
- zariadenia, ktoré patria do rozsahu pôsobnosti smernice 2014/90/EÚ o námornom vybavení lodí.

Delegované nariadenie (EÚ) 2025/1535 tiež vylučuje z uplatňovania CRA produkty s digitálnymi prvkami, ktoré patria do rozsahu pôsobnosti nariadenia (EÚ) č. 168/2013 o schvaľovaní a dohľade nad trhom dvoj- alebo trojkolesových vozidiel a štvorkoliek, s výnimkou vozidiel kategórie L1e určených na šliapanie.

4.4.3 Kategórie produktov

CRA kategorizuje výrobky podľa rizika na určenie zhody, pričom väčšina (približne 90 %) spadá do základnej kategórie. Vo všeobecnosti si výrobca zachováva flexibilitu, pokiaľ ide o výber postupu (sebahodnotenie alebo posúdenie treťou stranou), prostredníctvom ktorého preukazuje zhodu s CRA, s výnimkou niektorých kategórií výrobkov (dôležité a kritické výrobky uvedené v prílohe III a prílohe IV CRA), pre ktoré sa vyžaduje prísnejšie posudzovanie zhody:

a) **Základné (default)** produkty (napr. pamäťové čipy, mobilné aplikácie, inteligentné reproduktory, počítačové hry). Sebahodnotenie je povolené bez ohľadu na technickú špecifikáciu, ktorú výrobca použil na preukázanie zhody.

b) **Dôležité** produkty (napr. operačné systémy, antivírus, smerovače, firewally). V niektorých prípadoch je účasť notifikovaného orgánu povinná, najmä ak výrobca neuplatnil harmonizované normy na podporu CRA. Dôležité produkty sa delia do dvoch tried (Trieda I a Trieda II)

c) **Kritické** produkty (napr. inteligentné karty, bezpečnostné prvky, inteligentné meracie brány). Použitie notifikovaného orgánu je v každom prípade povinné.

V súlade s článkami 7 ods. 1 a 8 ods. 1 CRA by mal výrobca preskúmať základnú funkciu svojho produktu s digitálnymi prvkami, aby určil, či je daný výrobok dôležitým alebo kritickým výrobkom s digitálnymi prvkami, a preto podlieha zodpovedajúcim postupom posudzovania zhody. Technické popisy kategórií dôležitých a kritických produktov s digitálnymi prvkami sú stanovené vo vykonávacom nariadení Komisie (EÚ) 2025/2392 o technickom opise kategórií dôležitých a kritických produktov s digitálnymi prvkami.

4.4.4 Hospodárske subjekty

CRA buduje povinnosti naprieč dodávateľským reťazcom a pracuje s rolami výrobcu, dovozcu a distribútora.

4.4.4.1 Výrobca

Výrobcom je fyzická alebo právnická osoba, ktorá vyvíja alebo vyrába produkty s digitálnymi prvkami alebo si dáva navrhnúť, vyvinúť alebo vyrobiť produkty s digitálnymi prvkami a predáva ich pod svojím menom alebo svojou ochrannou známkou, či už za odplatu, speňaženie alebo bezodplatne. Výrobcovia pri uvádzaní produktu s digitálnymi prvkami na trh majú povinnosť zaistiť, aby bol navrhnutý, vyvinutý a vyrobený v súlade so základnými požiadavkami kybernetickej bezpečnosti stanovenými v časti I prílohy I CRA. Zároveň aj počas obdobia podpory výrobcovia zaistia, aby sa zraniteľnosti tohto produktu vrátane jeho komponentov riešili účinne a v súlade so základnými požiadavkami kybernetickej bezpečnosti stanovenými v časti II prílohy I CRA. Výrobcovia pred uvedením produktu s digitálnymi prvkami na trh vypracujú technickú dokumentáciu uvedenú v článku 31. Vykonajú alebo dajú vykonať zvolené postupy posudzovania zhody uvedené v článku 32.

Keď bol súlad produktu s digitálnymi prvkami so základnými požiadavkami kybernetickej bezpečnosti stanovenými v časti I prílohy I a procesov zavedených výrobcom so základnými požiadavkami kybernetickej bezpečnosti stanovenými v časti II prílohy I preukázaný týmto postupom posudzovania zhody, výrobcovia vypracujú EÚ vyhlásenie o zhode v súlade s článkom 28 a umiestnia označenie CE v súlade s článkom 30 CRA. Výrobcovia uchovávajú technickú dokumentáciu a EÚ vyhlásenie o zhode k dispozícii pre orgány pre dohľad nad trhom aspoň 10 rokov od uvedenia produktu s digitálnymi prvkami na trh alebo počas obdobia podpory, podľa toho, čo trvá dlhšie.

Výrobcovia zabezpečia, aby ich produkty s digitálnymi prvkami boli označené číslom typu, šarže alebo série alebo iným prvkom umožňujúcim ich identifikáciu, alebo ak to nie je možné, aby sa tieto informácie uvádzali na obale alebo v sprievodnej dokumentácii produktu s digitálnymi prvkami. Na produkte s digitálnymi prvkami, na jeho obale alebo v sprievodnej dokumentácii uvedú výrobcovia svoje meno, zapísané obchodné meno alebo zapísanú ochrannú známku, poštovú a e-mailovú adresu alebo iné digitálne kontaktné údaje, a prípadne webové sídlo, na ktorých sa s nimi možno skontaktovať. Tieto informácie sa uvedú aj v informáciách a návode pre používateľa stanovených v prílohe II CRA. Kontaktné údaje sú v jazyku ľahko zrozumiteľnom pre používateľov a orgány dohľadu nad trhom.

Výrobcovia sú povinný určiť jednotné kontaktné miesto, aby používatelia mohli s nimi priamo a rýchlo komunikovať, a to aj s cieľom uľahčiť nahlasovanie zraniteľností produktu s digitálnymi prvkami.

Výrobcovia zabezpečia, aby boli k produktom s digitálnymi prvkami priložené informácie a návod pre používateľa uvedené v prílohe II, a to v tlačenej alebo elektronickej podobe. Uvedené informácie a pokyny sa poskytujú v jazyku ľahko zrozumiteľnom pre používateľa a orgány dohľadu nad trhom. Musia byť jasné, zrozumiteľné, pochopiteľné a čitateľné. Musia umožniť bezpečnú inštaláciu, prevádzku a používanie produktov s digitálnymi prvkami. Pre potreby používateľov a orgánov dohľadu nad trhom uchovávajú výrobcovia informácie a návod pre používateľa uvedené v prílohe II aspoň 10 rokov od uvedenia produktu s digitálnymi prvkami na trh alebo počas obdobia podpory, podľa toho, čo trvá dlhšie.

Výrobcovia zabezpečia, aby bol v čase nákupu jasne a zrozumiteľne uvedený dátum skončenia obdobia podpory uvedeného v odseku 8, a to aspoň mesiac a rok, a to ľahko dostupným spôsobom a prípadne na produkte s digitálnymi prvkami, jeho obale alebo digitálnymi prostriedkami.

Výrobcovia spolu s produktom s digitálnymi prvkami sú povinní poskytnúť buď kópiu EÚ vyhlásenia o zhode alebo zjednodušené EÚ vyhlásenie o zhode. Ak poskytnú zjednodušené EÚ vyhlásenie o zhode, musí obsahovať presnú internetovú adresu, na ktorej je sprístupnené úplné znenie EÚ vyhlásenia o zhode.

Ak majú vedomosť alebo dôvod domnievať sa, že produkt s digitálnymi prvkami alebo nimi zavedené postupy nie sú v súlade so základnými požiadavkami kybernetickej bezpečnosti stanovenými v prílohe I, sú výrobcovia povinní bezodkladne prijať podľa

vhodnosti nápravné opatrenia potrebné na uvedenie tohto produktu s digitálnymi prvkami alebo postupov výrobcu do súladu s príslušnými požiadavkami alebo na stiahnutie produktu z trhu alebo od používateľa.

Výrobca, ktorý ukončí svoju činnosť a v dôsledku toho nie je schopný dosiahnuť súlad s týmto nariadením, ešte pred ukončením činnosti informuje príslušné orgány dohľadu nad trhom a všetkými dostupnými prostriedkami a v maximálnej možnej miere aj používateľov relevantných produktov s digitálnymi prvkami uvedených na trh o nastávajúcom ukončení činnosti.

4.4.4.2 Dovozca

Dovozcom sa rozumie fyzická alebo právnická osoba usadená v Únii, ktorá uvádza na trh produkt s digitálnymi prvkami označený menom alebo ochrannou známkou fyzickej alebo právnickej osoby usadenej mimo Únie.

Dovozcovia môžu uvádzať na trh len produkty s digitálnymi prvkami, ktoré spĺňajú základné požiadavky kybernetickej bezpečnosti stanovené v časti I prílohy I, a len ak sú postupy zavedené výrobcom v súlade so základnými požiadavkami kybernetickej bezpečnosti stanovenými v časti II prílohy I. Pred uvedením produktu s digitálnymi prvkami na trh sa dovozcovia uistia, že:

a) výrobca vykonal náležité postupy posudzovania zhody;

b) výrobca vypracoval technickú dokumentáciu;

c) produkt s digitálnymi prvkami má označenie CE a je k nemu priložené EÚ vyhlásenie o zhode, a informácie a pokyny pre používateľa stanovené v prílohe II, v jazyku zrozumiteľnom pre používateľov a orgány dohľadu nad trhom;

d) výrobca splnil požiadavky stanovené v článku 13 ods. 15, 16 a 19 CRA. Na účely tohto odseku musia byť dovozcovia schopní poskytnúť potrebné doklady.

Ak sa dovozca domnieva alebo má dôvod sa domnievať, že produkt s digitálnymi prvkami alebo postupy zavedené výrobcom nie sú v zhode s CRA, dovozca neuvedie produkt na trh, kým sa v prípade tohto produktu alebo postupov zavedených výrobcom nedosiahne zhoda s CRA. Ak produkt s digitálnymi prvkami predstavuje navyše významné kybernetickobezpečnostné riziko, dovozca o tom informuje výrobcu a orgány dohľadu nad trhom. Ak má dovozca dôvod domnievať sa, že produkt s digitálnymi prvkami môže

predstavovať významné kybernetickobezpečnostné riziko vzhľadom na netechnické rizikové faktory, informuje o tom orgány dohľadu nad trhom.

Ak sa dovozca produktu s digitálnymi prvkami dozvie, že výrobca tohto produktu ukončil činnosť a v dôsledku toho nie je schopný plniť povinnosti stanovené v tomto nariadení, dovozca informuje o tejto situácii príslušné orgány dohľadu nad trhom a všetkými dostupnými prostriedkami a v maximálnej možnej miere aj používateľov produktov s digitálnymi prvkami uvedených na trh.

4.4.4.3 Distribútor

Distribútorom je fyzická alebo právnická osoba v dodávateľskom reťazci okrem výrobcu alebo dovozcu, ktorá na trhu Únie sprístupňuje produkt s digitálnymi prvkami bez toho, aby ovplyvňovala jeho vlastnosti. Pri sprístupňovaní produktu s digitálnymi prvkami na trhu konajú distribútori vo vzťahu k požiadavkám stanoveným v tomto nariadení s náležitou starostlivosťou.

Pred sprístupnením produktu s digitálnymi prvkami na trhu distribútori overia, či:

a) je na produkte s digitálnymi prvkami umiestnené označenie CE;

b) výrobca a dovozca si splnili povinnosti stanovené v článku 13 ods. 15, 16, 18, 19 a 20 a článku 19 ods. 4 a distribútorovi poskytli všetky potrebné dokumenty.

Ak sa distribútor na základe svojich informácií domnieva alebo má dôvod sa domnievať, že produkt s digitálnymi prvkami alebo postupy zavedené výrobcom nie sú v zhode so základnými požiadavkami kybernetickej bezpečnosti stanovenými v prílohe I, nesmie produkt s digitálnymi prvkami sprístupniť na trhu, kým sa tento produkt alebo postupy zavedené výrobcom neuvedú do zhody s týmto nariadením. Ak produkt s digitálnymi prvkami predstavuje navyše významné kybernetickobezpečnostné riziko, distribútor o tom bezodkladne informuje výrobcu a orgány dohľadu nad trhom.

4.4.4.4 Kvázi výrobca: keď sa dovozca, distribútor alebo integrátor stáva výrobcom

CRA vychádza z toho, že primárnu zodpovednosť za kybernetickú bezpečnosť produktu s digitálnymi prvkami nesie výrobca. Zároveň však výslovne rieši situácie, keď sa povinnosti výrobcu prenášajú aj na iné subjekty v dodávateľskom reťazci alebo na osoby, ktoré produkt po uvedení na trh menia. CRA používa koncept tzv. „kvázi výrobcu", t.j. určitý subjekt nemusí byť „pôvodným" výrobcom, ale právne sa za výrobcu považuje a preberá jeho

povinnosti, ak svojím konaním reálne prevezme kontrolu nad produktom alebo jeho bezpečnostnými vlastnosťami.

Prvým typickým prípadom je dovozca alebo distribútor, ktorý uvedie produkt na trh **pod svojím menom alebo ochrannou známkou**. V takom prípade sa naňho na účely CRA hľadí ako na výrobcu a vzťahujú sa naňho najmä povinnosti podľa článkov 13 a 14, teda povinnosti týkajúce sa plnenia základných požiadaviek kybernetickej bezpečnosti a režimu oznamovania aktívne zneužívaných zraniteľností a závažných incidentov. Druhým prípadom je situácia, keď dovozca alebo distribútor vykoná **podstatnú úpravu** produktu, ktorý už bol uvedený na trh. Aj vtedy sa právne „preklopí" do pozície výrobcu, pretože mení vlastnosti produktu rozhodujúce pre jeho bezpečnosť a súlad.

CRA ide ešte ďalej a zavádza aj všeobecné pravidlo pre iné osoby mimo klasického reťazca výrobca–dovozca–distribútor. Ak akákoľvek fyzická alebo právnická osoba vykoná podstatnú úpravu produktu s digitálnymi prvkami a následne ho **sprístupní na trhu**, považuje sa za výrobcu. Zodpovednosť tejto osoby sa pritom viaže aspoň na tú časť produktu, ktorá je podstatnou úpravou dotknutá; ak však úprava ovplyvňuje kybernetickú bezpečnosť produktu ako celku, povinnosti sa môžu vzťahovať aj na celý produkt. V praxi to cieli najmä na integrátorov, systémových dodávateľov, distribútorov alebo subjekty, ktoré na pôvodný produkt „nadstavujú" nové funkcie a tým zvyšujú riziká.

Za **podstatnú úpravu** sa považuje zmena produktu po jeho uvedení na trh, ktorá buď (a) ovplyvňuje jeho súlad so základnými požiadavkami kybernetickej bezpečnosti podľa prílohy I, alebo (b) vedie k zmene zamýšľaného účelu, pre ktorý bol produkt posudzovaný. Z hľadiska kybernetickej bezpečnosti je dôležité, že podstatnou úpravou nemusia byť len „fyzické zásahy" do hardvéru. V praxi sem môžu patriť aj zásahy digitálnej povahy, napríklad doplnenie nových modulov, rozhraní, rozšírenie konektivity alebo významné úpravy konfigurácie a softvéru, ktoré rozširujú plochu útoku alebo menia bezpečnostné predpoklady produktu. Takéto zmeny môžu zásadne ovplyvniť, či produkt naďalej spĺňa požiadavky CRA, a preto CRA pri nich priraďuje zodpovednosť tomu, kto zmenu vykonal a produkt ďalej sprístupňuje.

4.4.5 Podpora a dokumentácia

CRA venuje osobitnú pozornosť obdobiu podpory produktu, vysledovateľnosti v dodávateľskom reťazci, ako aj informačným a dokumentačným povinnostiam výrobcov a

ďalších hospodárskych subjektov. Obdobie podpory má trvať najmenej päť rokov. Ak sa však predpokladá, že produkt s digitálnymi prvkami sa bude používať kratšie ako päť rokov, obdobie podpory musí zodpovedať očakávanému obdobiu jeho používania. Výrobcovia sú zároveň povinní uviesť v technickej dokumentácii podľa prílohy VII informácie, ktoré zohľadnili pri určovaní obdobia podpory produktu. Európska komisia môže navyše prostredníctvom delegovaných aktov určiť minimálne obdobie podpory pre konkrétne kategórie produktov, ak údaje z dohľadu nad trhom preukážu, že poskytované obdobie podpory je neprimerané.

Výrobca musí zároveň zabezpečiť, aby každá bezpečnostná aktualizácia, ktorá bola používateľom sprístupnená počas obdobia podpory, zostala po svojom vydaní k dispozícii najmenej desať rokov alebo počas zvyšku obdobia podpory, podľa toho, ktoré obdobie je dlhšie.

CRA upravuje aj povinnosti hospodárskych subjektov vo vzťahu k orgánom dohľadu nad trhom. Každý výrobca, dodávateľ alebo distribútor musí na požiadanie podľa článku 23 CRA poskytnúť meno a adresu každého hospodárskeho subjektu, ktorý mu dodal produkt s digitálnymi prvkami, ako aj meno a adresu každého hospodárskeho subjektu, ktorému produkt s digitálnymi prvkami dodal, ak sú tieto informácie k dispozícii. Hospodárske subjekty musia byť schopné tieto údaje poskytnúť počas desiatich rokov odo dňa, keď im bol produkt dodaný, ako aj počas desiatich rokov odo dňa, keď ho samy dodali ďalej.

Osobitnú skupinu povinností predstavujú informácie a návod pre používateľa podľa prílohy II CRA. Tieto informácie musia zahŕňať identifikáciu výrobcu a jeho kontaktné údaje, vrátane adresy, e-mailu a webového sídla. Ďalej sa vyžaduje určenie kontaktného miesta pre oznamovanie zraniteľností a informácia o politike koordinovaného zverejňovania zraniteľností. Používateľ musí mať k dispozícii názov a typ produktu s digitálnymi prvkami vrátane jeho jedinečnej identifikácie, údaje o plánovanom účele produktu, jeho základných funkciách a bezpečnostných vlastnostiach, ako aj informácie o predvídateľných okolnostiach používania alebo nesprávneho používania, ktoré môžu viesť ku kybernetickým rizikám. Ak je to relevantné, súčasťou týchto informácií má byť aj odkaz na EÚ vyhlásenie o zhode. Ďalej sa vyžaduje informácia o technickej podpore a o dátume ukončenia podpory bezpečnostných aktualizácií. Návod, alebo odkaz naň, má obsahovať informácie o bezpečnom používaní produktu, o vplyve zmien na bezpečnosť údajov, o inštalácii aktualizácií, o bezpečnom vyradení produktu z prevádzky, o možnosti vypnutia automatickej inštalácie aktualizácií a o

požiadavkách relevantných pre integrátorov. Ak výrobca sprístupňuje zoznam komponentov (Software Bill of Materials – SBOM), musí uviesť aj informáciu o tom, kde ho možno nájsť.

Technická dokumentácia podľa prílohy VII CRA má zahŕňať všeobecný opis produktu, teda jeho plánovaný účel, verzie softvéru, ktoré vplývajú na bezpečnosť, obrázky hardvéru, ak sú relevantné, a používateľský návod. Ďalej musí obsahovať opis riešenia, vývoja a výroby, vrátane návrhu a architektúry systému, postupov riešenia zraniteľností, kontaktného miesta pre hlásenia a spôsobu distribúcie aktualizácií, ako aj opis výrobného procesu a jeho validácie. Súčasťou technickej dokumentácie je aj posúdenie kyberneticko-bezpečnostných rizík, informácie týkajúce sa obdobia podpory, zoznam použitých noriem a špecifikácií, správy o skúškach preukazujúce zhodu produktu a procesov riešenia zraniteľností, EÚ vyhlásenie o zhode a prípadne aj zoznam SBOM, ak ho vyžaduje orgán dohľadu nad trhom.

4.4.6 Aktívne zneužívané zraniteľnosti a závažné incidenty

CRA osobitne upravuje aj aktívne zneužívané zraniteľnosti a závažné incidenty. Podľa článku 3 ods. 42 CRA sa za aktívne zneužívanú zraniteľnosť považuje taká zraniteľnosť, o ktorej existuje spoľahlivý dôkaz, že škodlivý subjekt ju zneužil v systéme bez povolenia vlastníka systému, teda že existujú spoľahlivé dôkazy o tom, že bola zneužitá v konkrétnom systéme. Ide teda o situácie, keď výrobca zistí, že bezpečnostné narušenie postihujúce jeho používateľov alebo iné fyzické či právnické osoby vzniklo v dôsledku toho, že škodlivý aktér využil slabinu v niektorom z produktov s digitálnymi prvkami, ktoré výrobca sprístupnil na trhu. Príkladom takýchto zraniteľností môžu byť nedostatky vo funkciách identifikácie a autentifikácie produktu.

Naopak, zraniteľnosti objavené bez škodlivého úmyslu, a to na účely dobromyseľného testovania, skúmania, opravy alebo zverejnenia s cieľom podporiť bezpečnosť alebo ochranu vlastníka systému a jeho používateľov, nepodliehajú povinnému oznamovaniu. Tento prístup výslovne potvrdzuje aj odôvodnenie 68.

Povinnosti oznamovania sa začínajú uplatňovať od 11. septembra 2026. Od tohto dátumu sú výrobcovia povinní dodržiavať článok 14, a najmä povinnosť oznamovať aktívne zneužívané zraniteľnosti a závažné incidenty, ktoré majú vplyv na bezpečnosť produktu, a to pri všetkých produktoch s digitálnymi prvkami patriacich do pôsobnosti CRA, vrátane produktov, ktoré boli uvedené na trh ešte pred 11. decembrom 2027.

Pri produktoch uvedených na trh pred 11. decembrom 2027 však môže nastať situácia, že výrobca nebude schopný takéto zraniteľnosti dôkladne preveriť, napríklad preto, že už neexistujú nástroje na skenovanie alebo spúšťanie starých verzií softvéru, nie je možné znovu vytvoriť prostredie potrebné na zostavenie starého kódu, závislosti už nie sú dostupné alebo nie sú kompatibilné s modernými systémami, prípadne organizáciu opustili pracovníci, ktorí mali znalosť starších kódových základov. V prípade takýchto produktov je výrobca povinný zraniteľnosť alebo incident oznámiť, avšak CRA od neho nevyžaduje, aby splnil aj ďalšie povinnosti, napríklad vo vzťahu k riešeniu zraniteľností.

Povinnosť oznámenia pritom vzniká okamihom, keď sa výrobca o aktívne zneužívanej zraniteľnosti alebo závažnom incidente dozvie po začiatku uplatňovania oznamovacích požiadaviek. Zároveň článok 14 ods. 8 ukladá výrobcovi povinnosť informovať dotknutých používateľov produktu s digitálnymi prvkami, a podľa okolností aj všetkých používateľov, o týchto zraniteľnostiach alebo incidentoch. Ak sa výrobca rozhodne neinformovať používateľov včas, CSIRT, ktoré prijali oznámenie, môžu túto informáciu poskytnúť používateľom samy, ak to považujú za primerané a nevyhnutné na predchádzanie dopadom zraniteľnosti alebo incidentu alebo na ich zmiernenie.

4.4.7 Posudzovanie zhody a harmonizované normy

CRA je vystavané na kombinácii základných požiadaviek a viacerých modulov posudzovania zhody (Príloha VIII). Rozlišuje najmä vnútornú kontrolu výroby podľa modulu A, EÚ skúšku typu v kombinácii so zhodou s typom založenou na internej kontrole výroby podľa modulov B a C, ako aj úplné zabezpečenie kvality podľa modulu H. Výber konkrétneho postupu sa pritom viaže na rizikovosť produktu a na jeho zaradenie do príslušnej kategórie.

Súčasne sa v tomto kontexte spomína aj schéma EUCC ako certifikačný rámec pracujúci s úrovňami záruky, ktorý môže predstavovať jeden z vhodných spôsobov preukazovania zhody, ak bude v ďalších krokoch bližšie určené, za akých podmienok bude s EUCC spojený predpoklad zhody.

Z pohľadu harmonizovaných noriem CRA vychádza z rozlíšenia medzi horizontálnymi a vertikálnymi normami. Horizontálne normy sa týkajú všeobecných oblastí, akými sú prístup založený na riziku, základné požiadavky kybernetickej bezpečnosti a riešenie zraniteľností. Vertikálne normy sú naopak viazané na konkrétne kategórie dôležitých a kritických produktov uvedených v prílohách III a IV.

Na uľahčenie posudzovania zhody so základnými požiadavkami Európska komisia prijala žiadosť o vypracovanie technických noriem adresovanú európskym normalizačným organizáciám CEN, CENELEC a ETSI, ktorou ich požiadala o vypracovanie harmonizovaných noriem pre technické oblasti pokryté CRA.[291] Táto žiadosť okrem iného požaduje vypracovanie horizontálnych harmonizovaných noriem pokrývajúcich základné požiadavky na produkty podľa prílohy I časti I CRA. Cieľom je jednak podporiť vytváranie ďalších, podrobnejších vertikálnych harmonizovaných noriem pre konkrétne produkty alebo typy produktov, a jednak pomôcť výrobcom pri určovaní a zavádzaní bezpečnostných požiadaviek uplatniteľných na ich produkty, a to najmä pri produktoch, ktoré nie sú pokryté existujúcimi alebo pripravovanými vertikálnymi normami.

Zároveň treba zdôrazniť, že používanie harmonizovaných noriem je dobrovoľné. Výrobcovia môžu preukázať zhodu so základnými požiadavkami aj inými technickými prostriedkami, pričom sú povinní tieto prostriedky riadne zdokumentovať vo svojej technickej dokumentácii.

4.4.8 Slobodný softvér a softvér s otvoreným zdrojovým kódom

CRA výslovne upravuje aj slobodný softvér a softvér s otvoreným zdrojovým kódom (Free and Open-Source Software - FOSS) a stanovuje kritériá, podľa ktorých sa posudzuje, kedy možno FOSS považovať za produkt uvádzaný na trh, teda za súčasť obchodnej činnosti. CRA pritom zohľadňuje osobitosti rôznych spôsobov vývoja a zverejňovania FOSS a poskytuje usmernenie na identifikáciu toho, či ide o produkt uvedený na trh v zmysle tohto nariadenia. Ako sa uvádza v recitály18, pri určovaní obchodnej alebo neobchodnej povahy činnosti sa nemá prihliadať len na okolnosti, za ktorých bol produkt s digitálnymi prvkami vyvinutý, ani na spôsob financovania jeho vývoja. Osobitne sa zdôrazňuje, že s cieľom jasne odlíšiť fázu vývoja od fázy dodávania sa poskytovanie produktov s digitálnymi prvkami, ktoré predstavujú FOSS a nie sú ich výrobcami speňažované, nemá považovať za obchodnú činnosť.

[291] COMMISSION IMPLEMENTING DECISION on a standardisation request to the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) Dostupné na: https://ec.europa.eu/transparency/documents-register/detail?ref=C(2025)618&lang=en

Z tohto dôvodu je potrebné objasniť, po prvé, čo sa rozumie pod pojmom FOSS, po druhé, kedy sa takýto softvér považuje za spadajúci pod zodpovednosť fyzickej alebo právnickej osoby, a po tretie, v akých prípadoch distribúcia FOSS predstavuje uvedenie na trh. Ak FOSS nie je uvedený na trh, nachádza sa mimo pôsobnosti CRA, s výnimkou prípadu, keď subjekt, ktorý ho zverejňuje, je právnickou osobou spĺňajúcou definíciu správcu softvéru s otvoreným zdrojovým kódom podľa článku 3 ods. 14 CRA. Správcom softvéru s otvoreným zdrojovým kódom je právnická osoba iná ako výrobca, ktorej účelom alebo cieľom je systematicky a trvalo podporovať vývoj špecifických produktov s digitálnymi prvkami považovaných za slobodný softvér a softvér s otvoreným zdrojovým kódom a určených na obchodné činnosti, a ktorá zabezpečuje životaschopnosť týchto produktov. V takom prípade sa naň vzťahujú iba povinnosti ustanovené v článku 24 CRA.

Podľa článku 3 ods. 48 CRA sa za FOSS považuje softvér, ktorého zdrojový kód je voľne dostupný a ktorý je vytvorený na základe bezplatnej a otvorenej licencie, ktorá udeľuje všetky práva na voľný prístup k nemu, jeho použiteľnosť, modifikovateľnosť a redistribúciu. Z tohto vymedzenia vyplýva, že na účely CRA musí softvér kumulatívne spĺňať dve podmienky. Po prvé, musí byť sprístupnený na základe otvorenej licencie, ktorá priznáva celý súbor práv uvedených v článku 3 ods. 48. Po druhé, jeho zdrojový kód musí byť otvorene zdieľaný.

Požiadavka, aby licencia zabezpečovala, že softvér je voľne prístupný, použiteľný, modifikovateľný a ďalej šíriteľný, zodpovedá tradičnému chápaniu FOSS, podľa ktorého musia používatelia mať možnosť pristupovať k zdrojovému kódu, používať ho bez neprimeraných obmedzení, upravovať ho a ďalej šíriť pôvodné aj upravené verzie. Prístup k zdrojovému kódu je pritom nevyhnutnou podmienkou výkonu ostatných práv, pretože bez neho nie je prakticky možné softvér upravovať ani zmysluplne opätovne používať.

Článok 3 ods. 48 CRA však neodkazuje iba na licenčné podmienky, ale výslovne vyžaduje aj to, aby bol zdrojový kód voľne dostupný. Recitál 18 tento záver ďalej podporuje tým, že uvádza, že FOSS sa vyvíja, udržiava a distribuuje voľne, a to aj prostredníctvom online platforiem. Zdrojový kód musí byť verejne dostupný, a nie iba poskytovaný obmedzenému okruhu osôb alebo za splnenia určitých podmienok. Softvér distribuovaný na základe FOSS licencie, ktorého zdrojový kód je sprístupnený iba platiacim zákazníkom alebo len obmedzenej skupine používateľov, sa preto nepovažuje za FOSS v zmysle článku 3 ods. 48. Na účely CRA sa teda za FOSS považuje len taký softvér, ktorého zdrojový kód je verejne

dostupný a ktorý je licencovaný na základe licencie poskytujúcej celý rozsah práv uvedených v tomto ustanovení.

Dôležité zároveň je, že podľa článku 13 ods. 5 CRA výrobcovia sú povinní uplatniť náležitú starostlivosť pri integrácii komponentov získaných od tretích strán tak, aby tieto komponenty neohrozovali kybernetickú bezpečnosť produktu s digitálnymi prvkami, a to aj pri integrácii komponentov FOSS, ktoré neboli sprístupnené na trhu v priebehu obchodnej činnosti. Ak výrobca produktu integruje komponenty tretích strán, vrátane FOSS, nesie zodpovednosť aj za tieto komponenty.

4.4.9 Zodpovednosť za chybný digitálny produkt

CRA a smernica o zodpovednosti za chybné výrobky (EÚ) 2024/2853, teda smernica o zodpovednosti za výrobky (Product Liability Directive - PLD), sa vzájomne dopĺňajú. PLD pokrýva aj softvér pri posudzovaní objektívnej zodpovednosti výrobcu, pričom pri hodnotení „chybovosti" výrobku sa prihliada aj na požiadavky kybernetickej bezpečnosti. Osobitne sa zdôrazňuje význam bezpečnostných aktualizácií, ako aj zodpovednosť za škody spôsobené súvisiacimi službami alebo absenciou aktualizácií potrebných na zabezpečenie kybernetickej bezpečnosti.

Definícia produktu bola spresnená tak, aby zahŕňala aj softvér vrátane systémov umelej inteligencie. Nová smernica sa preto vzťahuje na všetky typy softvéru vrátane aplikácií a systémov AI. Výrobca výrobku zodpovedá za škody spôsobené vadou svojho výrobku bez ohľadu na zavinenie alebo nedbanlivosť (objektívna zodpovednosť). Výrobca zároveň zodpovedá za chyby, ktoré sa môžu objaviť po aktualizácii alebo modernizácii softvéru vykonanej pod jeho kontrolou. Rovnako nesie zodpovednosť aj za chyby, ktoré sa môžu prejaviť v dôsledku neustáleho učenia sa systému AI, ak tento systém zostáva pod jeho kontrolou. Smernica sa navyše vzťahuje aj na digitálne služby, ktoré sú nevyhnutné pre fungovanie produktu a ktoré boli do produktu začlenené pod kontrolou výrobcu.

Smernica sa vzťahuje aj na ďalšie podstatné prvky. Produkt sa považuje za chybný, ak neposkytuje bezpečnosť, ktorú má osoba právo očakávať alebo ktorá sa vyžaduje podľa práva Európskej únie alebo vnútroštátneho práva. Pri posudzovaní chybnosti sa prihliada najmä na prezentáciu a vlastnosti produktu vrátane jeho označovania, na vplyv akejkoľvek schopnosti produktu neustále sa učiť alebo získavať nové funkcie, ako aj na rozumne predvídateľný vplyv iných výrobkov, pri ktorých sa dá očakávať, že budú používané spolu s daným výrobkom.

Právo na odškodnenie vzniká vtedy, ak chybný výrobok spôsobí smrť alebo ujmu na zdraví, vrátane lekársky uznaného poškodenia duševného zdravia, škodu na majetku alebo zničenie či poškodenie údajov, ktoré sa nepoužívali na profesionálne účely.

Smernica zároveň upravuje aj prístup k dôkazom, keďže stanovuje právo oboch strán požiadať o prístup k dôkazom potrebným na podporu ich nárokov. Pokiaľ ide o zodpovednosť a odškodnenie, každá osoba, ktorá utrpela škodu spôsobenú chybným výrobkom, môže podať žalobu na vnútroštátny súd. Podniky zostávajú zodpovedné za svoje chybné výrobky počas desiatich rokov od uvedenia výrobku na trh. Táto desaťročná lehota sa predlžuje na dvadsaťpäť rokov, ak sa ujma na zdraví prejavuje pomaly, teda ide o latentné poškodenie zdravia. Poškodená osoba má zároveň tri roky na to, aby podala žalobu o odškodnenie na vnútroštátny súd. Členské štáty sú povinné transponovať smernicu najneskôr do 9. decembra 2026.

4.5 Kybernetická bezpečnosť systémov a modelov AI

Umelá inteligencia (AI) v posledných rokoch zaznamenáva výraznú dynamiku rozvoja a čoraz širšiu integráciu naprieč rôznymi sektormi. Tento trend zásadným spôsobom ovplyvňuje fungovanie priemyslu, ekonomiky aj spoločnosti ako celku. Hlavným faktorom tohto pokroku sú najmä významné prelomy v oblasti strojového učenia, hlbokého učenia, ako aj prudký nárast výpočtových kapacít.

Napriek tomu, že technológie umelej inteligencie prinášajú zvýšenie efektivity a produktivity, zároveň zostávajú vystavené rastúcemu spektru bezpečnostných hrozieb a zraniteľností. Dynamický rozvoj AI preto vyvoláva potrebu dôkladného porozumenia meniacim sa rizikám, ktoré sú špecificky spojené s jej návrhom, vývojom a nasadením.

4.5.1 AI aktíva

Kľúčovým prvkom pri analýze hrozieb je identifikácia kategórií aktív, voči ktorým môžu byť hrozby smerované. Aktíva predstavujú všetko, čo má pre jednotlivca alebo organizáciu určitú hodnotu, a preto si vyžadujú primeranú ochranu. V kontexte umelej inteligencie ide zároveň o tie prvky, ktoré sú nevyhnutné na naplnenie účelu, na ktorý sú systémy AI využívané.

Popri všeobecných aktívach typických pre oblasť informačných a komunikačných technológií ako sú dáta, softvér, hardvér či komunikačné siete, prinášajú systémy AI aj

špecifické kategórie aktív. Ide najmä o modely, výpočtové zdroje (napr. procesory) a rôzne artefakty vznikajúce v procese vývoja a nasadenia AI systémov. Tieto aktíva môžu byť kompromitované alebo poškodené nielen úmyselnými útokmi, ale aj neúmyselnými chybami či zlyhaniami.

Cieľom je zachytiť nielen samotné komponenty AI, ale aj podporné prvky nevyhnutné pre vývoj a prevádzku AI systémov. Do kategórie aktív patria aj procesy súvisiace s AI, vzhľadom na ich prierezový charakter.

Agentúra ENISA klasifikuje AI aktíva do nasledujúcich šiestich kategórií:[292]

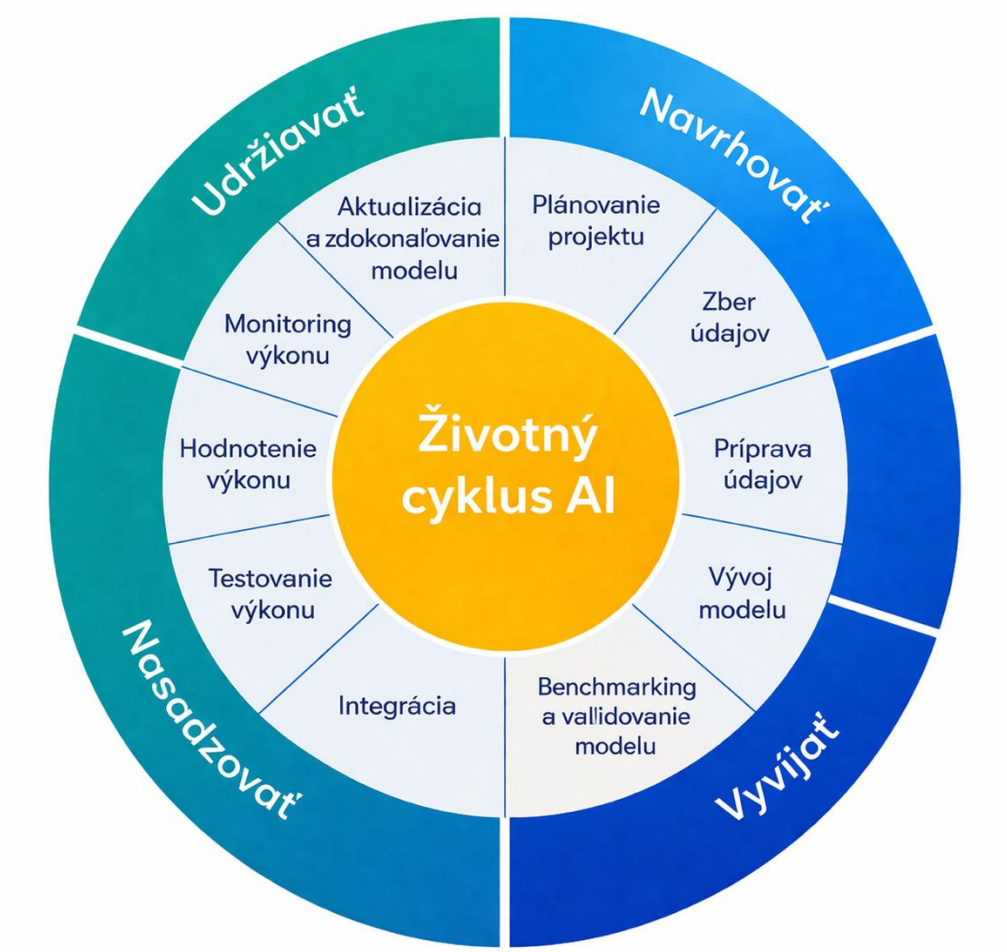
- **Dáta (napr. nespracované dáta, označené datasety, trénovacie datasety, testovacie údaje, hodnotiace údaje)**
- **Modely (napr. algoritmy, modely, parametre modelu)**
- **Aktéri (napr. vlastníci údajov, AI vývojári, dátoví inžinieri, koncoví používatelia, poskytovatelia cloudu, poskytovatelia modelov)**
- **Procesy (ukladanie, spracovanie, označovanie údajov, výber, budovanie, trénovanie a testovanie modelu)**
- **Prostredie / nástroje (napr. cloud, vizualizačné nástroje, komunikačné protokoly)**
- **Artefakty (napr. architektúra modelu, prípady použitia, politiky správy údajov, štatistické parametre)**

Táto klasifikácia umožňuje systematickejšie uchopenie rizík a hrozieb, keďže každá kategória aktív predstavuje odlišný vektor potenciálneho útoku alebo zlyhania.

4.5.2 Životný cyklus AI

Dáta predstavujú jedno z najhodnotnejších aktív v oblasti umelej inteligencie, pričom v priebehu celého životného cyklu AI dochádza k ich neustálej transformácii a spracovaniu. Životný cyklus umelej inteligencie pozostáva zo štyroch hlavných fáz: **návrh (design), vývoj (development), nasadenie (deployment) a udržiavanie (maintenance)**. Každá z týchto fáz zohráva kľúčovú úlohu pri vytváraní a udržiavaní efektívneho AI systému.

[292] ENISA: AI CYBERSECURITY CHALLENGES Threat Landscape for Artificial Intelligence December 2020. Dostupné na: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Artificial%20Intelligence%20Cybersecurity%20Challenges.pdf



Obrázok č. 9: Fázy životného cyklu AI.[293]

Vo fáze **návrhu** sa pozornosť sústreďuje na pochopenie riešeného problému, zber a prípravu relevantných dát, výber vhodných algoritmov a návrh prototypu na overenie základných konceptov. Hlavným cieľom tejto fázy je stanoviť plán a odôvodnenie využitia umelej inteligencie, konceptualizovať systém AI a definovať jeho ciele a funkčnosti. Táto fáza vytvára základ pre následný vývoj AI systému.

Fáza **vývoja** zahŕňa predspracovanie dát, implementáciu AI systému prostredníctvom výberu algoritmov, trénovanie modelu, jeho hodnotenie a optimalizáciu. Dáta sú pripravené a použité na trénovanie modelov, ktoré sú následne testované a optimalizované s cieľom dosiahnuť požadované výkonnostné parametre. Pre túto fázu je typická iteratívna povaha, ktorá umožňuje priebežné dolaďovanie modelu a zvyšovanie jeho efektívnosti.

[293] Vygenerované nástrojom UI (ChatGPT).

Po ukončení vývoja systém prechádza do fázy **nasadenia**, v rámci ktorej je integrovaný do reálneho prevádzkového prostredia. V tejto fáze sa hodnotí jeho škálovateľnosť a výkonnosť a zároveň sa monitoruje jeho správanie s cieľom identifikovať prípadné problémy alebo degradáciu výkonu (tzv. drift). Zavádzajú sa mechanizmy priebežného monitorovania a zberu spätnej väzby, aby systém spoľahlivo fungoval v reálnych podmienkach.

Fáza **údržiavania** zahŕňa kontinuálne aktivity, ako sú monitorovanie výkonu, opätovné trénovanie modelov, odstraňovanie chýb, aktualizácie a priebežné zlepšovanie systému. Výkonnosť modelov sa môže časom zhoršovať, preto je potrebné ich pravidelne aktualizovať na základe nových dát. Rovnako dôležité je zabezpečenie bezpečnosti a súladu systému s regulačnými požiadavkami.

Prevádzka a hodnotenie predstavujú prierezové činnosti, ktoré sú nevyhnutné na zabezpečenie dlhodobej funkčnosti a efektívnosti AI systémov. Prevádzka zahŕňa každodenný dohľad nad systémom, vrátane spracovania dát a rozhodovacích procesov. Priebežné hodnotenie počas celého životného cyklu umožňuje identifikovať potenciálne riziká, nedostatky a nové výzvy, čím podporuje prijímanie preventívnych opatrení na zachovanie integrity a spoľahlivosti systému.

4.5.3 Zraniteľnosti AI

Zraniteľnosti AI predstavujú špecifickú kategóriu bezpečnostných zraniteľností, ktoré vznikajú naprieč jednotlivými fázami životného cyklu AI. Ich charakter je rôznorodý, kombinujú tradičné softvérové a infraštruktúrne zraniteľnosti s novými, špecificky AI-orientovanými rizikami. Identifikácia týchto zraniteľností je kľúčová pre efektívne riadenie kybernetických hrozieb a zabezpečenie dôveryhodnosti AI systémov.

Fáza návrhu

Fáza návrhu predstavuje kritické obdobie, v ktorom sa vytvára základ AI systému. Zahŕňa procesy ako zber a príprava dát, plánovanie, návrh modelu a definovanie architektúry systému.

Medzi hlavné zraniteľnosti tejto fázy patria:

- **Nedostatočná bezpečnostná architektúra** – absencia princípov secure-by-design, nedostatočné riadenie prístupov a slabé sieťové konfigurácie môžu viesť k neoprávnenému prístupu alebo injektáži škodlivého kódu.
- **Nedostatočné modelovanie hrozieb** – neidentifikovanie potenciálnych útokov a vektorov vedie k prehliadnutiu kritických slabín systému.
- **Nedostatočná ochrana súkromia dát** – nedostatočné zabezpečenie citlivých dát počas vývoja zvyšuje riziko ich úniku alebo zneužitia.
- **Slabé autentifikačné a autorizačné mechanizmy** – umožňujú neoprávnený prístup a manipuláciu so systémom.
- **Nedostatočná validácia vstupov a výstupov** – otvára priestor pre útoky typu injection alebo cross-site scripting.
- **Nezabezpečené ukladanie a prenos dát** – zvyšuje riziko odpočúvania a krádeže dát.
- **Nedostatočné logovanie a spracovanie chýb** – sťažuje detekciu incidentov a môže odhaliť interné informácie o systéme.
- **Nevhodný výber modelu bez bezpečnostného posúdenia** – môže viesť k využitiu modelov náchylných na útoky.
- **Zraniteľnosti pri zbere a príprave dát** – manipulácia s dátami alebo slabá kontrola prístupov môže ovplyvniť kvalitu modelu.
- **Manipulácia s označením dát (label poisoning)** – vedie k narušeniu integrity trénovacích dát.
- **Injektovanie skreslenia do modelov** – spôsobuje diskriminačné alebo nesprávne rozhodnutia.

Fáza vývoja

Fáza vývoja zahŕňa implementáciu modelov, ich trénovanie, testovanie a optimalizáciu.

Typické zraniteľnosti zahŕňajú:

- **Nezabezpečené odporúčania kódu generované AI** – môžu obsahovať zraniteľnosti a viesť k nebezpečným implementáciám.
- **Zraniteľnosti v zdrojovom kóde** – napr. buffer overflow alebo nezabezpečené závislosti.

- **Nedostatočná ochrana dát počas spracovania** – umožňuje manipuláciu alebo odpočúvanie dát.
- **Slabé riadenie prístupov** – umožňuje neoprávnené zásahy do modelov alebo dát.
- **Injekcia príkazov do AI modelu (prompt/command injection)** – spôsobuje nepredvídané správanie modelu.
- **Zraniteľnosť voči nepriateľským vstupom (adversarial examples)** – vedie k nesprávnym výstupom modelu.
- **Nezabezpečený dodávateľský reťazec AI komponentov** – umožňuje zavedenie škodlivého kódu alebo zadných vrátok.
- **Nedostatočná ochrana AI aktív** – vedie k úniku modelov, dát alebo duševného vlastníctva.

Fáza nasadenia

Vo fáze nasadenia dochádza k integrácii AI systému do reálneho prostredia.

Medzi hlavné zraniteľnosti patria:

- **Nezabezpečené API rozhrania** – umožňujú neoprávnený prístup alebo manipuláciu vstupov.
- **Zraniteľnosti infraštruktúry** – slabé konfigurácie môžu viesť k výpadkom alebo kompromitácii systému.
- **Nešifrovaný prenos dát** – umožňuje odpočúvanie a manipuláciu dát.
- **Nesprávna konfigurácia cloudových služieb** – vedie k úniku dát alebo narušeniu služieb.
- **Krádež modelu** – umožňuje vytváranie kópií modelov a zneužitie duševného vlastníctva.
- **Extrahovanie promptov** – môže odhaliť citlivé informácie alebo internú logiku systému.
- **Nedostatočná ochrana výstupov modelu** – umožňuje rekonštrukciu modelu alebo únik dát.
- **Nedostatočné testovanie a hodnotenie** – vedie k nasadeniu zraniteľných alebo nespoľahlivých systémov.

Fáza udržiavania

Fáza udržiavania zabezpečuje dlhodobú funkčnosť a bezpečnosť AI systému.

Kľúčové zraniteľnosti zahŕňajú:

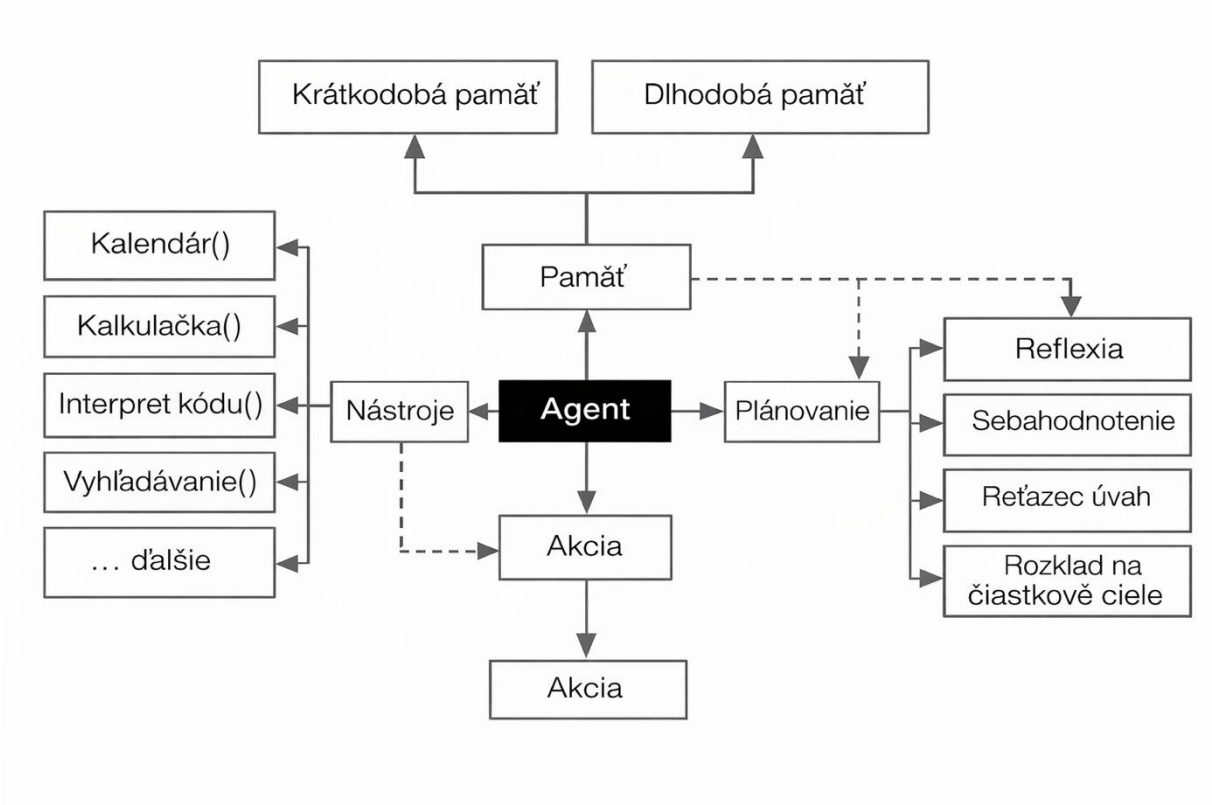
- **Oneskorené bezpečnostné aktualizácie** – umožňujú zneužitie známych zraniteľností.
- **Degradácia modelu a koncept driftu** – znižuje presnosť a môže byť zneužitá na manipuláciu výstupov.
- **Interné hrozby** – zamestnanci môžu zneužiť svoje oprávnenia.
- **Nedostatočné logovanie a monitoring** – sťažuje detekciu incidentov a umožňuje skryté útoky.

4.5.4 Agentická AI – širšia plocha útoku a nové druhy zraniteľností

Agentická umelá inteligencia (agentic AI) predstavuje významný posun v oblasti autonómnych systémov, ktorý je v súčasnosti výrazne podporený rozvojom veľkých jazykových modelov (LLM) a generatívnej AI. Hoci koncept agentov existoval už pred nástupom moderných LLM, ich prepojenie s generatívnou AI zásadne rozšírilo ich škálu využitia, schopnosti, ale aj súvisiace bezpečnostné riziká.

Agent možno definovať ako inteligentný softvérový systém, ktorý je schopný vnímať svoje prostredie, uvažovať o ňom, prijímať rozhodnutia a autonómne konať s cieľom dosiahnuť stanovené ciele. Takýto systém sa vyznačuje schopnosťou prispôsobovať sa meniacim sa podmienkam, učiť sa zo skúseností a robiť rozhodnutia v rámci svojich výpočtových a percepčných limitov.

Moderní AI agenti využívajú strojové učenie ako základ pre rozhodovanie a uvažovanie, pričom veľké jazykové modely často fungujú ako „motor uvažovania", ktorý riadi tok operácií a rozhodovacích procesov. Na rozdiel od tradičných prístupov, kde napríklad posilňované učenie (reinforcement learning) zohrával centrálnu úlohu, v súčasnosti slúži skôr ako podporný mechanizmus na zlepšovanie modelov.



Obrázok č. 10: Architektúra schopností agenta.[294]

Typický agentický AI systém vykazuje niekoľko kľúčových vlastností:

- **Plánovanie a uvažovanie**– agent je schopný plánovať kroky potrebné na dosiahnutie cieľov, aktualizovať svoje plány a riešiť komplexné úlohy. Moderné prístupy zahŕňajú reflexiu (hodnotenie vlastných krokov), sebakritiku, reťazenie úvah (chain-of-thought) a rozklad cieľov na čiastkové úlohy (subgoal decomposition).
- **Pamäť** – agent uchováva informácie z predchádzajúcich interakcií alebo krokov, či už vo forme krátkodobej (session-based) alebo dlhodobej pamäte.
- **Akcia a používanie nástrojov** – agent je schopný vykonávať akcie a využívať nástroje, vrátane externých API, vyhľadávania, výpočtov alebo generovania kódu.

Na rozdiel od tradičných modelov AI, ktoré sa sústreďujú najmä na zraniteľnosti ako otravovanie dát (data poisoning), inverziu modelu alebo adversariálne vstupy, agentická AI rozširuje priestor útoku. Dôvodom je najmä jej **kompozičný charakter**, prepojenosť viacerých komponentov a časté využívanie **multi-agentných architektúr**, kde spolu interaguje viacero autonómnych agentov.

[294] Vygenerované nástrojom UI (ChatGPT).

Táto komplexnosť vedie k vzniku nových tried zraniteľností, ktoré sú špecifické pre agentické systémy. Medzi hlavné riziká patria:[295]

1. **Zneužitie nástrojov agentom (Agentic AI Tool Misuse)** – agent môže nesprávne alebo škodlivo používať dostupné nástroje, napríklad vykonávať neautorizované operácie.
2. **Porušenie riadenia prístupov (Agent Access Control Violation)** – nedostatočná kontrola oprávnení umožňuje agentovi alebo útočníkovi prekročiť povolené hranice.
3. **Kaskádové zlyhania agentov (Agent Cascading Failures)** – chyby v jednom agentovi sa môžu šíriť naprieč systémom a ovplyvniť ďalšie komponenty.
4. **Zneužitie orchestrácie a multi-agentných systémov (Agent Orchestration Exploitation)** – komplexné interakcie medzi agentmi môžu byť zneužité na koordinované útoky.
5. **Impersonácia identity agenta (Agent Identity Impersonation)** – útočník sa môže vydávať za legitímneho agenta.
6. **Manipulácia pamäte a kontextu (Agent Memory and Context Manipulation)** – ovplyvnenie pamäte agenta vedie k nesprávnym rozhodnutiam.
7. **Nezabezpečená interakcia s kritickými systémami (Insecure Agent Critical Systems Interaction)** – agent môže nebezpečne zasahovať do externých systémov.
8. **Riziká dodávateľského reťazca (Agent Supply Chain Risk)** – zraniteľnosti v externých nástrojoch alebo závislostiach.
9. **Nedostatočná sledovateľnosť (Agent Untraceability)** – nemožnosť spätne analyzovať rozhodovanie agenta.
10. **Manipulácia cieľov a inštrukcií (Agent Goal and Instruction Manipulation)** – zmena cieľov vedie k nežiaducemu správaniu systému.

Dôležitou charakteristikou týchto rizík je ich vzájomná previazanosť. Zraniteľnosti sa často neprejavujú izolovane, ale navzájom sa posilňujú a môžu viesť ku kaskádovým efektom naprieč systémom. Napríklad zneužitie nástrojov môže byť kombinované s manipuláciou cieľov alebo nedostatočnou kontrolou prístupov, čím vznikajú komplexné a ťažko detekovateľné útoky.

[295] OWASP Agentic AI Core Security Risks In: AIVSS Scoring System For OWASP Agentic AI Core Security Risks v0.8, dostupné na: https://aivss.owasp.org.

Agentická AI tak predstavuje kvalitatívne novú úroveň rizika, kde tradičné bezpečnostné modely nie sú dostatočné. Vyžaduje si preto nové prístupy k riadeniu bezpečnosti, ktoré zohľadňujú autonómiu, adaptívnosť a prepojenosť týchto systémov.

4.5.5 AI Akt a kybernetická bezpečnosť

Prijatím nariadenia Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii) (ďalej aj ako „AI Akt") dochádza k významnému posunu v chápaní kybernetickej bezpečnosti AI. Kybernetická bezpečnosť už nie je vnímaná len ako externá ochrana informačnej infraštruktúry, ale ako **vnútorná a neoddeliteľná súčasť bezpečnosti samotného AI systému**. AI Akt tým presadzuje nový regulačný prístup, podľa ktorého bezpečnosť AI nemožno oddeliť od jej kybernetickej odolnosti. Inými slovami, vysokorizikový systém AI, ktorý nie je primerane kyberneticky zabezpečený, nemožno považovať za bezpečný v zmysle tohto nariadenia.

Tento prístup predstavuje aj normatívne zakotvenie zásady *cybersecurity-by-design*. Poskytovatelia AI systémov už nemôžu vnímať kybernetickú bezpečnosť ako doplnkovú alebo sekundárnu oblasť, ale musia ju integrovať priamo do návrhu, vývoja, testovania, nasadenia a údržby systému. Kybernetická bezpečnosť sa tak stáva jedným zo základných predpokladov uvedenia vysokorizikového AI systému na trh Európskej únie.

AI Akt stanovuje pre vysokorizikové systémy AI povinné požiadavky, ktoré sa vzťahujú najmä na riadenie rizík, kvalitu a relevantnosť dátových súborov, technickú dokumentáciu, uchovávanie záznamov, transparentnosť, poskytovanie informácií nasadzujúcim subjektom, ľudský dohľad, presnosť, spoľahlivosť a kybernetickú bezpečnosť. Tieto požiadavky sledujú ochranu zdravia, bezpečnosti a základných práv, pričom vychádzajú z logiky produktovej bezpečnosti v rámci nového legislatívneho rámca EÚ.

Z pohľadu kybernetickej bezpečnosti je osobitne významný **článok 15 AI Aktu**, podľa ktorého musia byť vysokorizikové systémy AI navrhnuté a vyvinuté tak, aby dosahovali primeranú úroveň **presnosti, spoľahlivosti a kybernetickej bezpečnosti** a aby tieto vlastnosti zachovávali konzistentne počas celého svojho životného cyklu. Spoľahlivosť

znamená, že musia byť čo najodolnejšie voči chybám, poruchám a nezrovnalostiam, ktoré môžu vzniknúť v samotnom systéme alebo v prostredí jeho prevádzky.

Pokiaľ ide o kybernetickú bezpečnosť, AI Akt výslovne požaduje, aby vysokorizikové systémy AI boli odolné voči pokusom neoprávnených tretích osôb zmeniť ich používanie, výstupy alebo výkon prostredníctvom zneužitia zraniteľností systému. Technické riešenia prijaté na zabezpečenie tejto odolnosti musia byť primerané konkrétnym okolnostiam a rizikám. AI Akt pritom výslovne reflektuje aj **zraniteľnosti špecifické pre AI**, najmä otrávenie trénovacích údajov, otrávenie modelov, adversariálne vstupy a ďalšie útoky smerujúce proti dôvernosti alebo správnemu fungovaniu modelu.

Kybernetická bezpečnosť v zmysle AI Aktu teda zahŕňa nielen ochranu tradičných digitálnych aktív a infraštruktúry, ale aj ochranu aktív špecifických pre AI, ako sú tréningové datasety, predtrénované komponenty, modely, parametre či výstupy systému. Poskytovatelia vysokorizikových systémov AI musia preto zavádzať primerané technické a organizačné opatrenia vrátane bezpečnostných opatrení, ktoré zohľadňujú tak všeobecnú IKT infraštruktúru, ako aj osobitosti AI systémov.

Významným aspektom právneho rámca je aj vzťah AI Aktu k nariadeniu CRA stanovuje horizontálne požiadavky kybernetickej bezpečnosti pre produkty s digitálnymi prvkami, zatiaľ čo AI Akt upravuje osobitné požiadavky vzťahujúce sa na AI systémy. Oba predpisy sú súčasťou európskeho produktového bezpečnostného acquis vybudovaného na princípoch nového legislatívneho rámca. V prípade vysokorizikových systémov AI, ktoré zároveň patria do pôsobnosti CRA, môže byť súlad s požiadavkami kybernetickej bezpečnosti podľa AI Aktu preukázaný splnením základných požiadaviek CRA, pokiaľ sa to riadne preukáže v EÚ vyhlásení o zhode.

Zároveň AI Akt pracuje s mechanizmami **predpokladu zhody**, pričom významnú úlohu budú zohrávať harmonizované normy a certifikačné schémy kybernetickej bezpečnosti. Podľa článku 42 sa vysokorizikové systémy AI, ktoré boli certifikované alebo pre ktoré bolo vydané vyhlásenie o zhode v rámci certifikačnej schémy kybernetickej bezpečnosti, považujú za systémy spĺňajúce požiadavky článku 15, ak sa certifikát alebo vyhlásenie na tieto požiadavky vzťahuje. Tým sa posilňuje previazanosť medzi AI reguláciou, produktovou bezpečnosťou a certifikáciou.

Osobitný režim sa vzťahuje aj na **modely AI na všeobecné účely so systémovým rizikom**. Ich poskytovatelia musia okrem všeobecných povinností zabezpečiť primeranú

úroveň kybernetickobezpečnostnej ochrany samotného modelu aj jeho fyzickej infraštruktúry počas celého životného cyklu. Sú povinní identifikovať a zmierňovať systémové riziká, vykonávať hodnotenia modelov vrátane testovania na adversariálne útoky, zavádzať politiky riadenia rizík, vykonávať monitorovanie po uvedení na trh a spolupracovať s relevantnými aktérmi v rámci hodnotového reťazca AI. Dôraz sa pritom kladie aj na ochranu pred neoprávneným prístupom, krádežou modelu, únikom váh modelu, obchádzaním bezpečnostných opatrení či zneužitím fyzickej a digitálnej infraštruktúry.

Je však potrebné zdôrazniť, že hoci AI Akt explicitne upravuje požiadavky na kybernetickú bezpečnosť predovšetkým pre vysokorizikové systémy AI a modely AI na všeobecné účely so systémovým rizikom, neznamená to, že ostatné AI systémy alebo modely sú z pohľadu kybernetickej bezpečnosti neregulované alebo že by sa na ne nevzťahovali žiadne požiadavky.

Naopak, kybernetická bezpečnosť predstavuje horizontálnu požiadavku, ktorá sa uplatňuje naprieč regulačným rámcom Európskej únie. V prípade **AI systémov, ktoré nespadajú do kategórie vysokorizikových, sa požiadavky na kybernetickú bezpečnosť uplatnia nepriamo**, najmä prostredníctvom iných právnych predpisov, predovšetkým nariadenia **CRA**, ako aj sektorových regulácií alebo všeobecných požiadaviek na bezpečnosť produktov.

Osobitne významná je situácia, keď AI systém alebo model predstavuje **komponent produktu s digitálnymi prvkami**, alebo je súčasťou takéhoto produktu. V takom prípade sa naň vzťahujú požiadavky CRA, ktoré ukladajú výrobcom povinnosť zabezpečiť kybernetickú bezpečnosť počas celého životného cyklu produktu, vrátane návrhu, vývoja, výroby a údržby. To znamená, že aj AI komponenty, ktoré samy osebe nie sú klasifikované ako vysokorizikové podľa AI Aktu, musia spĺňať primerané požiadavky kybernetickej bezpečnosti, ak sú integrované do digitálneho produktu.

Z praktického hľadiska to vedie k situácii, v ktorej AI Akt stanovuje špecifické požiadavky pre určité kategórie AI systémov, najmä vysokorizikové systémy a modely AI na všeobecné účely so systémovým rizikom, zatiaľ čo CRA a ďalšie horizontálne alebo sektorové predpisy zabezpečujú kybernetickú bezpečnosť širšieho spektra digitálnych produktov, vrátane tých, ktoré obsahujú AI komponenty.

4.5.6 Oznamovanie AI incidentov

AI Akt zavádza povinnosť oznamovania závažných incidentov v článku 73, ktorá sa vzťahuje na poskytovateľov vysokorizikových systémov AI. Táto povinnosť predstavuje dôležitý nástroj dohľadu a riadenia rizík, pričom sleduje viacero cieľov.

V prvom rade ide o vytvorenie mechanizmu včasného varovania, ktorý umožňuje orgánom dohľadu identifikovať opakujúce sa vzorce zlyhaní alebo vznikajúce riziká spojené s vysokorizikovými AI systémami. Zároveň sa tým posilňuje zodpovednosť poskytovateľov, ako aj v určitých prípadoch nasadzujúcich subjektov (deployerov), za bezpečné fungovanie týchto systémov. Oznamovacia povinnosť tiež umožňuje orgánom verejnej moci prijímať včasné nápravné opatrenia a zároveň prispieva k transparentnosti fungovania AI systémov, čím podporuje dôveru verejnosti.

AI Akt definuje „**závažný incident**" v článku 3 ods. 49 tak, že je to incident alebo porucha systému AI, ktoré priamo alebo nepriamo vyústia do ktorejkoľvek z týchto situácií:

a) smrť osoby alebo vážna ujma na zdraví osoby;

b) vážne a nezvratné narušenie riadenia alebo prevádzky kritickej infraštruktúry;

c) porušenie povinností vyplývajúcich z práva Únie, ktorých cieľom je ochrana základných práv;

d) vážna ujma na majetku alebo životnom prostredí

Zaujímavým aspektom je, že samotný pojem incident nie je v AI Akte výslovne definovaný. Vychádza sa preto z širšieho regulačného kontextu, kde incident predstavuje udalosť s negatívnymi dôsledkami alebo potenciálom takýchto dôsledkov. AI Akt zároveň rozlišuje medzi incidentom a poruchou (malfunction), pričom porucha predstavuje situáciu, keď systém nefunguje podľa očakávaní alebo deklarovaných parametrov. V praxi však toto rozlíšenie nemá striktne oddelený charakter a poruchy zohrávajú kľúčovú úlohu pri identifikácii incidentov.

Dôležitým prvkom je aj kauzalita, teda incident alebo porucha musí byť príčinou (priamou alebo nepriamou) vzniku škody. Zohľadňuje sa pritom aj použitie systému v súlade s jeho určeným účelom a predvídateľným použitím.

Návrh usmernenia Komisie podrobnejšie rozpracúva jednotlivé kategórie následkov:[296]

- **Poškodenie zdravia** zahŕňa napríklad život ohrozujúce stavy, hospitalizáciu, trvalé poškodenie zdravia alebo závažné psychické ochorenia.
- **Narušenie kritickej infraštruktúry** sa posudzuje najmä podľa jeho závažnosti a nezvratnosti v kontexte požiadaviek smerníc NIS2 a CER.
- **Porušenie základných práv** sa týka najmä situácií, ktoré majú významný dopad na väčší počet osôb, napríklad diskriminácia v náborových alebo úverových systémoch.
- **Škoda na majetku a životnom prostredí** sa posudzuje podľa rozsahu, ekonomického dopadu, trvácnosti a širších následkov.

Osobitnú kategóriu predstavuje **rozsiahle porušenie právnych predpisov** (widespread infringement), ktoré sa týka kolektívnych záujmov osôb vo viacerých členských štátoch a má cezhraničný charakter.

Poskytovatelia vysokorizikových AI systémov sú povinní:

- oznámiť závažný incident orgánom dohľadu bezodkladne, najneskôr do 15 dní od jeho zistenia,
- v prípade mimoriadne závažných situácií (napr. smrť, narušenie infraštruktúry alebo rozsiahle porušenie právnych predpisov) v kratších lehotách (2 až 10 dní),
- vykonať bezodkladné vyšetrovanie incidentu vrátane analýzy príčin a prijatia nápravných opatrení,
- spolupracovať s príslušnými orgánmi a notifikovanými osobami.

Nasadzujúce subjekty majú povinnosť informovať poskytovateľa a príslušné orgány bezodkladne, spravidla do 24 hodín od zistenia incidentu. V prípade, že nasadzujúci subjekt nedokáže poskytovateľa kontaktovať, uplatňuje sa obdobne článok 73 AI aktu.

Poskytovatelia modelov AI na všeobecné účely so systémovým rizikom majú osobitnú povinnosť monitorovať, dokumentovať a oznamovať závažné incidenty príslušným orgánom vrátane úradu pre AI.

Orgány dohľadu sú povinné prijať opatrenia v krátkych lehotách, koordinovať postup a v prípade potreby informovať ďalšie orgány, vrátane Európskej komisie.

[296] Európska komisia zverejnila návrh usmernenia k článku 73 Aktu o umelej inteligencii dňa 26. septembra 2025. Dostupné na: https://digital-strategy.ec.europa.eu/en/consultations/ai-act-commission-issues-draft-guidance-and-reporting-template-serious-ai-incidents-and-seeks.

Oznamovanie incidentov podľa AI Aktu je potrebné vnímať v širšom kontexte existujúcich regulácií, najmä smernice NIS2 a smernice CER. V súlade s článkom 73 ods. 9 AI Aktu, v sektoroch, kde už existujú povinnosti oznamovania incidentov (napr. energetika, doprava, zdravotníctvo alebo finančný sektor), sa AI Akt uplatní doplnkovo, pričom oznamovanie sa zameriava na **porušenia základných práv**. To znamená, že nedochádza k duplicite oznamovacích povinností, ale k ich vzájomnému doplneniu.

4.6 Nariadenie DORA[297]

Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011 (ďalej len „DORA") predstavuje kľúčový prvok regulačného rámca Európskej únie zameraného na **posilnenie kybernetickej bezpečnosti a odolnosti finančných subjektov** voči rizikám vyplývajúcim z využívania informačných a komunikačných technológií (ďalej len IKT). Legislatívne dôvody prijatia nariadenia DORA súvisia so skutočnosťou, že finančný sektor sa stal kriticky závislým od IKT systémov, pričom akékoľvek narušenie ich fungovania môže mať okamžité a závažné dopady na jeho stabilitu. Táto závislosť zároveň zvyšuje zraniteľnosť sektora voči kybernetickým hrozbám, ktoré majú čoraz sofistikovanejší charakter[298]. DORA "*zvyšuje úroveň harmonizácie rôznych zložiek digitálnej odolnosti zavedením požiadaviek na riadenie IKT rizika a nahlasovanie incidentov súvisiacich s IKT, ktoré sú prísnejšie v porovnaní s požiadavkami stanovenými v súčasnom práve Únie v oblasti finančných služieb, táto vyššia úroveň predstavuje zvýšenú harmonizáciu aj v porovnaní s požiadavkami stanovenými v smernici NIS 2. DORA preto predstavuje* ***lex specialis vo vzťahu k smernici NIS 2***"[299].

4.6.1 Predmet úpravy a rozsah pôsobnosti

Predmet úpravy nariadenia DORA je vymedzený v článku 1. S **cieľom dosiahnuť vysokú spoločnú úroveň digitálnej prevádzkovej odolnosti** DORA stanovuje nasledujúce **jednotné požiadavky týkajúce sa bezpečnosti sietí a informačných systémov podporujúcich obchodné procesy finančných subjektov**:

[297] Skratka z anglického Digital Operational Resilience Act.
[298] Recitály 1-3 nariadenia DORA.
[299] Recitál 16 nariadenia DORA. K uvedenému viď aj čl. 1 bod 2. DORA.

- požiadavky, ktoré sa vzťahujú na finančné subjekty v súvislosti s týmito aspektmi:
    - riadenie rizika v oblasti IKT
    - nahlasovanie závažných incidentov súvisiacich s IKT a dobrovoľné oznamovanie významných kybernetických hrozieb príslušným orgánom
    - nahlasovanie závažných prevádzkových incidentov alebo bezpečnostných incidentov súvisiacich s platbami príslušným orgánom zo strany finančných subjektov uvedených v článku 2 ods. 1 písm. a) až d) DORA
    - testovanie digitálnej prevádzkovej odolnosti
    - výmena informácií a spravodajských informácií v súvislosti s kybernetickými hrozbami a zraniteľnými miestami
    - opatrenia na správne riadenie externého IKT rizika
- požiadavky súvisiace so zmluvnými dojednaniami uzavretými medzi externými poskytovateľmi IKT služieb a finančnými subjektmi
- pravidlá zriadenia a vykonávania rámca dozoru nad kritickými externými poskytovateľmi IKT služieb, keď tieto služby poskytujú finančným subjektom
- pravidlá spolupráce medzi príslušnými orgánmi a pravidlá dohľadu a presadzovania príslušnými orgánmi v súvislosti so všetkými záležitosťami, na ktoré sa vzťahuje DORA[300].
- Nariadením DORA nie je dotknutá zodpovednosť členských štátov, pokiaľ ide o základné funkcie štátu týkajúce sa verejnej bezpečnosti, obrany a národnej bezpečnosti v súlade s právom Únie[301].

Rozsah pôsobnosti nariadenia DORA

Nariadenie DORA reguluje pomerne široký okruh finančných subjektov, pričom v článku 2 pozitívne vymedzuje regulované subjekty. Pod reguláciu spadajú nasledujúce subjekty:

- úverové inštitúcie[302]

[300] Čl. 1. bod 1. DORA.
[301] Čl. 1 bod 3. DORA.
[302] V zmysle vymedzenia v článku 4 ods. 1 bode 1 nariadenia Európskeho parlamentu a Rady (EÚ) č. 575/2013

- platobné inštitúcie[303] vrátane platobných inštitúcií vyňatých podľa smernice (EÚ) 2015/2366[304]
- poskytovatelia služieb informovania o účte[305]
- inštitúcie elektronického peňažníctva[306] vrátane inštitúcií elektronického peňažníctva vyňatých podľa smernice 2009/110/ES[307]
- investičné spoločnosti[308]
- poskytovatelia služieb kryptoaktív,[309] ktorým bolo udelené povolenie podľa nariadenia Európskeho parlamentu a Rady o trhoch s kryptoaktívami a o zmene nariadení (EÚ) č. 1093/2010 a (EÚ) č. 1095/2010 a smerníc 2013/36/EÚ a (EÚ) 2019/1937 (ďalej len „nariadenie o trhoch s kryptoaktívami") a emitenti tokenov krytých aktívami[310]
- centrálne depozitáre cenných papierov[311]
- centrálne protistrany[312]
- obchodné miesta[313]
- archívy obchodných údajov[314]
- správcovia alternatívnych investičných fondov[315]
- správcovské spoločnosti[316]
- poskytovatelia služieb vykazovania údajov[317]

[303] V zmysle vymedzenia v článku 4 bode 4 smernice (EÚ) 2015/2366.
[304] 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.
[305] Je poskytovateľ služieb informovania o účte, ako sa uvádza v článku 33 ods. 1 smernice (EÚ) 2015/2366.
[306] V zmysle vymedzenia v článku 2 bode 1 smernice Európskeho parlamentu a Rady 2009/110/ES.
[307] Smernica Európskeho parlamentu a Rady 2009/110/ES zo 16. septembra 2009 o začatí a vykonávaní činností a dohľade nad obozretným podnikaním inštitúcií elektronického peňažníctva, ktorou sa menia a dopĺňajú smernice 2005/60/ES a 2006/48/ES a zrušuje smernica 2000/46/ES.
[308] V zmysle vymedzenia v článku 4 ods. 1 bode 1 smernice 2014/65/EÚ.
[309] Je poskytovateľ služieb kryptoaktív v zmysle vymedzenia nariadenia Európskeho parlamentu a Rady o trhoch s kryptoaktívami a o zmene nariadení (EÚ) č. 1093/2010 a (EÚ) č. 1095/2010 a smerníc 2013/36/EÚ a (EÚ) 2019/1937.
[310] Je emitent tokenov krytých aktívami v zmysle vymedzenia nariadenia Európskeho parlamentu a Rady o trhoch s kryptoaktívami a o zmene nariadení (EÚ) č. 1093/2010 a (EÚ) č. 1095/2010 a smerníc 2013/36/EÚ a (EÚ) 2019/1937.
[311] V zmysle vymedzenia v článku 2 ods. 1 bode 1 nariadenia (EÚ) č. 909/2014.
[312] V zmysle vymedzenia v článku 2 bode 1 nariadenia (EÚ) č. 648/2012.
[313] V zmysle vymedzenia v článku 4 ods. 1 bode 24 smernice 2014/65/EÚ.
[314] V zmysle vymedzenia v článku 2 bode 2 nariadenia (EÚ) č. 648/2012.
[315] V zmysle vymedzenia v článku 4 ods. 1 písm. b) smernice 2011/61/EÚ.
[316] V zmysle vymedzenia v článku 2 ods. 1 písm. b) smernice 2009/65/ES.
[317] V zmysle nariadenia (EÚ) č. 600/2014, ako sa uvádza v jeho článku 2 ods. 1 bodoch 34 až 36.

- poisťovne[318] a zaisťovne[319]
- sprostredkovatelia poistenia[320], sprostredkovatelia zaistenia[321] a sprostredkovatelia doplnkového poistenia[322]
- inštitúcie zamestnaneckého dôchodkového zabezpečenia[323]
- ratingové agentúry[324]
- správcovia kritických referenčných hodnôt[325]
- poskytovatelia služieb hromadného financovania[326]
- archívy sekuritizačných údajov[327]
- externí poskytovatelia IKT služieb[328]

DORA taktiež negatívne vymedzuje osobnú pôsobnosť, keď sa nariadenie neuplatňuje na nasledujúce subjekty:

- správcov alternatívnych investičných fondov, ako sa uvádza v článku 3 ods. 2 smernice 2011/61/EÚ[329]
- poisťovne a zaisťovne, ako sa uvádza v článku 4 smernice 2009/138/ES[330]
- inštitúcie zamestnaneckého dôchodkového zabezpečenia, ktoré prevádzkujú dôchodkové plány, ktoré spolu nemajú viac ako 15 členov
- fyzické alebo právnické osoby oslobodené podľa článkov 2 a 3 smernice 2014/65/EÚ[331]

[318] V zmysle vymedzenia v článku 13 bode 1 smernice 2009/138/ES.
[319] V zmysle vymedzenia v článku 13 bode 4 smernice 2009/138/ES.
[320] V zmysle vymedzenia v článku 2 ods. 1 bode 3 smernice Európskeho parlamentu a Rady (EÚ) 2016/97.
[321] V zmysle vymedzenia v článku 2 ods. 1 bode 5 smernice (EÚ) 2016/97.
[322] V zmysle vymedzenia v článku 2 ods. 1 bode 4 smernice (EÚ) 2016/97.
[323] V zmysle vymedzenia v článku 6 bode 1 smernice (EÚ) 2016/2341.
[324] V zmysle vymedzenia v článku 3 ods. 1 písm. b) nariadenia (ES) č. 1060/2009.
[325] V zmysle vymedzenia v článku 3 ods. 1 bode 25 (EÚ) 2016/1011.
[326] V zmysle vymedzenia v článku 2 ods. 1 písm. e) nariadenia Európskeho parlamentu a Rady (EÚ) 2020/1503.
[327] V zmysle vymedzenia v článku 2 bode 23 nariadenia Európskeho parlamentu a Rady (EÚ) 2017/2402.
[328] V zmysle článku 3 bodu 19 DORA, externý poskytovateľ IKT služieb" je podnik poskytujúci IKT služby.
[329] Smernica Európskeho parlamentu a Rady 2011/61/EÚ z 8. júna 2011 o správcoch alternatívnych investičných fondov a o zmene a doplnení smerníc 2003/41/ES a 2009/65/ES a nariadení (ES) č. 1060/2009 a (EÚ) č. 1095/2010
[330] Smernica Európskeho parlamentu a Rady 2009/138/ES z 25. novembra 2009 o začatí a vykonávaní poistenia a zaistenia (Solventnosť II).
[331] Smernica Európskeho parlamentu a Rady 2014/65/EÚ z 15. mája 2014 o trhoch s finančnými nástrojmi, ktorou sa mení smernica 2002/92/ES a smernica 2011/61/EÚ.

- sprostredkovateľov poistenia, sprostredkovateľov zaistenia a sprostredkovateľov doplnkového poistenia, ktorými sú mikropodniky [332]alebo malé[333] alebo stredné podniky[334]
- poštové sporožírové inštitúcie ako sa uvádza v článku 2 ods. 5 bode 3 smernice 2013/36/EÚ[335]

Nariadenie DORA dáva právomoc členským štátom z rozsahu pôsobnosti vylúčiť subjekty uvedené v článku 2 ods. 5 bodoch 4 až 23 smernice 2013/36/EÚ[336], ktoré sa nachádzajú na ich príslušných územiach. Ak členský štát využije takúto možnosť, informuje o tom, ako aj o všetkých jej následných zmenách Komisiu. Komisia tieto informácie zverejní na svojom webovom sídle alebo inými ľahko dostupnými prostriedkami[337].

4.6.2 Kľúčové pojmy nariadenia DORA

Nariadenie DORA v článku 3 prináša viaceré definície pojmov v oblasti kybernetickej bezpečnosti a odolnosti, ktoré vytvárajú komplexný terminologický rámec, umožňujúci jednotnú interpretáciu nariadenia naprieč členskými štátmi. Význam niektorých definícií spočíva nielen v kontexte nariadenia DORA, ale aj v kontexte práva kybernetickej bezpečnosti. Pre ilustráciu v nasledujúcej časti vyberáme pre čitateľa najdôležitejšie pojmy.
Jedným z ústredných pojmov nariadenia je pojem **„digitálna prevádzková odolnosť",** ktorý DORA definuje ako "*schopnosť finančného subjektu budovať, zabezpečovať a preskúmavať svoju prevádzkovú integritu a spoľahlivosť tak, že priamo alebo nepriamo prostredníctvom využívania služieb poskytovaných externými poskytovateľmi IKT služieb zabezpečí celú škálu spôsobilostí súvisiacich s IKT, ktoré sú potrebné na zaistenie bezpečnosti sietí a informačných*

[332] Článok 3 bod 60 DORA definuje mikropodnik ako finančný subjekt iný ako obchodné miesto, centrálna protistrana, archív obchodných údajov alebo centrálny depozitár cenných papierov, ktorý zamestnáva menej ako 10 osôb a ktorého ročný obrat a/alebo celková ročná súvaha nepresahuje 2 milióny EUR.
[333] Článok 3 bod 63 DORA definuje malý podnik ako finančný subjekt, ktorý zamestnáva 10 alebo viac osôb, ale menej ako 50 osôb a ktorého ročný obrat a/alebo ročná súvaha presahujú 2 milióny EUR, ale nepresahujú 10 miliónov EUR.
[334] Článok 3 bod 64 DORA definuje stredný podnik ako finančný subjekt, ktorý nie je malým podnikom, zamestnáva menej ako 250 osôb a jeho ročný obrat nepresahuje 50 miliónov EUR a/alebo ročná súvaha nepresahuje 43 miliónov EUR.
[335] Smernica Európskeho parlamentu a Rady 2013/36/EÚ z 26. júna 2013 o prístupe k činnosti úverových inštitúcií a prudenciálnom dohľade nad úverovými inštitúciami a investičnými spoločnosťami, o zmene smernice 2002/87/ES a o zrušení smerníc 2006/48/ES a 2006/49/ES.
[336] Smernica Európskeho parlamentu a Rady 2013/36/EÚ z 26. júna 2013 o prístupe k činnosti úverových inštitúcií a prudenciálnom dohľade nad úverovými inštitúciami a investičnými spoločnosťami, o zmene smernice 2002/87/ES a o zrušení smerníc 2006/48/ES a 2006/49/ES.
[337] Článok 2 bod 4. DORA.

systémov[338]*, ktoré finančný subjekt využíva, a ktoré podporujú nepretržité poskytovanie finančných služieb a ich kvalitu, a to aj počas narušení."*[339] S uvedeným úzko súvisí pojem **„IKT riziko"**, ktorý je definovaný ako "*každá primerane identifikovateľná okolnosť v súvislosti s používaním sietí a informačných systémov, ktorá, ak k nej dôjde, môže ohroziť bezpečnosť sietí a informačných systémov, akéhokoľvek nástroja alebo procesu závislého od technológií, ako aj bezpečnosť operácií a procesov alebo poskytovania služieb vytvorením nepriaznivých účinkov v digitálnom alebo fyzickom prostredí*[340]*."* Okrem uvedeného, nariadenie DORA definuje aj pojem **„externé IKT riziko"** ktoré "*môže finančnému subjektu vzniknúť v súvislosti s jeho využívaním IKT služieb, ktoré poskytujú externí poskytovatelia IKT služieb alebo ich subdodávatelia, a to aj prostredníctvom dohôd o outsourcingu."*[341] **"IKT služby"** DORA definuje ako "*digitálne a dátové služby poskytované prostredníctvom IKT systémov jednému alebo viacerým interným alebo externým používateľom priebežne vrátane hardvéru ako služby a hardvérových služieb, ktoré zahŕňajú poskytovanie technickej podpory prostredníctvom aktualizácií softvéru alebo firmvéru poskytovateľom hardvéru s výnimkou tradičných analógových telefónnych služieb"*[342]*.*

Význam a prínos nariadenia DORA je aj v oblasti legálnej definície pojmu aktívum. DORA konkrétne definuje **"informačné aktívum"** ako "*súbor informácií, buď hmotných alebo nehmotných, ktoré sa oplatí chrániť*"[343] a **„IKT aktívum"** ako "*softvérové alebo hardvérové aktívum v sieťach a informačných systémoch, ktoré používa finančný subjekt*"[344].

V súvislosti s incidentmi DORA definuje **"incident súvisiaci s IKT"** ako "*jedna udalosť alebo séria prepojených udalostí, ktoré finančný subjekt neplánoval a ktoré narúšajú bezpečnosť sietí a informačných systémov a majú nepriaznivý vplyv na dostupnosť, pravosť, integritu alebo dôvernosť údajov alebo na služby, ktoré poskytuje finančný subjekt*"[345] a **"závažný incident súvisiaci s IKT"** ako "*incident súvisiaci s IKT, ktorý má veľký nepriaznivý vplyv na siete a informačné systémy, ktoré podporujú kritické alebo dôležité funkcie finančného subjektu*"[346].

---

[338] Nariadenie DORA preberá definíciu "sietí a informačných systémov" zo smernice NIS 2 v zmysle článku 6 bodu 1. Rovnako preberá aj definíciu "bezpečnosti sietí a informačných systémov" z NIS 2, konkrétne z článku 6 bod 2.
[339] Článok 3 bod 1 DORA.
[340] Článok 3 bod 5 DORA.
[341] Článok 3 bod 18 DORA.
[342] Článok 3 bod 21 DORA.
[343] Článok 3 bod 6 DORA.
[344] Článok 3 bod 7 DORA.
[345] Článok 3 bod 8 DORA.
[346] Článok 3 bod 10 DORA.

DORA rozoznáva aj pojmy **"prevádzkový alebo bezpečnostný incident súvisiaci s platbami",** ktorý definuje ako "*jedna udalosť alebo séria prepojených udalostí, ktoré finančné subjekty uvedené v článku 2 ods. 1 písm. a) až d) neplánovali, bez ohľadu na to, či súvisia s IKT alebo nie, a ktoré majú nepriaznivý vplyv na dostupnosť, pravosť, integritu alebo dôvernosť údajov súvisiacich s platbami, alebo na služby súvisiace s platbami, ktoré poskytuje finančný subjekt*"[347] a **"závažný prevádzkový alebo bezpečnostný incident súvisiaci s platbami"** definovaný ako **"***prevádzkový alebo bezpečnostný incident súvisiaci s platbami, ktorý má veľký nepriaznivý vplyv na poskytované služby súvisiace s platbami*"[348].

Nariadenie DORA nedefinuje kybernetickú hrozbu, túto definíciu preberá z nariadenia o kybernetickej bezpečnosti 2019/881[349]. DORA však zavádza definíciu pojmu **"významná kybernetická hrozba",** ktorá je definovaná ako "*kybernetická hrozba, ktorej technické charakteristiky naznačujú, že by mohla mať potenciál viesť k závažnému incidentu súvisiacemu s IKT alebo závažnému prevádzkovému alebo bezpečnostnému incidentu súvisiacemu s platbami*".[350] Okrem uvedeného DORA definuje aj pojem **"kybernetický útok",** ako "*zlomyseľný incident súvisiaci s IKT spôsobený prostredníctvom pokusu, ktorého sa dopustil akýkoľvek aktér hrozby, o zničenie, odhalenie, zmenu, znefunkčnenie, krádež alebo získanie neoprávneného prístupu k aktívu, alebo o neoprávnené použitie aktíva"*[351] *a* **"zraniteľnosť",** ako "*slabé miesto, náchylnosť alebo chyba aktíva, systému, procesu alebo kontroly, ktoré môžu byť zneužité*"[352].

4.6.3 Najdôležitejšie piliere nariadenia DORA

Nariadenie DORA systematicky buduje komplexný regulačný model digitálnej prevádzkovej odolnosti, ktorý možno rozdeliť do niekoľkých základných pilierov. Tieto piliere predstavujú jadro právnej úpravy a zároveň určujú povinnosti finančných subjektov. Na plnenie povinností zo strany regulovaných subjektov sa vzťahuje **zásada proporcionality,** ktorá stanovuje, že pri plnení povinností sa zohľadňuje veľkosť, celkový rizikový profil, povaha, rozsah a zložitosť služieb, činností a operácií finančných subjektov[353].

[347] Článok 3 bod 9 DORA.
[348] Článok 3 bod 11 DORA.
[349] V zmysle vymedzenia v článku 2 bode 8 nariadenia (EÚ) 2019/881.
[350] Článok 3 bod 13 DORA.
[351] Článok 3 bod 14 DORA.
[352] Článok 3 bod 16 DORA.
[353] Zásada proporcionality je upravená v článku 4 DORA.

V nasledujúcej časti sa budeme venovať piatim pilierom DORA:

1) Riadenie IKT rizika
2) Riadenie, klasifikácia a nahlasovanie incidentov súvisiacich s IKT
3) Testovanie digitálnej prevádzkovej odolnosti
4) Riadenie externého IKT rizika
5) Výmena informácií

Ad. 1) **Riadenie IKT rizika** obsahuje zásady a požiadavky na riadenie IKT rizík. Uvedený pilier je upravený v článkoch 5 až 16 nariadenia. DORA zavádza požiadavku na vytvorenie komplexného interného rámca riadenia IKT rizík, ktorý musí byť integrálnou súčasťou celkového systému riadenia regulovaného subjektu. Tento rámec zahŕňa identifikáciu (čl.8), ochranu a prevenciu (čl. 9), detekciu (čl. 10), reakciu a obnovu (čl. 11), pričom osobitný dôraz sa kladie na zapojenie riadiacich orgánov[354], ktoré nesú konečnú zodpovednosť za riadenie IKT rizík. Riadiace orgány zároveň nesú celkovú zodpovednosť za stanovenie a schválenie stratégie digitálnej prevádzkovej odolnosti, vrátane primeranej úrovne tolerancie IKT rizika finančného subjektu[355]. Schvaľujú, vykonávajú a pravidelne preskúmavajú vykonávanie politiky kontinuity činností finančného subjektu v oblasti IKT a plánov reakcie a obnovy v oblasti IKT. Riadiace orgány schvaľujú a preskúmavajú plány vnútorných auditov IKT, ktoré vypracováva finančný subjekt.[356] Medzi ďalšie povinnosti riadiacich orgánov patrí tiež prideľovanie a preskúmavanie rozpočtu na splnenie potrieb finančného subjektu v oblasti digitálnej prevádzkovej odolnosti[357], schvaľovanie a pravidelné preskúmavanie politiku finančného subjektu týkajúcu sa opatrení súvisiacich s využívaním IKT služieb, ktoré sú poskytované externými poskytovateľmi IKT služieb[358].

Medzi vybrané povinnosti finančných subjektov (iných ako mikropodnikov) v rámci tohto pilieru patrí:

[354] Článok 3. bod 30 uvádza, že "riadiaci orgán" je riadiaci orgán v zmysle vymedzenia v článku 4 ods. 1 bode 36 smernice Európskeho parlamentu a Rady 2014/65/EÚ, v článku 3 ods. 1 bode 7 smernice Európskeho parlamentu a Rady 2013/36/EÚ, v článku 2 ods. 1 písm. s) smernice Európskeho parlamentu a Rady 2009/65/ES ([31]), v článku 2 ods. 1 bode 45 nariadenia (EÚ) č. 909/2014, v článku 3 ods. 1 bode 20 nariadenia (EÚ) 2016/1011 a v príslušnom ustanovení nariadenia o trhoch s kryptoaktívami alebo rovnocenné osoby, ktoré daný subjekt skutočne riadia alebo vykonávajú kľúčové funkcie v súlade s príslušným právom Únie alebo vnútroštátnym právom.
[355] Článok 6 bod 8 DORA.
[356] Článok 5 bod 2 písm. e) DORA.
[357] Článok 5 bod 2 písmeno g) DORA.
[358] Článok 5 bod 2 písm. h) DORA.

- nastaviť a aplikovať rámec vnútornej správy a riadenia a kontroly, ktorým sa zabezpečí účinné a obozretné riadenie IKT rizika s cieľom dosiahnuť vysokú úroveň digitálnej prevádzkovej odolnosti
- zaviesť politiky zamerané na zabezpečenie zachovania vysokých noriem dostupnosti, pravosti, integrity a dôvernosti údajov
- stanoviť úlohy a zodpovednosti pre všetky funkcie súvisiace s IKT, zaviesť vhodné mechanizmy správy a riadenia s cieľom zabezpečiť účinnú a včasnú komunikáciu, spoluprácu a koordináciu medzi týmito funkciami
- používať a udržiavať aktualizované IKT systémy, protokoly a nástroje, ktoré sú vhodné, spoľahlivé, technologicky odolné a majú dostatočnú kapacitu (článok 7)
- identifikovať, klasifikovať a primerane dokumentovať všetky obchodné funkcie, úlohy a povinnosti podporované IKT, informačné aktíva a IKT aktíva . Nepretržite identifikovať všetky zdroje rizika (článok 8)
- nepretržite monitorovať a kontrolovať bezpečnosť a fungovanie IKT systémov a nástrojov a minimalizovať vplyv IKT rizika na IKT systémy zavedením vhodných nástrojov, politík a postupov v oblasti bezpečnosti IKT (článok 9)
- zaviesť mechanizmy na rýchle odhaľovanie anomálnych činností súvisiacich s IKT, ako aj identifikovať potenciálne závažné miesta zlyhania (článok 10)
- zaviesť komplexnú politiku kontinuity činností v oblasti IKT (článok 11)
- vypracovať a zdokumentovať politiky a postupy zálohovania, v ktorých sa špecifikuje rozsah údajov, ktoré sú predmetom zálohovania a minimálna frekvencia zálohovania na základe kritickosti informácií alebo úrovne dôvernosti údajov a vypracovať a zdokumentovať postupy a metódy reštaurovania a obnovy (článok 12)
- disponovať spôsobilosťami a personálom na zhromažďovania informácií o zraniteľných miestach a kybernetických hrozbách, incidentoch súvisiacich s IKT, a analyzovať vplyv, ktoré majú na digitálnu prevádzkovú odolnosť.
- zaviesť krízové komunikačné plány, ktoré umožňujú zverejňovanie aspoň závažných incidentov súvisiacich s IKT alebo zraniteľných miest pre klientov a protistrany, ako aj pre verejnosť (článok 14)

Ad. 2) **Riadenie, klasifikácia a nahlasovanie incidentov súvisiacich s IKT** ako druhý pilier nariadenia DORA kladie na regulované subjekty povinnosti vymedziť, zaviesť a vykonávať **proces riadenia incidentov** súvisiacich s IKT. Zároveň s uvedeným sú regulované subjekty povinné **klasifikovať incidenty** súvisiace s IKT a určiť ich vplyv na základe nasledujúcich kritérií:

- počet a/alebo relevantnosť klientov alebo finančných protistrán a prípadne výška alebo počet transakcií, ktoré sú ovplyvnené incidentom súvisiacim s IKT a prípadne, či incident súvisiaci s IKT mal vplyv na dobré meno
- trvanie incidentu súvisiace s IKT, ako aj trvanie výpadku služby
- geografické rozloženie, pokiaľ ide o oblasti postihnuté incidentom súvisiacim s IKT predovšetkým ak sa týka viac ako dvoch členských štátov
- straty údajov, ktoré incident súvisiaci s IKT prináša vo vzťahu k dostupnosti, pravosti, integrite alebo dôvernosti údajov,
- kritickosť zasiahnutých služieb vrátane transakcií a operácií finančného subjektu,
- hospodársky vplyv , predovšetkým priame a nepriame náklady a straty.[359]

Nariadenie DORA deleguje na Európsku komisiu právomoc doplniť nariadenie prijatím regulačných technických predpisov. Vo vzťahu k uvedenému Komisia vydala Delegované nariadenie Komisie 2024/1772[360], v ktorom sa bližšie určujú klasifikačné kritériá incidentov súvisiacich s IKT a kybernetických hrozieb, stanovujú prahové hodnoty významnosti a spresňujú podrobnosti správ o závažných incidentoch.

Regulované subjekty **sú povinné nahlasovať závažné incidenty súvisiace s IKT** relevantnému príslušnému orgánu podľa článku 46 DORA. V prípade slovenských finančných subjektov ide o **Národnú banku Slovenska**. Hlásenia sa vypĺňajú podľa vzoru stanoveného vo Vykonávacom nariadení Komisie 2025/302.[361] Nariadenie DORA a Delegované nariadenie

[359] Článok 18 bod 1 DORA.

[360] DELEGOVANÉ NARIADENIE KOMISIE (EÚ) 2024/1772 z 13. marca 2024, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, v ktorých sa bližšie určujú klasifikačné kritériá incidentov súvisiacich s IKT a kybernetických hrozieb, stanovujú prahové hodnoty významnosti a spresňujú podrobnosti správ o závažných incidentoch.

[361] VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2025/302 z 23. októbra 2024,
ktorým sa stanovujú vykonávacie technické predpisy na uplatňovanie nariadenia Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o štandardné formuláre, vzory a postupy pre finančné subjekty na nahlasovanie závažných incidentov súvisiacich s IKT a na oznamovanie významných kybernetických hrozieb.

Komisie 2025/301[362] stanovujú nahlasovať závažné incidenty súvisiace s IKT nasledujúcim spôsobom:

1) **Počiatočné oznámenie** nahlasuje regulovaný subjekt čo najskôr**, najneskôr do 24** od momentu, keď sa o **závažnom incidente súvisiaceho s IKT dozvedel**. Zároveň s uvedeným právna úprava počíta aj s možnosťou, že finančný subjekt môže **preklasifikovať incident súvisiaceho súvisiaci s IKT na závažný incident súvisiaci s IKT** a vtedy finančný subjekt musí uvedené nahlásiť **do 4 hodín** od takejto klasifikácie. Finančný subjekt nahlasuje v počiatočnom oznámení okrem všeobecných informácií vyžadovaných v zmysle článku 1 Delegovaného nariadenia Komisie 2025/301, aspoň nasledujúce špecifické informácie:
    - referenčný kód incidentu pridelený finančným subjektom,
    - dátum a čas zistenia a klasifikáciu incidentu podľa Delegovaného nariadenia Komisie 2024/1774
    - opis incidentu súvisiaceho s IKT
    - kritériá na základe ktorých finančný subjekt klasifikoval incident súvisiaci s IKT ako závažný
    - členské štáty, ktoré sú ovplyvnené incidentom súvisiacim s IKT
    - informácie ako bol incident súvisiaci s IKT zistený
    - ak sú k dispozícii, informácie o pôvode incidentu súvisiaceho s IKT
    - informácie o tom, či finančný subjekt aktivoval plán kontinuity činností
    - informácie o preklasifikovaní incidentu súvisiaceho s IKT zo závažného na menej závažný
    - akékoľvek ďalšie relevantné informácie.[363]
2) **Priebežnú správu** podáva finančný subjekt najneskôr do 72 hodín od nahlásenia počiatočného oznámenia a to aj v prípade, že sa stav alebo spôsob riešenia incidentu nezmenil. Finančné subjekty sú povinné predkladať aktualizovanú priebežnú správu v každom prípade po obnovení pravidelných činností. Priebežná správa obsahuje:

[362] DELEGOVANÉ NARIADENIE KOMISIE (EÚ) 2025/301 z 23. októbra 2024, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, v ktorých sa stanovuje obsah a lehoty na počiatočné oznámenie, a priebežnú a záverečnú správu o závažných incidentoch súvisiacich s IKT a obsah dobrovoľného oznamovania v prípade významných kybernetických hrozieb.
[363] Článok 2 Delegované nariadenie Komisie 2025/301.

- v náležitých prípadoch referenčný kód incidentu poskytnutý príslušným orgánom,
- dátum a čas výskytu incidentu súvisiaceho s IKT,
- v náležitých prípadoch dátum a čas, kedy finančný subjekt obnovil svoje pravidelné činnosti,
- informácie o tom, ako boli splnené kritériá stanovené v článkoch 1 až 8 Delegovaného nariadenia (EÚ) 2024/1772, na základe ktorých finančný subjekt klasifikoval incident súvisiaci s IKT ako závažný,
- typ incidentu súvisiaceho s IKT,
- v náležitých prípadoch hrozby a techniky používané aktérom hrozby,
- dotknuté funkčné oblasti a obchodné procesy
- dotknuté komponenty infraštruktúry podporujúce obchodné procesy
- vplyv na finančné záujmy klientov
- informácie o nahlasovaní incidentov súvisiacich s IKT iným orgánom
- dočasné kroky alebo opatrenia, ktoré finančný subjekt prijal alebo plánuje prijať na obnovu po incidente súvisiacom s IKT,
- v náležitých prípadoch informácie o ukazovateľoch ohrozenia.[364]

3) **Záverečnú správu** predloží finančný subjekt najneskôr do 1 mesiaca po predložení priebežnej správy alebo v špecifických prípadoch po poslednej aktualizovanej priebežnej správe. Finančný subjekt v záverečnej správe uvedie nasledujúce informácie:
   - informácie o hlavných príčinách incidentu súvisiaceho s IKT,
   - dátumy a časy, kedy bol incident súvisiaci s IKT vyriešený a kedy bola odstránená jeho hlavná príčina,
   - informácie o riešení incidentu súvisiaceho s IKT,
   - v náležitých prípadoch informácie relevantné pre orgány na riešenie krízových situácií,
   - informácie o priamych a nepriamych nákladoch a stratách vyplývajúcich z incidentu súvisiaceho s IKT a informácie o finančných náhradách,

[364] Článok 3 Delegované nariadenie Komisie 2025/301.

- v náležitých prípadoch informácie o opakujúcich sa incidentoch súvisiacich s IKT.[365]

Nariadenie DORA umožňuje v zmysle článku 19 bodu 2 finančným subjektom **dobrovoľne oznamovať významné kybernetické hrozby** relevantnému príslušnému orgánu, v prípade ak sa domnievajú, že **hrozba je relevantná pre finančný systém, používateľov služieb alebo klientov.** Delegované nariadenie Komisie 2025/301 upresňuje obsah dobrovoľného oznámenia o významných kybernetických hrozbách v článku 6.

Príslušný orgán podľa nariadenia DORA po prijatí počiatočného oznámenia, priebežnej správy, aktualizovanej priebežnej správy a záverečnej správy poskytne podľa článku 19 bodu 6 včas podrobné údaje o závažnom incidente súvisiacom s IKT nasledujúcim príjemcom a to náležite na základe ich príslušnej právomoci:

- Orgánom EBA (Európsky orgán pre bankovníctvo), ESMA (Európsky orgán pre cenné papiere a trhy) alebo EIOPA (Európsky orgán pre poisťovníctvo a dôchodkové poistenie zamestnancov),
- ECB (Európska centrálna banka) v prípade finančných subjektov uvedených v článku 2 bode 1 písm. a), b) a d),
- príslušným orgánom, jednotným kontaktným miestam alebo jednotkám CSIRT určeným alebo zriadeným podľa NIS 2,
- orgánom pre riešenie krízových situácií uvedeným v článku 3 smernice 2014/59/EÚ a Jednotnej rade pre riešenie krízových situácií (SRB), pokiaľ ide o subjekty uvedené v článku 7 ods. 2 nariadenia Európskeho parlamentu a Rady (EÚ) č. 806/2014, a pokiaľ ide o subjekty a skupiny uvedené v článku 7 ods. 4 písm. b) a článku 7 ods. 5 nariadenia (EÚ) č. 806/2014, ak sa takéto údaje týkajú incidentov, ktoré predstavujú riziko pre zabezpečenie kritických funkcií v zmysle článku 2 ods. 1 bodu 35 smernice 2014/59/EÚ,
- iným príslušným verejným orgánom podľa vnútroštátneho práva.

Ad. 3) **Testovanie digitálnej prevádzkovej odolnosti** ako tretí pilier nariadenia DORA vychádza z prístupu, aby finančné subjekty neobmedzovali riadenie IKT rizík len na prijímanie interných pravidiel, bezpečnostných opatrení a kontrolných mechanizmov, ale aby svoju digitálnu prevádzkovú odolnosť aj reálne overovali prostredníctvom systematického

[365] Článok 4 Delegované nariadenie Komisie 2025/301.

testovania. DORA stanovuje **6 všeobecných požiadaviek na vykonávanie testovania digitálnej prevádzkovej odolnosti** obsiahnutých v článku 24.

1. DORA ukladá finančným subjektom, ktoré nie sú mikropodnikmi, povinnosť zriadiť, udržiavať a preskúmavať spoľahlivý a komplexný program testovania digitálnej prevádzkovej odolnosti ako integrálnu súčasť ich rámca riadenia IKT rizika podľa článku 6 DORA. Už zo samotnej formulácie článku 24 vyplýva, že program testovania nemá byť izolovanou technickou aktivitou, ale musí byť pevne zabudovaný do celkovej správy a riadenia IKT rizika. Testovanie má preto nadväzovať na identifikované riziká, klasifikáciu kritických alebo dôležitých funkcií, povahu informačných aktív a na širší profil rizík daného finančného subjektu. DORA súčasne explicitne vyžaduje, aby sa pri navrhovaní a vykonávaní programu testovania prihliadalo na kritériá proporcionality uvedené v článku 4 ods. 2, teda najmä na veľkosť subjektu, jeho celkový rizikový profil, rozsah, povahu a zložitosť poskytovaných služieb a činností.
2. Nariadenie DORA stanovuje, aby testovanie digitálnej prevádzkovej odolnosti zahŕňalo celý rad posúdení, testov, metodík, postupov a nástrojov, ktoré sa majú uplatňovať v súlade s článkami o testovaní IKT nástrojov a systémov (článok 25) a pokročilého testovania IKT nástrojov, systémov a procesov vychádzajúcich z penetračného testovania na základe konkrétnej hrozby ("TLPT", článok 26).
3. Program testovania sa musí vykonávať na základe rizikovo orientovaného prístupu. Tento prístup je v rámci DORA kľúčový, pretože bráni tomu, aby sa testovanie redukovalo na mechanické splnenie formálnych požiadaviek. Finančný subjekt je povinný zohľadniť vyvíjajúce sa prostredie IKT rizík, všetky špecifické riziká, ktorým je alebo by mohol byť vystavený, kritickosť informačných aktív a služieb a akýkoľvek ďalší faktor, ktorý sám považuje za relevantný.
4. Dôležitou požiadavkou podľa článku 24 ods. 4 je nezávislosť osôb vykonávajúcich testy. Finančné subjekty iné ako mikropodniky, musia zabezpečiť, aby testovanie vykonávali nezávislé strany, či už interné alebo externé. Ak sa využije interný testovací subjekt, musí mať k dispozícii dostatočné zdroje a zároveň musia byť prijaté opatrenia na zabránenie konfliktom záujmov vo fáze navrhovania aj vykonávania testu. DORA v prípade pokročilého testovania TLPT stanovuje ešte prísnejšie požiadavky na

testovacie subjekty v článku 27 a Delegovanom nariadení 2025/1190[366]. V kontexte TLPT zohráva kľúčovú úlohu TIBER - EÚ, ktorý je *"rámcový program pre kybernetickú bezpečnosť, ktorý sa zameriava na simuláciu realistických kybernetických útokov na finančné subjekty. Na rozdiel od iných metodík rámec TIBER-EÚ umožňuje vykonávanie testov v reálnom prostredí na systémoch IKT, ktoré zabezpečujú kritické alebo dôležité funkcie, procesy alebo osoby v rámci finančného subjektu bez nutnosti samostatného testovacieho prostredia, napríklad v produkčnom prostredí. Cieľom je neustále zlepšovať kybernetickú odolnosť celého finančného sektora a umožniť subjektu dosiahnuť vyššiu úroveň kybernetickej zrelosti."*[367]

5. Finančné subjekty iné ako mikropodniky musia stanoviť postupy a politiky na určenie priorít, klasifikáciu a nápravu všetkých problémov odhalených počas vykonávania testov a zaviesť interné metodiky validácie s cieľom zabezpečiť úplné riešenie všetkých zistených slabých miest, nedostatkov a medzier.
6. Finančné subjekty iné ako mikropodniky zabezpečia, aby sa aspoň raz ročne vykonávali vhodné testy všetkých IKT systémov a aplikácií podporujúcich kritické alebo dôležité funkcie. Pre porovnanie k uvedenej všeobecnej zásade uvádzame, že v zmysle článku 26 bod 1, finančné subjekty iné ako subjekty uvedené v článku 16 bode 1 prvom pododseku a iné ako mikropodniky, ktoré sú identifikované v súlade s bodom 8 tretím pododsekom tohto článku, vykonávajú aspoň každé tri roky pokročilé testovanie prostredníctvom TLPT. Na základe rizikového profilu finančného subjektu a s prihliadnutím na prevádzkové okolnosti môže príslušný orgán v prípade potreby požiadať finančný subjekt o zníženie alebo zvýšenie tejto frekvencie.

Ad. 4) Štvrtým pilierom DORA je **riadenie externého IKT rizika** ako integrálnej súčasti rámca riadenia IKT rizika finančného subjektu. **Základnými zásadami sú**, že finančný subjekt

[366] Delegované nariadenie Komisie (EÚ) 2025/1190 z 13. februára 2025, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, v ktorých sa bližšie špecifikujú kritériá používané na identifikáciu finančných subjektov povinných vykonať penetračné testovanie na základe konkrétnej hrozby, požiadavky a normy, ktorými sa riadi využívanie interných testovacích subjektov, požiadavky týkajúce sa rozsahu pôsobnosti, metodiky testovania a prístupu pre každú fázu testovania, výsledkov, záverečného a nápravného štádia a druh spolupráce v oblasti dohľadu a v iných relevantných oblastiach potrebnej na vykonávanie TLPT a na uľahčenie vzájomného uznávania

[367] Popis TIBER-EÚ In: Národná banka Slovenska: TIBER-SK, Implementačný dokument. Národná banka Slovenska, jún 2025, str. 4. Dostupné na https://nbs.sk/dokument/f5665acb-39d2-4fee-bb01-7275de210be2/stiahnut?force=false.

zostáva **vždy plne zodpovedný za dodržiavanie povinností podľa DORA** a u**platniteľného práva v oblasti finančných služieb,** aj keď využíva externého poskytovateľa IKT služieb. Zároveň **riadenie externého IKT rizika sa má vykonávať primerane, so zohľadnením povahy, rozsahu, zložitosti a významu IKT závislostí, ako aj kritickosti alebo dôležitosti podporovanej funkcie**. Finančné subjekty musia prijať stratégiu týkajúcu sa externého IKT rizika vrátane politiky využívania IKT služieb podporujúcich kritické alebo dôležité funkcie a riadiaci orgán má pravidelne preskúmavať riziká spojené s týmito zmluvnými dojednaniami[368].

DORA vyžaduje, aby finančné subjekty **viedli a aktualizovali register informácií o všetkých zmluvných dojednaniach s externými poskytovateľmi IKT služieb**, pričom musia rozlišovať medzi službami podporujúcimi kritické alebo dôležité funkcie a ostatnými službami. Orgánom dohľadu minimálne raz ročne ohlasujú nové dojednania a register musí byť dostupný na požiadanie. **Pred uzavretím zmluvy** je **finančný subjekt povinný posúdiť, či ide o službu podporujúcu kritickú alebo dôležitú funkciu, identifikovať relevantné riziká vrátane rizika koncentrácie, preveriť vhodnosť poskytovateľa, splnenie podmienok dohľadu a možné konflikty záujmov**[369]. Finančné subjekty **môžu uzatvárať zmluvy len s poskytovateľmi, ktorí spĺňajú primerané normy informačnej bezpečnosti.** Pri kritických alebo dôležitých funkciách sa vyžaduje osobitné zohľadnenie aktuálnych a prísnych bezpečnostných štandardov. Zmluvy musia umožňovať výkon práv prístupu, inšpekcie a auditu, pričom frekvencia a rozsah auditov sa určujú na základe rizika. Pri technicky zložitých službách musí finančný subjekt overiť odbornú spôsobilosť audítorov[370].

DORA kladie dôraz aj na možnosť ukončenia zmluvného vzťahu. Zmluva musí umožniť ukončenie najmä pri závažnom porušení práva alebo zmluvy, pri slabinách poskytovateľa v riadení IKT rizika, pri okolnostiach ohrozujúcich výkon funkcií alebo ak by orgán dohľadu už nemohol účinne vykonávať dohľad. Pri službách podporujúcich kritické alebo dôležité funkcie musia existovať zdokumentované, testované a pravidelne preskúmavané exit stratégie vrátane alternatívnych riešení, plánov transformácie, bezpečného prenosu údajov a pohotovostných opatrení na zachovanie kontinuity činností.[371]

[368] Článok 28 bod 1 a 2 DORA.
[369] Článok 28 bod 3 a 4 DORA.
[370] Článok 28 bod 5 a 6 DORA.
[371] Článok 28 bod 7 a 8 DORA.

Osobitná úprava DORA sa týka **rizika koncentrácie**. **Pred uzavretím zmluvy má finančný subjekt posúdiť, či by využitie konkrétneho poskytovateľa neviedlo k závislosti od ťažko nahraditeľného subjektu alebo ku kumulácii viacerých kritických alebo dôležitých služieb u toho istého alebo úzko prepojeného poskytovateľa.** Pri subdodávateľoch sa posudzuje najmä riziko dlhých alebo zložitých subdodávateľských reťazcov, vplyv na dohľad, tretie krajiny, ochrana údajov, insolvenčné právo a schopnosť obnovy údajov.[372]

Zmluvné dojednania musia byť písomné a musia jasne určovať práva a povinnosti strán. Minimálne **musia obsahovať opis poskytovaných IKT služieb, miesta poskytovania služieb a spracúvania údajov, ustanovenia o dostupnosti, pravosti, integrite a dôvernosti údajov, pravidlá obnovy a návratu údajov, úrovne služieb, pomoc pri IKT incidente, spoluprácu s orgánmi dohľadu a právo ukončiť zmluvu**. Pri kritických alebo dôležitých funkciách sa navyše vyžadujú presné kvalitatívne a kvantitatívne výkonnostné ciele, oznamovacie povinnosti poskytovateľa, testovanie krízových plánov, spolupráca pri TLPT, neobmedzené práva auditu a jasne upravené prechodné obdobie pri ukončení spolupráce.[373] DORA zároveň zavádza rámec dozoru nad kritickými externými poskytovateľmi IKT služieb. **Európske orgány dohľadu určujú kritických poskytovateľov podľa kritérií systémového vplyvu, významu finančných subjektov, závislosti od služieb podporujúcich kritické alebo dôležité funkcie a nahraditeľnosti poskytovateľa.** Kritickí poskytovatelia sa zapisujú do zoznamu na úrovni Únie a poskytovatelia z tretích krajín môžu byť využívaní len vtedy, ak do 12 mesiacov od určenia založia dcérsky podnik v EÚ. [374]

Ad. 5) Piatym pilierom DORA je **výmena informácií,** ktorý upravuje možnosť dobrovoľnej výmeny informácií a spravodajských poznatkov o kybernetických hrozbách medzi finančnými subjektmi s cieľom posilniť ich digitálnu prevádzkovú odolnosť. Predmetom výmeny môžu byť najmä ukazovatele ohrozenia, taktiky, techniky a postupy útočníkov, bezpečnostné varovania či konfiguračné nástroje. Takáto výmena sa musí uskutočňovať v rámci dôveryhodných skupín a na základe pravidiel zabezpečujúcich ochranu obchodného tajomstva, osobných údajov podľa GDPR a pravidiel hospodárskej súťaže. DORA zároveň vyžaduje, aby dojednania o výmene informácií upravovali podmienky účasti, prípadné

[372] Článok 29 DORA.
[373] Článok 30 DORA.
[374] Článok 31 DORA.

zapojenie verejných orgánov alebo externých poskytovateľov IKT služieb a využívanie technických platforiem. Finančné subjekty sú povinné oznámiť príslušnému orgánu svoju účasť alebo ukončenie účasti v takýchto dojednaniach[375].

4.6.4 Sankcie

DORA zavádza rámec administratívnych a umožňuje členským štátom zaviesť aj trestnoprávne sankcie za porušenie povinností v oblasti digitálnej prevádzkovej odolnosti. DORA stanovuje, že príslušné orgány musia disponovať rozsiahlymi dohľadovými, vyšetrovacími a sankčnými právomocami vrátane prístupu k dokumentom a údajom, vykonávania inšpekcií a požadovania nápravných opatrení[376]. Členské štáty sú povinné zabezpečiť, aby sankcie boli účinné, primerané a odrádzajúce, pričom môžu zahŕňať príkazy na ukončenie protiprávneho konania, peňažné opatrenia, verejné oznámenia o porušení alebo opatrenia voči členom riadiacich orgánov.[377] Pri určovaní druhu a výšky sankcie sa zohľadňuje najmä závažnosť, trvanie a úmyselnosť porušenia, miera spolupráce s orgánom dohľadu, finančná sila subjektu či predchádzajúce porušenia.[378] DORA zároveň umožňuje členským štátom zaviesť trestnoprávne sankcie za porušenia nariadenia a upravuje povinnosť zverejňovania právoplatných sankčných rozhodnutí, pričom rešpektuje zásady proporcionality, ochrany osobných údajov a stability finančných trhov.[379]

[375] Článok 45 DORA.
[376] Článok 50 bod 1 a 2 DORA.
[377] Článok 50 bod 3-5 DORA.
[378] Článok 51 bod 2 DORA.
[379] Články 52-54 DORA.

5. PRÁVO KYBERNETICKEJ BEZPEČNOSTI NA ÚROVNI PRÁVNEHO PORIADKU SLOVENSKEJ REPUBLIKY

Primárnym právnym predpisom v oblasti kybernetickej bezpečnosti je zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „**ZoKB**"), ktorý je vykonávaný niekoľkými vyhláškami Národného bezpečnostného úradu (ďalej len „NBÚ"). Predmetný zákon, ktorý bol uverejnený v Zbierke zákonov Slovenskej republiky 9.3.2018 bol výsledkom transpozície smernice NIS. Po prijatí smernice NIS 2 bolo potrebné prijať transpozičnú novelu, ktorou bol zákon č. 366/2024 Z. z. ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony (ďalej len „transpozičná novela".

STRATEGICKÉ DOKUMENTY
Prijatiu ZoKB predchádzalo niekoľko strategických dokumentov v oblasti informačnej a kybernetickej bezpečnosti, konkrétne: Národná stratégia pre informačnú bezpečnosť SR (2008), Akčný plán informačnej bezpečnosti (2010), Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020 (2015), Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020 (2016). V januári 2021 bola schválená Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025. Vo februári 2026 bola schválená Národná stratégia kybernetickej bezpečnosti na roky 2026 – 2030.

Cieľom ZoKB je vytvoriť organizačnými, technickými a právnymi opatreniami prostredie, v rámci ktorého by bola kritická informačná a komunikačná infraštruktúra[380], ako aj vybrané informačné systémy a siete, chránené na dostatočnej úrovni pred rôznymi kybernetickými bezpečnostnými hrozbami, ktoré by mohli v konečnom dôsledku ohroziť riadne fungovanie dôležitých hospodárskych či spoločenských činností v štáte.

[380] Kritická informačná a komunikačná infraštruktúra predstavuje zákonom vymedzený komplex informačných systémov, služieb a elektronických komunikačných sietí, ktorých nedostupnosť by mala vážny dopad na bezpečnosť štátu, ekonomiku, verejnú správu a zabezpečenie základných životných potrieb obyvateľstva. Pozri JIRÁSEK, P. a kol.: *Výkladový slovník kybernetické bezpečnosti*. Druhé aktualizované vydání pod záštitou Národního centra kybernetické bezpečnosti České republiky a Národního bezpečnostního úřadu České, Praha 2013, s. 54-55.

Vykonávacie právne predpisy
K januáru 2026 sú účinné nasledujúce vykonávacie predpisy k ZoKB: • Vyhláška Národného bezpečnostného úradu č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov • Vyhláška Národného bezpečnostného úradu č. 492/2022 Z. z., ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti • Vyhláška Národného bezpečnostného úradu č. 493/2022 Z. z. o audite kybernetickej bezpečnosti • Vyhláška Národného bezpečnostného úradu č. 226/2025 Z. z., ktorou sa ustanovujú podrobnosti o hláseniach • Vyhláška Národného bezpečnostného úradu č. 227/2025 Z. z. o bezpečnostných opatreniach

ZoKB je prvým legislatívnym aktom na úrovni právneho poriadku Slovenskej republiky, ktorý obsahuje legálnu definíciu pojmu kybernetická bezpečnosť. V zmysle § 3 písm. h) ZoKB je **kybernetická bezpečnosť**[381] 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 NIS. Predmetná definícia v ZoKB nenadväzuje na definíciu kybernetickej bezpečnosti, ktorá je použitá v smernici NIS 2.

ZoKB ďalej definuje aj jednotlivé bezpečnostné požiadavky na ochranu informácií konkrétne dôvernosť, dostupnosť, integritu, avšak ZoKB už nedefinuje pravosť.[382]

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

[382] Pravosť, z anglického pojmu *authenticity* predstavuje vlastnosť, ktorá znamená, že deklarovaná identita entity je pravdivá.

Dôvernosť je definovaná ako:

„záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom."[383]

Dostupnosť je definovaná ako:

„záruka, že údaj alebo poskytovaná služba sú pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď sú potrebné a požadované." [384]

Integrita je definovaná ako:

„záruka, že bezchybnosť, úplnosť alebo správnosť údaja neboli narušené." [385]

ZoKB v súvislosti s definíciou pojmu **sieť a informačný systém,** tak ako je definovaný v zmysle smernice NIS 2**,** poskytuje odlišný prístup a definuje špecificky pojem sieť a pojem informačný systém.

Sieť je definovaná ako:

„elektronická komunikačná sieť podľa osobitného predpisu[386]*."*[387]

Informačný systém je definovaný ako:

„informačným systémom funkčný celok, ktorý zabezpečuje získavanie, zhromažďovanie, automatické spracúvanie, udržiavanie, sprístupňovanie,

[383] § 3 ods. 1 písm. e) ZoKB.
[384] § 3 ods. 1 písm. f) ZoKB.
[385] § 3 ods. písm. g) ZoKB.
[386] § 2 ods. 1 zákona č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov.
[387] § 3 ods. 1 písm. a) ZoKB.

poskytovanie, prenos, ukladanie, archiváciu, likvidáciu a ochranu údajov prostredníctvom technických prostriedkov alebo programových prostriedkov."[388]

5.1 Predmet a pôsobnosť ZoKB

Po prijatí transpozičnej novely sa predmet ZoKB rozšíril. ZoKB upravuje:

a) **podmienky pre riadenie a zabezpečenie kybernetickej bezpečnosti,** najmä

1. postavenie a povinnosti prevádzkovateľa základnej služby,
2. bezpečnostné opatrenia,
3. hlásenie kybernetického bezpečnostného incidentu, významnej kybernetickej hrozby, udalosti odvrátenej v poslednej chvíli a zraniteľnosti,
4. riešenie kybernetického bezpečnostného incidentu,
5. opatrenia proti produktom IKT, službám IKT alebo procesom IKT ohrozujúcim kybernetickú bezpečnosť a proti škodlivému obsahu,

b) **správu v oblasti kybernetickej bezpečnosti,** najmä

1. organizáciu, pôsobnosť a povinnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti,
2. úlohy a pôsobnosť národnej autority pre certifikáciu kybernetickej bezpečnosti,
3. národnú stratégiu kybernetickej bezpečnosti,
4. národný plán reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy,
5. jednotný informačný systém kybernetickej bezpečnosti,
6. súčinnosť a výmenu informácií,

c) **organizáciu a pôsobnosť jednotiek pre riešenie kybernetických bezpečnostných incidentov (ďalej len „jednotka CSIRT") a ich akreditáciu,**

d) **audit kybernetickej bezpečnosti a dohľad nad plnením povinností prevádzkovateľa základnej služby** podľa tohto zákona alebo povinností uložených na základe tohto zákona (ďalej len „dohľad").".

[388] § 3 ods. 1 písm. b) ZoKB.

Pôsobnosť ZoKB je vymedzená pozitívne aj negatívne. V zmysle pozitívneho vymedzenia pôsobnosti ZoKB sa predmetný zákon vzťahuje na informačné systémy zriadené a prevádzkované v pôsobnosti Ministerstva obrany Slovenskej republiky v rozsahu určenom ústredným orgánom spôsobom podľa § 33 ods. 5. [389] Z predmetného ustanovenia by sa mohlo javiť, že ZoKB sa vzťahuje len na informačné systémy zriadené a prevádzkované v pôsobnosti Ministerstva obrany Slovenskej republiky v stanovenom rozsahu. Takýto záver by bol samozrejme nesprávny, a to vzhľadom na ďalšie ustanovenia ZoKB, z ktorých vyplýva, že zákon sa vzťahuje aj na iné subjekty, resp. siete a informačné systémy. V znení ZoKB pred transpozičnou novelou bola pozitívna pôsobnosť stanovená nasledovne:

> *„Tento zákon ustanovuje minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti."*[390]

V súvislosti s prijatím transpozičnej novely sa pôsobnosť zákona rozšírila aj na niektorých poskytovateľov digitálnych služieb a infraštruktúry, ktorí nemajú trvalý pobyt, miesto podnikania alebo sídlo na území Slovenskej republiky. Týka sa najmä osôb, ktoré poskytujú službu DNS, službu registrácie názvu domény, službu cloud computingu, službu dátového centra, sieť na sprístupňovanie obsahu, riadenú službu, bezpečnostnú službu, službu online trhu, službu internetového vyhľadávača alebo platformu služieb sociálnej siete. Takéto osoby možno zapísať do registra prevádzkovateľov základnej služby, ak má väzbu na Slovenskú republiku buď tým, že sa tu prijímajú kľúčové rozhodnutia o bezpečnostných opatreniach, vykonávajú opatrenia na zachovanie kybernetickej bezpečnosti alebo sa tu nachádza prevádzkareň s najvyšším počtom zamestnancov v rámci EÚ. Ak ide o subjekt mimo EÚ, zákon sa naň môže vzťahovať aj prostredníctvom jeho zástupcu so sídlom alebo pobytom na Slovensku, prípadne aj vtedy, ak si povinného zástupcu vôbec neurčil. Ustanovenie tak zabezpečuje, aby sa poskytovatelia významných digitálnych služieb nemohli vyhnúť slovenskému režimu kybernetickej bezpečnosti len preto, že formálne nemajú sídlo na území Slovenskej republiky.

[389] § 2 ods. 1 ZoKB.
[390] § 2 ods. 1 ZoKB účinného v znení do 31.12.2024.

V zmysle **negatívneho vymedzenia pôsobnosti** sa ZoKB nevzťahuje na konkrétne právne predpisy, resp. na požiadavky na kybernetickú bezpečnosť upravené v konkrétnych právnych predpisoch. Zo zákona sú vyňaté požiadavky vyplývajúce z právnej úpravy ochrany utajovaných skutočností, osobitné oprávnenia spravodajských služieb pri ochrane kybernetického priestoru, ako aj činnosti orgánov pri vyšetrovaní, odhaľovaní a stíhaní trestných činov. Samostatne sú vylúčené aj požiadavky na bezpečnosť sietí a informačných systémov v bankovníctve, financiách a finančnom systéme, ak sú upravené osobitnými predpismi[391], vrátane pravidiel a štandardov prijatých Európskou centrálnou bankou, Európskym systémom centrálnych bánk, Eurosystémom alebo európskymi orgánmi dohľadu. Rovnako sa zákon nevzťahuje ani na dohľad a kontrolu plnenia týchto osobitných požiadaviek, ani na platobné systémy a systémy zúčtovania a vyrovnania cenných papierov a ich infraštruktúry, ak podliehajú dohľadu alebo prevádzke Európskej centrálnej banky alebo Eurosystému. Účelom tejto výluky je predísť duplicite právnej regulácie a zachovať prednosť špecializovaných režimov v oblastiach, kde kybernetická bezpečnosť podlieha osobitným pravidlám.[392]

5.2 Pôsobnosť orgánov verejnej moci

Ústredným orgánom štátnej správy v oblasti kybernetickej bezpečnosti je od. 1. januára 2016 **NBÚ**.[393] Postavenie NBÚ ako ústredného orgánu štátnej správy pre kybernetickú bezpečnosť bolo definované už v Koncepcii kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020.[394] NBÚ je národným kontaktným miestom pre kybernetickú bezpečnosť, pre vnútroštátnu spoluprácu a pre zahraničie a zabezpečuje spoluprácu s jednotnými kontaktnými miestami členských štátov Európskej únie. [395]

NBÚ plní v oblasti kybernetickej bezpečnosti v zmysle § 5 ZoKB viacero úloh. Medzi tieto úlohy patrí napr. správa a prevádzkovanie jednotného informačného systému kybernetickej bezpečnosti, akreditácia jednotiek CSIRT, vypracovanie národnej stratégie

[391] Nariadenie DORA.
[392] Bližšie pozri § 2 ods. 3 ZoKB.
[393] § 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.
[394] Dostupné na: http://www.nbusr.sk/wp-content/uploads/kyberneticka-bezpecnost/Koncepcia-kybernetickej-bezpecnosti-SR-na-roky-2015-2020-A4.pdf.
[395] § 5 ods. 1 písm. e) ZoKB.

kybernetickej bezpečnosti a i. NBÚ taktiež koná vo veci určenia subjektu ako prevádzkovateľa základnej služby a jeho zápisu do registra prevádzkovateľov základnej služby.[396] V zmysle § 6 ZoKB NBÚ zriaďuje Národné centrum kybernetickej bezpečnosti ako svoju organizačnú zložku, ktorá má postavenie národnej jednotky CSIRT s pôsobnosťou pre Slovenskú republiku. Táto jednotka je zaradená do zoznamu akreditovaných jednotiek CSIRT zo zákona a nepodlieha akreditácii.

NBÚ taktiež plní úlohy v oblasti **certifikácie kybernetickej bezpečnosti. J**e vnútroštátnym orgánom pre certifikáciu kybernetickej bezpečnosti a orgánom posudzovania zhody podľa aktu o kybernetickej bezpečnosti.[397]

Do pôsobnosti NBÚ patrí taktiež **blokovanie**. ZoKB rozlišuje medzi blokovaním z vlastnej iniciatívy NBÚ a blokovaním na žiadosť subjektov. V prípade blokovania z vlastnej iniciatívy je NBÚ oprávnený blokovať napr. webové stránky, ktoré obsahujú škodlivý obsah alebo škodlivú aktivitu.[398]

> *„Škodlivým obsahom sa rozumie programový prostriedok alebo údaj, ktorý zapríčiňuje alebo môže zapríčiniť kybernetický bezpečnostný incident. Škodlivou aktivitou sa rozumie akákoľvek činnosť, ktorá zapríčiňuje alebo môže zapríčiniť kybernetický bezpečnostný incident, podvodnú činnosť, odcudzenie osobných údajov alebo citlivých údajov, závažné dezinformácie a iné formy hybridných hrozieb.*"

NBÚ vydáva rozhodnutie o blokovaní, v ktorom bude uvedený spôsob blokovania podľa pravidiel blokovania tak, aby bolo účinné, účelné a primerané vo vzťahu k možným rizikám spojeným s blokovaním. NBÚ doručí rozhodnutie o blokovaní osobe, ktorá prevádzkuje infraštruktúru, na ktorej je blokovanie potrebné vykonať. Takáto osoba (napr. poskytovateľ prístupu na internet či hosting provider) je povinná vykonať blokovanie a zabezpečiť jeho vykonanie. Rozhodnutie o blokovaní je preskúmateľné súdom a správna žaloba nemá odkladný účinok.[399] Proti rozhodnutiu nemožno podať opravné prostriedky

[396] § 5 ods. 1 ZoKB.
[397] § 5 ods. 1 písm. y) ZoKB.
[398] § 27b ZoKB.
[399] § 27b ods. 1, 4, 5 a 6 ZoKB.

v zmysle zákona č. 71/1967 Z. o správnom konaní (správny poriadok).[400] Štátne orgány (napr. policajný zbor, Slovenská informačná služba a pod.) sú povinné bez meškania oznamovať NBÚ škodlivý obsah a škodlivé aktivity, ktoré zistia pri svojej činnosti.[401] Napriek skutočnosti, že inštitút blokovania je upravený v ustanovení § 27b ZoKB, v zmysle ods. 9 predmetného ustanovenia mohlo NBÚ rozhodnúť o blokovaní škodlivého obsahu alebo škodlivej aktivity len s platnosťou do 30. septembra 2022.

BLOKOVANIE DEZINFORMÁCII

ZoKB nedefinuje pojem dezinformácia a neupravuje kritériá, ktoré musia byť splnené, aby sme dezinformáciu považovali za závažnú. Zo ZoKB nepriamo vyplýva, že nie každá dezinformácia bude závažná. V tomto prípade ide o neurčitý právny pojem, ktorého správne naplnenie bude úlohou aplikujúceho orgánu, čiže NBÚ.

Európsky súd pre ľudské práva vo svojich rozhodnutiach zdôrazňuje predovšetkým otázku zákonnosti blokovania webových stránok. Hlavným problémom v týchto prípadoch bolo, že blokovanie, ktoré bolo nariadené súdmi alebo inými orgánmi verejnej moci často blokovalo aj iný obsah ako ten, ktorý bol predmetom záujmu.[402] Blokovanie webových stránok nie je novým inštitútom a Slovenská republika a aj iné štáty za určitým účelom obmedzujú prístup k určitým webovým stránkam. Ide najmä o prípady, kedy webová stránka obsahuje detskú pornografiu, neoprávnene sa na nej prevádzkujú hazardné hry, obsah porušuje autorské práva alebo ochranu práv spotrebiteľa. Judikatúra Európskeho súdu pre ľudské práva a Súdneho dvora Európskej únie často hovorí o tom, že by mala existovať akási notifikácia blokovanému subjektu ešte pred priamym zablokovaním a aby existovala „rovnosť zbraní" v rámci komunikácie blokovaného a blokujúceho. Inými slovami, mali by platiť určité záruky, aby nedochádzalo k zneužitiu blokovania napríklad prostredníctvom vyššie uvedených mechanizmov alebo transparentnosti a nezávislého dohľadu. Určite budú existovať situácie, kedy aj blokovanie bez predchádzajúcej notifikácie môže byť legitímne, avšak existuje množstvo situácií, keď to vhodné nie je a je skôr potrebné dať prevádzkovateľovi webu vhodný čas, aby obsah sám odstránil a až neskôr pristúpiť k blokovaniu.

[400] § 33 ods. 1 ZoKB.
[401] § 27b ods. 8 ZoKB.
[402] Bližšie pozri HUSOVEC, M.: *Ľudské práva ako všeobecný limit technológií. In* HUSOVEC, M. MESARČÍK, M. ANDRAŠKO, J. Právo informačných a komunikačných technológií 1. Bratislava: TINCT, 2020, s. 96 – 103.

NBÚ má taktiež právomoc **zakázať alebo obmedziť používanie konkrétneho produktu, procesu, služby alebo tretej strany na poskytovanie služby**. Ide o prípady, kedy NBÚ zistí, že takéto používanie neumožňuje alebo zásadným spôsobom sťažuje udržanie kybernetickej bezpečnosti, a tým ohrozuje život alebo zdravie osôb, hospodárske fungovanie štátu, verejný poriadok, bezpečnosť alebo majetok osôb. Ďalším prípadom je situácia, ak by konkrétny produkt, proces, služba alebo tretia strana na poskytovanie služby ohrozovala bezpečnostné záujmy Slovenskej republiky. Na základe rozhodnutia NBÚ je prevádzkovateľ základnej služby povinný zdržať sa používania konkrétneho produktu, procesu, služby alebo tretej strany na poskytovanie služby alebo ich používanie obmedziť. V rozhodnutí NBÚ určí primeranú dobu zákazu alebo obmedzenia používania konkrétneho produktu, procesu, služby alebo tretej strany, ktorá nemôže byť dlhšia ako dva roky. [403]

PRÍKLAD

Nariadením prezidenta USA z roku 2019 bolo zakázané používanie telekomunikačných zariadení od zahraničných firiem považovaných za riziko pre národnú bezpečnosť. V nariadení sa uvádzajú dôvody ako riziko sabotáže komunikácií, všeobecné riziká národnej bezpečnosti a riziko kritickej infraštruktúry a digitálnej ekonomiky. Pre tieto účely sa vytvoril zoznam spoločností, ktoré nemohli obchodovať so žiadnou organizáciou, ktorá pôsobí v USA. Na tomto zozname sa objavila napr. spoločnosť Huawei, ktorá bola podozrievaná, že prostredníctvom ich technológií vykonáva špionáž.[404]

ZoKB špecificky upravuje úlohy **ústredných orgánov**[405], 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,

[403] § 27a ZoKB.
[404] Dostupné na: https://www.androidauthority.com/huawei-google-android-ban-988382/.
[405] Medzi ústredné orgány podľa § 4 písm. b) ZoKB patria Ministerstvo dopravy 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, Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky a Správa štátnych hmotných rezerv Slovenskej republiky.

identifikuje prevádzkovateľa základnej služby a ich aktuálny zoznam predkladá NBú na účely zaradenia do registra PZS a i.

Pôsobnosť orgánov verejnej moci popri NBÚ a ústredných orgánoch dopĺňajú **iné orgány štátnej správy**.[406]

5.3 Prevádzkovateľ základnej služby a prevádzkovateľ kritickej základnej služby

Po prijatí transpozičnej novely došlo k zmene v otázke regulovaných subjektov. Predchádzajúca právna úprava sa vzťahovala na PZS a poskytovateľov digitálnych služieb. Po prijatí smernice NIS 2 sa očakávala zmena na národnej úrovni v otázke regulovaných subjektov, nakoľko smernica NIS 2 sa vzťahuje na kľúčové a dôležité subjekty. Slovenský regulátor sa však pri transpozičnej novele rozhodol, že nepoužije pojmológiu v zmysle smernice NIS 2 (kľúčové a dôležité subjekty) ale bude upravovať PZS a prevádzkovateľov kritických základných služieb (ďalej len „PKZS").

ZÁKLADNÁ SLUŽBA V ZÁKONE O KRITICKEJ INFRAŠTRUKTÚRE

Ponechanie pojmu prevádzkovateľ **základnej služby** môže byť z pojmologického hľadiska mätúce, a to najmä vzhľadom na právnu úpravu zákona č. 367/2024 Z. z. o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov (ďalej len „**zákon o kritickej infraštruktúre**"). Predmetný zákon je výsledkom transpozície smernica Európskeho parlamentu a Rady (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/114/ES. Zákon o kritickej infraštruktúre definuje **základnú službu** ako:

„služba kritického subjektu, ktorá má zásadný význam z hľadiska zachovania životne dôležitých spoločenských funkcií alebo hospodárskych činností, vrátane ochrany verejného zdravia, bezpečnosti alebo životného prostredia a ktorá je uvedená v prílohe č. 1."[407]

[406] Medzi iné orgány štátnej správy podľa § 4 písm. c) ZoKB 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 .

[407] § 2 písm. b)

Taktiež zákon o kritickej infraštruktúre obsahuje v § 9 obsahuje **proces identifikácie**, ktorý je podobný tomu, ktorý sa pred transpozičnou novelou ZoKB aplikoval prípade PZS.

V ustanovení § 17 ZoKB je uvedený výpočet prípadov, kedy sa subjekty **zapisujú do registra PZS**. Do registra PZS sa zapisuje:[408]

a) **ústredný orgán štátnej správy a iný štátny orgán s celoštátnou pôsobnosťou**,
b) **kritický subjekt**,
c) osoba bez ohľadu na splnenie podmienok veľkosti pre stredný podnik, ktorá vykonáva činnosť v niektorom zo **sektorov podľa prílohy č. 1 alebo prílohy č. 2 a ktorá**

1. je podnikom poskytujúcim verejnú elektronickú komunikačnú sieť alebo verejnú elektronickú komunikačnú službu,
2. je poskytovateľom dôveryhodnej služby,
3. je správcom TLD,
4. poskytuje službu DNS,
5. je v Slovenskej republike jediným poskytovateľom služby, ktorá je kľúčovou službou,
6. poskytuje službu, ktorej narušenie by mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie,
7. poskytuje službu alebo má také postavenie, že narušenie poskytovania služby alebo zásah do postavenia by mohli vyvolať významné systémové riziko najmä v sektore, v ktorom by takéto narušenie alebo zásah mohli mať cezhraničný vplyv,
8. je vzhľadom na svoj osobitný význam na vnútroštátnej alebo regionálnej úrovni kritická pre konkrétny sektor, alebo
9. je určená ako subjekt hospodárskej mobilizácie spôsobom podľa osobitného predpisu[409],

d) **štátny orgán vykonávajúci pôsobnosť v najmenej dvoch okresoch a vyšší územný celok**, ak by narušenie ich činnosti mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie; ustanovenie písmena a) tým nie je dotknuté,
e) **osoba, ktorá spĺňa najmenej podmienky veľkosti pre stredný podnik** a vykonáva činnosť v niektorom zo **sektorov podľa prílohy č. 1 alebo prílohy č. 2**,

[408] § 17 ods. 1 ZoKB.
[409] § 4 ods. 1 písm. d) zákona č. 179/2011 Z. z. v znení neskorších predpisov.

f) **mesto**, ak by narušenie výkonu jeho pôsobnosti mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie,

g) **správca informačnej technológie verejnej správy**,[410] na ktorého sa vo vzťahu k informačným technológiám verejnej správy vzťahujú minimálne bezpečnostné opatrenia Kategórie II alebo Kategórie III podľa osobitného predpisu,[411]

h) **osoba, ktorá poskytuje službu registrácie názvu domény bez ohľadu na splnenie podmienok veľkosti pre stredný podnik** alebo

i) **tretia strana**, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti, a má uzatvorenú zmluvu s prevádzkovateľom základnej služby, ktorý prevádzkuje kritickú základnú službu.

POJMY
ZoKB definuje pojmy „kľúčová služba", „významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie" a „významné systémové riziko". **kľúčovou službou** služba pre zachovanie dôležitých spoločenských oblastí alebo hospodárskych činností, pri ktorej dopad kybernetického bezpečnostného incidentu v informačnom systéme alebo v sieti, na ktorých fungovaní je závislé poskytovanie služby, môže spôsobiť 1. ohrozenie dostupnosti, pravosti, integrity alebo dôvernosti uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov, ktoré postihuje viac ako 25 000 osôb, 2. obmedzenie alebo narušenie kritického subjektu, jeho základnej služby alebo kritickej infraštruktúry, 3. hospodársku stratu vyššiu ako 0,1 % hrubého domáceho produktu podľa údajov z bezprostredne predchádzajúceho rozpočtového roka, alebo

[410] § 2 ods. 5 zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení zákona č. 67/2026 Z. z.

[411] § 3 ods. 3 a 4 vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.

4. hospodársku stratu alebo hmotnú škodu najmenej jednému užívateľovi viac ako 250 000 eur.[412]

významným vplyvom na verejný poriadok, bezpečnosť alebo verejné zdravie vplyv, pri ktorom dopad kybernetického bezpečnostného incidentu v informačnom systéme alebo v sieti, na ktorých fungovaní je závislé poskytovanie služby, môže spôsobiť narušenie verejného poriadku, bezpečnosti, ohrozenie verejného zdravia, mimoriadnu udalosť alebo tieseň, ktorá môže

1. vyžadovať vykonanie záchranných prác alebo výkon činností a opatrení súvisiacich s poskytovaním pomoci v tiesni,
2. spôsobiť viac ako 100 zranených osôb vyžadujúcich lekárske ošetrenie alebo úmrtie aspoň jednej osoby.[413]

významným systémovým rizikom riziko narušenia systému, ktoré môže mať závažné negatívne dôsledky alebo zásadným spôsobom sťažuje udržanie kybernetickej bezpečnosti, a tým ohrozuje život alebo zdravie osôb, hospodárske fungovanie štátu, verejný poriadok, bezpečnosť alebo majetok osôb, alebo ohrozuje bezpečnostné záujmy Slovenskej republiky.[414]

Z vyššie uvedeného je zjavné, že rozsah regulovaných subjektov sa po transpozičnej novele značne rozšíril, a to aj vzhľadom na **nové sektory a podsektory**. **Príloha č. 1** - **sektory s vysokou úrovňou kritickosti** obsahuje nasledujúce sektory:

1. Energetika
2. Doprava
3. Financie
4. Zdravotníctvo
5. Voda a atmosféra
6. Digitálna infraštruktúra
7. Riadenie služieb IKT medzi podnikmi

[412] § 3 ods. 1 písm. y) ZoKB.
[413] § 3 ods. 1 písm. z) ZoKB.
[414] § 3 ods. 1 písm. aa) ZoKB.

8. Verejná správa
9. Vesmír

V **prílohe č. 2 - iné kritické sektory** sú uvedené nasledujúce sektory:

1. Poštové a kuriérske služby
2. Odpadové hospodárstvo
3. Výroba a distribúcia chemických látok
4. Výroba, spracovanie a distribúcia potravín
5. Výroba
6. Poskytovatelia digitálnych služieb
7. Výskum

Ten, kto vykonáva činnosť podľa § 17 odseku 1 je povinný **do 60 dní** odo dňa, kedy činnosť začne vykonávať, **oznámiť to NBÚ**. Oznámenie musí obsahovať nasledujúce obsahové náležitosti:[415]

a) názov, sídlo a kontaktné údaje vrátane elektronických adries, verejných IP adries a telefónnych čísel,
b) zoznam členských štátov Európskej únie, v ktorých vykonáva činnosť alebo poskytuje službu,
c) názov, sídlo a kontaktné údaje zástupcu podľa § 21 ods. 1 ZoKB.

Po splnení si oznamovacej povinnosti voči NBÚ **zapíše NBÚ do registra PZS** príslušnú osobu:[416]

a) po predchádzajúcej konzultácii s príslušným ústredným orgánom, a to z vlastnej iniciatívy alebo na základe odôvodnenej žiadosti osoby alebo
b) na návrh príslušného ústredného orgánu.

Zápis do registra PZS má oznamovací, nie rozhodovací charakter. NBÚ po vykonaní zápisu bezodkladne informuje dotknutého PZS prostredníctvom jednotného informačného

[415] § 17 ods. 2 ZoKB.
[416] § 17 ods. 3 ZoKB.

systému kybernetickej bezpečnosti a zároveň mu oznámenie doručí do elektronickej schránky. Samostatné rozhodnutie sa pri zápise nevydáva.[417]

Práva a povinnosti PZS nevznikajú okamihom samotného zápisu, ale až dňom uvedeným v oznámení o zápise, najskôr však tridsiaty deň po zápise do registra. Ak sa neskôr zmenia zapísané údaje, NBÚ ich môže v registri upraviť aj bez návrhu. PZS je zároveň povinný oznámiť NBÚ každú zmenu zapísaných skutočností, ktorá nie je referenčným údajom, najneskôr do 14 dní, a to prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.[418]

ZoKB taktiež upravuje situáciu, kedy by PZS **spadol pod viaceré sektory alebo rôzne ústredné orgány**. V takomto prípade pôsobnosť podľa ZoKB je určená NBÚ na základe predchádzajúcej konzultácie s dotknutým PZS a ústredným orgánom.

PRÍKLAD
Ako príklad, kedy by PZS mohol spadnúť do 2 rôznych sektorov resp. podsektorov je prevádzkovateľ inteligentných dopravných systémov. Tento PZS môže spadnúť pod sektor Doprava/podsektor Cestná doprava a zároveň pod sektor Verejná správa ako správcovia a prevádzkovatelia informačných systémov verejnej správy podľa prílohy č. 1 ZoKB.

V praxi môžu nastať situácie, kedy bude PZS požadovať o vyradenie resp. vymazanie z registra PZS. Pôjde o situácie, kedy už nespĺňa podmienky v zmysle ZoKB pre zápis do registra PZS, resp. bol zapísaný v rozpore so ZoKB. **Výmaz** PZS z registra PZS môže NBÚ vykonať viacerými spôsobmi. Môže tak urobiť na základe odôvodnenej žiadosti samotného PZS, pričom pred výmazom konzultuje vec s príslušným ústredným orgánom a o žiadosti rozhodne najneskôr do 60 dní od jej doručenia. Výmaz je možný aj na základe oznámenia ústredného orgánu alebo z vlastnej iniciatívy NBÚ, a to len v odôvodnených prípadoch. O vykonaní výmazu z registra PZS informuje NBÚ dotknutého PZS. Výmazom prestáva byť subjekt vedený ako PZS, čo má význam najmä z hľadiska ďalšieho trvania osobitných práv a povinností spojených s týmto postavením.[419]

[417] § 17 ods. 4 ZoKB.
[418] § 17 ods. 6 ZoKB.
[419] § 17 ods. 7 ZoKB.

Ako už bolo spomínané, ZoKB popri PZS reguluje aj **prevádzkovateľov kritickej základnej služby** (PKZS). Kritickou základnou službou je:[420]

a) výkon pôsobnosti ústredného orgánu štátnej správy[421] alebo iného štátneho orgánu s celoštátnou pôsobnosťou,
b) činnosť v sektore podľa prílohy č. 1, okrem sektoru verejná správa, ak ju vykonáva osoba, ktorá prekračuje limity veľkosti určené pre stredný podnik,[422]
c) kvalifikovaná dôveryhodná služba,
d) správa TLD,
e) služba DNS,
f) poskytovanie verejnej elektronickej komunikačnej siete alebo verejnej elektronickej komunikačnej služby osobou, ktorá dosahuje najmenej podmienky veľkosti pre stredný podnik,
g) vykonávanie činnosti alebo existencia postavenia podľa § 17 ods. 1 písm. c) piateho až deviateho bodu,
h) poskytovanie základnej služby kritickým subjektom, alebo
i) informačná činnosť a elektronické služby, vykonávané s použitím informačnej technológie verejnej správy,[423] určených NBÚ.

V prípade ak PZS vykonáva aspoň jednu z kritických základných služieb, je PKZS a túto skutočnosť je povinný oznámiť NBÚ.[424]

Skutočnosť, že PZS prevádzkuje kritickú základnú službu, ako aj každú zmenu v týchto skutočnostiach, zapíše NBÚ do registra PZS. Na toto oznámenie a spôsob zápisu, ako aj na povinnosť oznamovania zmien a na ich zápis sa primerane použije § 17 ods. 3 ZoKB.[425]

[420] § 18 ods. 1 ZoKB.
[421] § 3 a 21 zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov.
[422] Odporúčanie Komisie 2003/361/ES zo 6. mája 2003 o vymedzení pojmu mikro, malých a stredných podnikov (Ú. v. EÚ L 124, 20. 5. 2003).
[423] § 2 ods. 5 zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení zákona č. 67/2026 Z. z.
[424] § 18 ods. 2 ZoKB.
[425] § 18 ods. 3 ZoKB.

Zaradenie PZS a poskytovateľov digitálnych služieb po transpozičnej novele[426]
Prechodné ustanovenia ZoKB zabezpečujú kontinuitu právneho postavenia subjektov, ktoré boli regulované podľa predchádzajúcej právnej úpravy účinnej do 31. decembra 2024. **PZS podľa doterajšej právnej úpravy sa od 1. januára 2025 automaticky považuje za PKZS**. Nejde teda o nové individuálne určenie subjektu, ale o zákonný prechod jeho postavenia do nového režimu. Úrad však môže do 31. decembra 2026 preskúmať, či takýto subjekt skutočne spĺňa podmienky ustanovené pre PKZS podľa novej právnej úpravy. Ak dospeje k záveru, že tieto podmienky splnené nie sú, môže rozhodnúť, že daná osoba prevádzkovateľom kritickej základnej služby nie je. Podobný mechanizmus sa uplatňuje aj pri **poskytovateľoch digitálnych služieb** podľa právnej úpravy účinnej do 31. decembra 2024. Títo poskytovatelia sa od 1. januára 2025 považujú za **PZS**. Aj v tomto prípade má NBÚ právomoc do 31. decembra 2026 preskúmať, či konkrétny subjekt spĺňa zákonné podmienky na zaradenie medzi PZS. Ak ich nespĺňa, NBÚ môže rozhodnúť, že takáto osoba PZS nie je. Účelom týchto ustanovení je zabrániť vzniku právnej neistoty pri prechode zo starej právnej úpravy na novú. ZoKB preto najskôr zachováva regulačné postavenie dotknutých subjektov automaticky a následne umožňuje úradu vykonať dodatočné posúdenie ich zaradenia podľa nových kritérií.

5.5 Povinnosti PZS

Povinnosti PZS vznikajú PZS dňom uvedeným v oznámení o zápise do registra PZS, najskôr však tridsiaty deň nasledujúci po dni tohto zápis.[427] Medzi základné povinnosti možno zaradiť najmä implementáciu a dodržiavanie bezpečnostných opatrení[428] a hlásenie závažných kybernetických bezpečnostných incidentov.

[426] § 34b ods. 1 až 4 ZoKB.
[427] § 17 ods. 5 ZoKB.
[428] K bezpečnostným opatreniam pozri kapitolu 1.6 Bezpečnostné opatrenia.

ROZDIEL MEDZI PZS a PKZS

Rozdiel medzi PZS a PKZS nie je v tom, že by PKZS mal úplne iný katalóg povinností. Rozdiel je najmä v tom, že **PKZS je prísnejšie regulovaný PZS**. Hlavné sprísnenia sú najmä povinnosť oznámiť prevádzkovanie kritickej základnej služby, prísnejší režim významných tretích strán, oznamovanie významných dodávateľských zmlúv, nemožnosť nahradiť audit samohodnotením v rozsahu priznanom nekritickým PZS a vyšší sankčný rámec pri najzávažnejších porušeniach.

Ak PZS zverí tretej strane činnosť, ktorá priamo súvisí s dostupnosťou, dôvernosťou alebo integritou jeho sietí a informačných systémov, musí s touto treťou stranou uzatvoriť osobitnú zmluvu. Predmetom zmluvy je zabezpečenie plnenia bezpečnostných opatrení a notifikačných povinností podľa ZoKB, a to počas celého obdobia, v ktorom tretia strana danú činnosť vykonáva. Pri uzatváraní takejto zmluvy sa zároveň musí vykonať analýza rizík.
Tretia strana je počas trvania zmluvného vzťahu povinná dodržiavať a realizovať bezpečnostné opatrenia v rozsahu určenom písomnou zmluvou a ZoKB. Zároveň musí umožniť PZS kontrolu toho, či tieto povinnosti riadne plní. Ak je zmluva uzatvorená s PZS, ktorý prevádzkuje **kritickú základnú službu**, kontrolu plnenia bezpečnostných opatrení môže vykonať aj NBÚ. Na účely takejto kontroly má **tretia strana postavenie PZS.**[429]

Tretia strana

Tretiu stranu v zmysle ZoKB chápeme ako dodávateľa na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre PZS.[430] Nižšie uvádzame niekoľko praktických príkladov:

Externý správca IT infraštruktúry

Firma, ktorá spravuje servery, operačné systémy, virtualizačnú platformu, Active Directory, sieťové prvky alebo zálohovacie prostredie PZS. Typicky má privilegované administrátorské práva, preto priamo ovplyvňuje dostupnosť, integritu aj dôvernosť systémov.

[429] § 19 ods. 2 ZoKB.
[430] § 5 ods. 1 písm. ad) ZoKB.

Dodávateľ kyberbezpečnostného monitoringu/SOC

Externý SOC, MDR alebo bezpečnostná služba, ktorá monitoruje logy, SIEM, EDR/XDR, deteguje incidenty a eskaluje ich na PZS. Ide o činnosť priamo súvisiacu s kybernetickou bezpečnosťou a aj s notifikačnými povinnosťami.

Externý prevádzkovateľ helpdesku alebo servisdesku s privilegovaným prístupom

Ak dodávateľ resetuje heslá, spravuje používateľské účty, prideľuje oprávnenia alebo rieši incidenty v produkčných systémoch, nejde len o administratívnu podporu. Taká služba má priamy dopad na dôvernosť a integritu systému.

Dodávateľ vzdialenej správy OT/ICS systémov

Napríklad pri energetike, vodárenstve, doprave alebo priemysle dodávateľ SCADA, PLC, riadiacich systémov alebo priemyselnej automatizácie. Ak má vzdialený servisný prístup alebo vykonáva aktualizácie, ide o významný príklad tretej strany.

V tejto časti učebnice sa zameriame najmä na oznamovacie povinnosti. PZS je povinný hlásiť každý závažný kybernetický bezpečnostný incident.[431]

Pre zodpovedanie otázky či regulovanému subjektu vznikla povinnosť nahlásiť závažný kybernetický bezpečnostný incident je potrebné v prvom rade ozrejmiť či ide v danom prípade o kybernetický bezpečnostný incident. V zmysle ZoKB je **kybernetickým bezpečnostným incidentom**:

> **„***udalosť ohrozujúca dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov***.“**[432]

Následne je potrebné rozhodnúť či kybernetický bezpečnostný incident napĺňa znaky závažného kybernetického bezpečnostného incidentu.

[431] § 24 ods. 1 ZoKB.
[432] § 3 ods. 1 písm. m) ZoKB.

Za **závažný kybernetický bezpečnostný incident** sa považuje **rozsiahly kybernetický bezpečnostný incident** a **kybernetický bezpečnostný incident**, ktorý

a) spôsobil alebo môže spôsobiť **závažné narušenie fungovania** prevádzkovateľa základnej služby, alebo škodu, inú ujmu na majetku alebo ušlý zisk vo veľkom rozsahu,[433]
b) zasiahol alebo môže zasiahnuť iné osoby tým, že im spôsobí škodu, inú ujmu alebo ušlý zisk v značnom rozsahu.[434]

Za závažný kybernetický bezpečnostný incident možno označiť kybernetický bezpečnostný incident, ktorý napĺňa znaky v troch nasledujúcich situáciách. **V prvom prípade** pôjde **rozsiahly kybernetický bezpečnostný incident.**

> *„kybernetický bezpečnostný incident, ktorý spôsobí narušenie na úrovni presahujúcej schopnosť Slovenskej republiky naň reagovať, alebo ktorý má významný vplyv aspoň na dva členské štáty Európskej únie"*[435]

V druhom prípade pôjde o kybernetický bezpečnostný incident, ktorý **spôsobil alebo môže spôsobiť závažné narušenie fungovania PZS, alebo škodu, inú ujmu na majetku alebo ušlý zisk vo veľkom rozsahu.** Závažné narušenie fungovania PZS sa posudzuje v zmysle vyhlášky Národného bezpečnostného úradu č. 226/2025 Z. z., ktorou sa ustanovujú podrobnosti o hláseniach. V predmetnej vyhláške sú vymedzené identifikačné kritériá závažného narušenia fungovania PZS.

PRÍLOHA Č. 1 VYHLÁŠKY Č. 226/2025 Z. Z., KTOROU SA USTANOVUJÚ PODROBNOSTI O HLÁSENIACH
IDENTIFIKAČNÉ KRITÉRIÁ ZÁVAŽNÉHO NARUŠENIA FUNGOVANIA PZS
1. Úplný výpadok alebo nedostupnosť činnosti
1.1 prevádzkovateľa kritickej základnej služby na viac ako 30 minút, alebo
1.2 prevádzkovateľa základnej služby na viac ako 60 minút,

[433] § 125 ods. 1 Trestného zákona.
[434] § 125 ods. 1 Trestného zákona.
[435] § 3 ods. 1 písm. n) ZoKB.

2. Narušenie alebo obmedzenie činnosti

2.1 prevádzkovateľa kritickej základnej služby na viac ako 60 minút, alebo

2.2 prevádzkovateľa základnej služby na viac ako 180 minút,

3. Ohrozenie dostupnosti, pravosti, integrity alebo dôvernosti údajov chránených podľa osobitného predpisu,[436]

4. Ohrozenie dostupnosti, pravosti, integrity alebo dôvernosti uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov, ktoré postihuje viac ako 25 000 osôb,

5. Spôsobenie hospodárskej straty vyššej ako 0,1 % hrubého domáceho produktu podľa údajov z bezprostredne predchádzajúceho rozpočtového roka,

6. Spôsobenie hospodárskej straty alebo hmotnej škody najmenej jednému užívateľovi viac ako 250 000 eur,

7. Vykonanie záchranných prác alebo výkon činností a opatrení súvisiacich s poskytovaním pomoci v tiesni alebo spôsobenie viac ako 100 zranených osôb vyžadujúcich lekárske ošetrenie alebo úmrtie aspoň jednej osoby, alebo

8. Udalosť,

8.1 pri ktorej došlo k zjavne neoprávnenému prístupu do siete alebo informačného systému alebo došlo k znefunkčneniu siete alebo informačného systému a ktorá by mohla spôsobiť následky uvedené v prvom až siedmom bode,

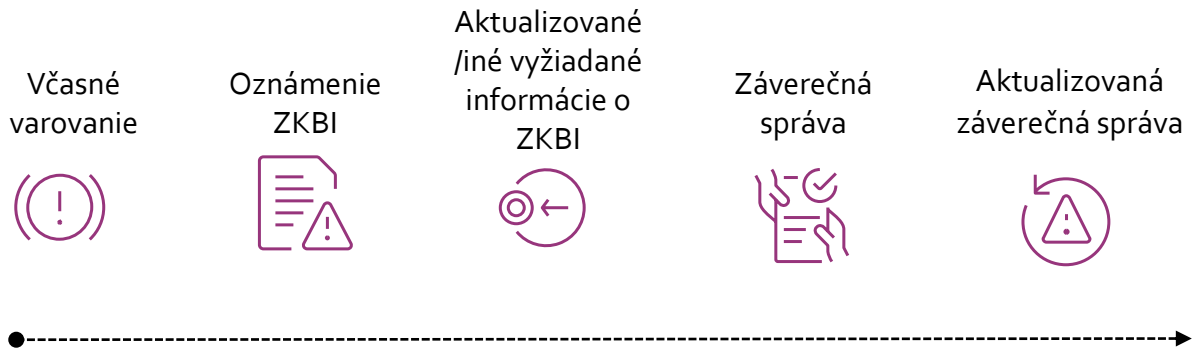
[436] Napríklad § 17 až 20 Obchodného zákonníka, § 39 zákona Slovenskej národnej rady č. 323/1992 Zb. o notároch a notárskej činnosti (Notársky poriadok) v znení neskorších predpisov, § 23 zákona Národnej rady Slovenskej republiky č. 46/1993 Z. z. o Slovenskej informačnej službe, zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 23 zákona 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 zákona č. 297/2008 Z. z., zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 24 a 25 zákona č. 576/2004 Z. z. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 11 zákona č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 10 zákona č. 324/2011 Z. z. o poštových službách a o zmene a doplnení niektorých zákonov, § 6 zákona č. 452/2021 Z. z. o elektronických komunikáciách, § 41 zákona č. 500/2022 Z. z. o Vojenskom spravodajstve.

8.2 ktorá môže významne narušiť alebo ktorá narúša fungovanie iného prevádzkovateľa kritickej základnej služby, alebo 8.3 ktorá je významným incidentom podľa osobitného predpisu[437] alebo incidentom podľa osobitného predpisu.[438]

Škoda, iná ujma na majetku alebo ušlý zisk vo **veľkom rozsahu** sa stanovuje v zmysle § 125 ods. 1 Trestného zákona.

Tretím prípadom je kybernetický bezpečnostný incident, ktorý zasiahol alebo môže zasiahnuť iné osoby tým, že im spôsobí škodu, inú ujmu alebo ušlý zisk **v značnom rozsahu** v zmysle § 125 ods. 1 Trestného zákona.

Nižšie je uvedené grafické znázornenie oznamovacej povinnosti týkajúcej sa závažného kybernetického bezpečnostného incidentu (ZKBI), ako aj popis viacvrstvového prístupu pri plnení oznamovacej povinnosti s uvedenými lehotami a obsahovými náležitosťami.



Obrázok č. 11: Oznamovacie povinnosti týkajúce sa závažného kybernetického bezpečnostného incidentu.

[437] Čl. 3 vykonávacieho nariadenia Komisie (EÚ) 2024/2690 .
[438] Zákon č. 367/2024 Z. z. o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov.

Druh	Lehota	Obsahové náležitosti (v prípade potreby)
včasné varovanie	bez zbytočného odkladu, avšak najneskôr do **24 hodín** od zistenia ZKBI	• či závažný kybernetický bezpečnostný incident mohol byť spôsobený protiprávnym konaním, alebo či môže mať cezhraničný vplyv • uvádza sa tiež vplyv na poskytovanie dôveryhodných služieb (ak PZS je poskytovateľ DS)
oznámenie o ZKBI	bez zbytočného odkladu najneskôr do **72** hodín od zistenia ZKBI *poskytovateľ dôveryhodných služieb do 24 hodín	• aktualizujú sa a dopĺňajú informácie z včasného varovania, • sa uvádza prvotné posúdenie kybernetického bezpečnostného incidentu, jeho závažnosti a následkov
aktualizované alebo iné vyžiadané informácie o priebehu ZKBI	• na žiadosť toho, kto prevádzkuje jednotku CSIRT • v určenej lehote	
záverečná správa	najneskôr **jeden mesiac** po nahlásení oznámenia o ZKBI	• podrobný opis ZKBI vrátane jeho závažnosti a následkov, • druh kybernetickej hrozby alebo hlavnú príčinu, ktorá

		pravdepodobne kybernetický bezpečnostný incident spôsobila, • zavedené a prebiehajúce opatrenia a • cezhraničný vplyv, ak existuje,
aktualizovaná záverečná správa (prebiehajúce ZKBI-cezhraničné)	• do **30 dní** odo dňa obnovy riadnej prevádzky siete a informačného systému • ak ide o ZKBI **s cezhraničným vplyvom**	
aktualizovaná záverečná správa + ďalšie aktualizované alebo iné vyžiadané informácie (prebiehajúce ZKBI)	• do **30 dní** odo dňa, keď sa KBI vyriešil	

Tabuľka č. 1: Popis viacvrstvového prístupu pri plnení oznamovacej povinnosti.

PZS má v súvislosti s oznamovacími povinnosťami taktiež **povinnosť hlásiť:**

a) významnú kybernetickú hrozbu,
b) udalosť odvrátenú v poslednej chvíli,
c) zraniteľnosti.

Ad) a

PZS prostredníctvom jednotného informačného systému kybernetickej bezpečnosti hlási **významnú kybernetickú hrozbu,** o ktorej sa dozvie.[439]

Kybernetickou hrozbou je:

„kybernetická hrozba podľa čl. 2 bodu 8 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (ďalej len „nariadenie (EÚ) 2019/881")"

Významnou kybernetickou hrozbou je:

„kybernetická hrozba, o ktorej možno na základe jej technických charakteristík predpokladať, že má potenciál spôsobiť závažný kybernetický bezpečnostný incident alebo môže mať iný závažný vplyv na sieť a informačný systém subjektu alebo používateľov služieb subjektu tým, že spôsobí značnú škodu,[9)]"

Ad) b

PZS prostredníctvom jednotného informačného systému kybernetickej bezpečnosti **udalosť odvrátenú v poslednej chvíli,** ktorá mohla spôsobiť závažný kybernetický bezpečnostný incident.[440]

Udalosťou odvrátenou v poslednej chvíli je:

„udalosť, ktorá by mohla ohroziť dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov, ale ktorej vzniku sa úspešne zabránilo alebo ku ktorej nedošlo."[441]

[439] § 24 ods. 5 písm. a) ZoKB.
[440] § 24 ods. 5 písm. b) ZoKB.
[441] § 3 ods. 1 písm. p) ZoKB.

Ad) c

PZS prostredníctvom jednotného informačného systému kybernetickej bezpečnosti hlási:

> *„zraniteľnosť ním prevádzkovaných verejne dostupných sietí a informačných systémov, ktorá podľa dostupných informácií a technických znalostí môže byť zneužitá na spôsobenie závažného kybernetického bezpečnostného incidentu a prevádzkovateľ základnej služby nemohol v primeranom čase prijať opatrenia na jej odstránenie alebo zníženie rizika."*[442]

Zraniteľnosťou je:

> *„akýkoľvek nežiaduci stav alebo chyba technického prostriedku alebo programového prostriedku, alebo nedostatok procesu vrátane nesprávnej bezpečnostnej konfigurácie, ktorá môže byť zneužitá kybernetickou hrozbou."*[443]

ZoKB umožňuje, aby PZS, ako aj iná osoba, dobrovoľne nahlásili **kybernetický bezpečnostný incident, kybernetickú hrozbu alebo udalosť odvrátenú v poslednej chvíli** aj nad rámec svojej zákonnej oznamovacej povinnosti. Pri takomto dobrovoľnom hlásení sa primerane použije postup stanovený pre povinné hlásenia. Dobrovoľné hlásenia spracúva a analyzuje NBÚ, avšak len v rozsahu, ktorý mu umožňujú jeho technické možnosti a kapacity. Zároveň sa musí dbať na to, aby spracúvanie týchto hlásení neviedlo k neprimeranému zaťažovaniu dotknutých subjektov ani k obmedzeniu medzinárodnej spolupráce v oblasti kybernetickej bezpečnosti. Ak dobrovoľné hlásenie podá osoba, ktorá nie je PZS, samotné podanie takéhoto hlásenia jej nezakladá žiadne práva ani povinnosti podľa ZoKB.[444]

Náležitosti hlásenia závažného kybernetického bezpečnostného incidentu sú uvedené vo vyhláške č. 226/2025 Z. z., ktorou sa ustanovujú podrobnosti o hláseniach.

V osobitných prípadoch môže NBÚ dohodnúť s PZS **odlišný spôsob a formu hlásenia kybernetických bezpečnostných incidentov**. Ide najmä o situácie, keď je takýto postup

[442] § 24 ods. 5 písm. c) ZoKB.
[443] § 3 ods. 1 písm. q) ZoKB.
[444] § 24 ods. 6 ZoKB.

potrebný na hlásenie závažných kybernetických bezpečnostných incidentov alebo na zaistenie kybernetickej bezpečnosti. Namiesto štandardného postupu podľa § 8 ods. 6 ZoKB môže NBÚ uzatvoriť s PZS písomnú zmluvu, v ktorej sa upraví osobitný režim hlásenia. Takáto dohoda prichádza do úvahy len pri tých PZS, pri ktorých je odlišný režim odôvodnený ich osobitným postavením, rozsahom vykonávanej činnosti alebo obsahom tejto činnosti.[445] Uvedené ustanovenie tak umožňuje flexibilnejší prístup k plneniu hlásiacich povinností tam, kde by všeobecný spôsob hlásenia prostredníctvom jednotného informačného systému kybernetickej bezpečnosti nemusel byť vzhľadom na povahu subjektu alebo jeho činnosti dostatočný alebo primeraný.

ZoKB ukladá PZS aj viacero **reakčných a koordinačných povinností**. Ich cieľom je zabezpečiť, aby sa kybernetický bezpečnostný incident nielen formálne nahlásil, ale aby bol aj efektívne riešený, zdokumentovaný a vyhodnotený. PZS je v prvom rade povinný **riešiť kybernetický bezpečnostný incident**.[446] Riešenie kybernetického bezpečnostného incidentu predstavuje aktivitu a postup zamerané na prevenciu, odhaľovanie, analýzu a obmedzovanie kybernetického bezpečnostného incidentu alebo na reakciu naň a zotavenie z neho.[447]

S tým úzko súvisí povinnosť **spolupracovať s NBÚ a príslušným ústredným orgánom** pri riešení nahláseného incidentu. PZS im musí poskytnúť potrebnú súčinnosť a relevantné informácie, ktoré získal pri vlastnej činnosti a ktoré môžu byť významné pre objasnenie príčin, priebehu alebo následkov kybernetického bezpečnostného incidentu.[448] Prakticky môže ísť napríklad o technické logy, interné zistenia, časovú os udalostí, opis zasiahnutých systémov alebo informácie o prijatých opatreniach.

Osobitný význam má povinnosť **zabezpečiť dôkaz alebo dôkazný prostriedok** počas kybernetického bezpečnostného incidentu tak, aby ho bolo možné použiť v trestnom konaní.[449] PZS musí preto pri dokumentovaní kybernetického bezpečnostného incidentu postupovať tak, aby nedošlo k znehodnoteniu digitálnych stôp. V praxi to vyžaduje najmä zachovanie integrity dát, evidovanie spôsobu ich získania a minimalizáciu neodborných zásahov do napadnutých systémov.

[445] § 24 ods. 4 ZoKB.
[446] § 19 ods. 6 písm. a) ZoKB.
[447] § 3 ods. 1 písm. o) ZoKB.
[448] § 19 ods. 6 písm. c) ZoKB.
[449] § 19 ods. 6 písm. d) ZoKB.

Ak sa PZS hodnoverným spôsobom dozvie, že kybernetický bezpečnostný incident súvisí so spáchaním trestného činu, je povinný túto skutočnosť **oznámiť orgánu činnému v trestnom konaní alebo Policajnému zboru**.[450] Táto povinnosť prepája režim kybernetickej bezpečnosti s trestnoprávnou rovinou ochrany informačných systémov.

Ďalšou povinnosťou je **analyzovať závislosti vlastných aktív, informačných systémov, využívaných IKT produktov a služieb tretích strán v dodávateľskom reťazci**. Cieľom tejto analýzy je zistiť, aké dopady môže mať kybernetický bezpečnostný incident.[451] PZS teda musí rozumieť nielen svojim vlastným systémom, ale aj tomu, ako je závislý od dodávateľov, cloudových služieb, externých poskytovateľov bezpečnostných služieb alebo iných tretích strán.

Napokon ZoKB vyžaduje, aby prevádzkovateľ vytvoril a zaviedol **účinný mechanizmus včasného informovania štatutárneho orgánu a zodpovedných vedúcich zamestnancov**. Tí musia byť informovaní najmä o kybernetických hrozbách, zraniteľnostiach, bezpečnostných incidentoch, udalostiach odvrátených v poslednej chvíli, možných dopadoch kybernetických bezpečnostných incidentov, výsledkoch analýzy rizík a stave implementácie opatrení na ošetrenie rizík.[452] Táto povinnosť zdôrazňuje, že kybernetická bezpečnosť nie je len technickou otázkou, ale aj otázkou riadenia organizácie a zodpovednosti jej vedenia.

PZS má taktiež povinnosti v oblasti **auditu**. Auditom sa preveruje, či sú prijaté bezpečnostné opatrenia účinné a či PZS plní požiadavky ZoKB. Prvý audit sa musí vykonať **do dvoch rokov** odo dňa zaradenia PZS do registra PZS.[453]

Audit sa nevykonáva iba jednorazovo. PZS je povinný vykonať audit aj **po každej zmene, ktorá má významný vplyv na realizované bezpečnostné opatrenia**, a následne v pravidelných časových intervaloch ustanovených vykonávacím predpisom. Podľa vyhlášky č. 493/2022 Z. z. o audite kybernetickej bezpečnosti sa audit vykonáva **každé dva roky** a pri významnej zmene sa musí začať **najneskôr do dvoch mesiacov** od okamihu, keď zmena nadobudla významný vplyv na realizované bezpečnostné opatrenia.[454]

[450] § 19 ods. 6 písm. e) ZoKB.
[451] § 19 ods. 6 písm. f) ZoKB.
[452] § 19 ods. 6 písm. h) ZoKB.
[453] § 29 ods. 1 ZoKB.
[454] Vyhláška č. 493/2022 Z. z. o audite kybernetickej bezpečnosti.

5.6 Jednotný informačný systém kybernetickej bezpečnosti

Jednotný informačný systém kybernetickej bezpečnosti (ďalej len „JISKB") predstavuje informačný systém, ktorého správcom a prevádzkovateľom je úrad a ktorý slúži na efektívne riadenie, koordináciu, evidenciu a kontrolu výkonu štátnej správy v oblasti kybernetickej bezpečnosti a jednotiek CSIRT. Jeho správcom a prevádzkovateľom je NBÚ.[455]

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 a neverejnú časť. Verejná časť obsahuje: [456]

a) *register ústredných orgánov,*
b) *register prevádzkovateľov základnej služby,*
c) *zoznam akreditovaných jednotiek CSIRT,*
d) *metodiky, usmernenia, štandardy, politiky a oznamy,*
e) *informácie potrebné na používanie jednotného informačného systému kybernetickej bezpečnosti,*
f) *výstrahy, varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov kybernetického bezpečnostného incidentu,*
g) *nástroj na registráciu zmien, hlásenie zmien a ostatné súvisiace nástroje.*

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, Národná banka Slovenska, Úrad na ochranu osobných údajov Slovenskej republiky, Úrad pre reguláciu elektronických komunikácií a poštových služieb a iný orgán verejnej moci rozhodnutím NBÚ.[457]

5.7 Dohľad a sankcie

Po prijatí transpozičnej novely vykonáva NBÚ dohľad:[458]

a) vybavovaním sťažností,

[455] § 8 ods. 1 ZoKB.
[456] § 8 ods. 2 ZoKB.
[457] § 8 ods. 5 ZoKB.
[458] § 29a ods. 1 ZoKB.

b) kontrolou,
c) ukladaním opatrení na zastavenie porušovania povinností a nápravu nezákonného stavu (ďalej len „opatrenia na nápravu"),
d) schvaľovaním dohody o náprave,
e) prejednávaním správnych deliktov a ukladaním poriadkových pokút a pokút.

NBÚ má oprávnenie ukladať **opatrenia na nápravu**, ak pri dohľade zistí nedostatky v plnení povinností PZS. NBÚ pritom prihliada najmä na závažnosť, rozsah, trvanie, následky a povahu zistených nedostatkov. NBÚ môže PZS uložiť najmä povinnosť vykonať audit kybernetickej bezpečnosti, realizovať odporúčania z auditu, prijať konkrétne nápravné opatrenia alebo informovať dotknuté osoby či verejnosť o rizikách a následkoch porušenia povinností. Vo výnimočných prípadoch môže NBÚ zakázať poskytovanie služby až do nápravy nezákonného stavu, najmä ak je bezprostredne ohrozený život alebo zdravie a iné opatrenia neboli účinné. [459]

Ak prevádzkovateľ nesplní uložené opatrenia včas, NBÚ mu môže uložiť aj **penále za každý deň omeškania**. V tom istom konaní môže NBÚ uložiť aj pokutu za správny delikt, ak porušenie napĺňa jeho skutkovú podstatu.[460]

Pri **prevádzkovateľovi kritickej základnej služby** ZoKB umožňuje ešte prísnejší postup. Ak nesplní povinnosť vykonať audit alebo prijať opatrenia na nápravu ani v dodatočnej lehote, NBÚ môže:[461]

> *„zakázať štatutárnemu orgánu prevádzkovateľa základnej služby alebo členovi štatutárneho orgánu prevádzkovateľa základnej služby, jeho vedúcemu zamestnancovi na najvyššej úrovni riadenia zodpovednému za príslušnú činnosť alebo výkonom tejto činnosti poverenému splnomocnencovi vykonávať ich funkciu, zamestnanie alebo činnosť u prevádzkovateľa základnej služby, a to až do doby splnenia týchto povinností."*

Táto možnosť sa však neuplatní pri orgánoch verejnej moci.

[459] § 29j ods. 1 ZoKB.
[460] § 29j ods. 2 a 3 ZoKB.
[461] § 29j ods. 4 ZoKB.

ZoKB popri **priestupkoch**, kedy je potrestaná fyzická osoba neplniaca si povinnosti v pracovnoprávnom vzťahu s PZS, upravuje aj **správne delikty**, kedy sa vyvodzuje zodpovednosť voči PZS.

PRÍKLAD

Nemocnica ako PZS má pravidlo, že vzdialený administrátorský prístup do informačných systémov sa môže používať iba cez služobné zariadenie a viacfaktorové overenie.
IT administrátor sa napriek tomu prihlási do systému zo súkromného notebooku bez dodržania bezpečnostných pravidiel. Cez toto zariadenie sa do systému dostane škodlivý kód a vznikne kybernetický bezpečnostný incident.

V takom prípade môže byť sankcionovaný:
IT administrátor ako fyzická osoba
Za priestupok, pretože nepostupoval podľa technických, organizačných alebo personálnych opatrení prijatých prevádzkovateľom základnej služby.

Nemocnica ako právnická osoba
Za správny delikt, ak sa preukáže, že bezpečnostné opatrenia neprijala, nevykonávala alebo nedostatočne kontrolovala ich dodržiavanie.
Nejde o dvojité potrestanie tej istej osoby. Fyzická osoba zodpovedá za vlastné protiprávne konanie, zatiaľ čo právnická osoba zodpovedá za porušenie svojich povinností ako PZS.

Za priestupok môže NBÚ uložiť **pokutu** od 100 eur až do 5 000 eur.[462]

Pri správnych deliktoch ZoKB rozlišuje porušenia podľa ich závažnosti. Pri menej závažných porušeniach môže NBÚ uložiť pokutu spravidla od **300 eur do 500 000 eur**. Pri závažnejších porušeniach prevádzkovateľa základnej služby môže pokuta dosiahnuť až **7 000 000 eur** alebo **1,4 % celkového celosvetového ročného obratu**. Ak ide o prevádzkovateľa kritickej základnej služby, sankcia môže byť ešte vyššia, a to až **10 000 000 eur** alebo **2 % celkového celosvetového ročného obratu**.[463]

[462] § 30 ods. 2 ZoKB.
[463] § 31 ZoKB.

Pokuty sa môžu týkať najmä porušenia povinností pri prijímaní bezpečnostných opatrení, hlásení a riešení kybernetických bezpečnostných incidentov, poskytovaní súčinnosti NBÚ, vedení bezpečnostnej dokumentácie alebo plnení uložených opatrení.

Pri určovaní výšky pokuty NBÚ prihliada na závažnosť, trvanie, následky a okolnosti porušenia. Ak je následok nepatrný alebo postačuje samotné prejednanie veci, NBÚ pokutu nemusí uložiť. Pri opakovanom porušení možno sankciu zvýšiť.[464]

5.8 Súvisiace právne predpisy

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. 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.

Špecifická právna úprava kybernetickej bezpečnosti informačných systémov verejnej správy (ďalej „ISVS") je upravená zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „**zákon o ITVS**").

Bezpečnosť informačných technológiách vo verejnej správe (ďalej len „ITVS") je v zákone o ITVS upravená v § 18 až § 23a. 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 ITVS zároveň aj PZS v zmysle ZoKB. V § 23 predmetného zákona sú upravené osobitné

[464] § 31 ods. 12 ZoKB.

opatrenia na úseku bezpečnosti ITVS (napr. bezpečnostný projekt, hlásenie kybernetických bezpečnostných incidentov).

Správcovia ITVS sú povinní identifikovať a realizovať potrebné bezpečnostné opatrenia a taktiež sú povinní hlásiť kybernetické bezpečnostné incidenty.[465]

V praxi môžu nastať situácie, kedy správca ITVS bude zároveň aj v postavení PZS podľa ZoKB. Z pohľadu správcu ITVS bude dôležité, aby vedel ktorý právny predpis má aplikovať pri prijímaní konkrétnych bezpečnostných opatrení. V zmysle § 18 ods. 2 zákona o ITVS platí, že:

> *„Správca, ktorý je prevádzkovateľom základnej služby, prijíma a realizuje bezpečnostné opatrenia k informačnej technológii verejnej správy podľa tohto zákona a aj v rozsahu a za podmienok podľa osobitného predpisu..[20]).*"

Osobitným predpisom je ZoKB s odkazom na § 20 ods. 4.

Z predmetného ustanovenia vyplýva, že ZoITVS a jeho príslušná vyhláška č. 179/2020 Z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy predstavujú **sektorovú právnu úpravu**, pričom regulované subjekty, ktoré sú v dvoch právnych postaveniach musia prijímať a realizovať bezpečnostné opatrenia v rozsahu a za podmienok podľa § 20 ods. 4 ZoKB.

PRÍKLAD
Štatistický úrad Slovenskej republiky je správcom ITVS v zmysle zákona o ITVS, nakoľko je správcom integrovaného volebného informačného systému.[466] Štatistický úrad Slovenskej republiky je zároveň aj PZS a PKZS v zmysle ZoKB, nakoľko bol zaradený do registra PZS.

V súvislosti s povinnosťou **hlásiť kybernetické bezpečnostné incidenty** platí, že správcovia ITVS sú v zmysle ZoITVS povinní nahlasovať každý kybernetický bezpečnostný incident vládnej jednotke CSIRT. Pri pojme kybernetický bezpečnostný incident sa vychádza z pojmu definovanom v ZoKB v mysle ustanovenia § 3 ods. 1 písm. m).

[465] Obsah bezpečnostných opatrení je upravený vo vyhláške Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.
[466] Dostupné na: https://metais.vicepremier.gov.sk/

V prípade ak je správca ITVS zároveň aj PZS podľa ZoKB, nahlasuje popri kybernetických bezpečnostných incidentoch v zmysle ZoITVS aj závažné kybernetické bezpečnostné incidenty v zmysle ZoKB.

V prípade porušenia povinností na úseku bezpečnosti informačných technológií verejnej správy podľa § 19 až 21, § 23 alebo § 23a zákona o ITVS, môže MIRRI v závislosti od spáchania konkrétneho **správneho deliktu** uložiť správcovi ITVS pokutu od 500 eur do 35 000 eur.[467]

Medzi ďalšie právne predpisy, ktoré čiastkovo upravujú problematiku kybernetickej bezpečnosti možno zaradiť zákon č. 367/2024 Z. z. o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov (ďalej len „**zákon o kritickej infraštruktúre**"). Predmetný zákon upravuje nový právny rámec ochrany a odolnosti kritickej infraštruktúry, teda subjektov poskytujúcich základné služby významné pre fungovanie štátu a spoločnosti. Stanovuje pôsobnosť vlády, Ministerstva vnútra SR a sektorových ústredných orgánov, postup identifikácie kritických subjektov a kritických subjektov osobitného európskeho významu, ich povinnosti pri posudzovaní rizík, prijímaní bezpečnostných a organizačných opatrení, oznamovaní incidentov, ochrane limitovaných informácií, ako aj pravidlá kontroly, auditu a sankcií. Zákon o kritickej infraštruktúre kladie dôraz na prevenciu, pripravenosť, reakciu a obnovu po incidentoch, pričom výslovne chápe „odolnosť" ako schopnosť incidentom predchádzať, chrániť sa pred nimi, reagovať na ne, zmierňovať ich dopady a zotaviť sa z nich.

Každý subjekt, ktorý je v zmysle zákona o kritickej infraštruktúre identifikovaný ako kritický subjekt je v zmysle ZoKB zároveň aj PZS.[468]

Poskytovanie základnej služby kritickým subjektom je zmysle ZoKB považované za kritickú základnú službu.[469]

[467] § 29 ods. 1 písm. a) zákona o ITVS.
[468] § 17 ods. 1 písm. b) ZoKB.
[469] § 18 ods. 1 písm. h) ZoKB.

6. OCHRANA SÚKROMIA V KONTEXTE (KYBERNETICKEJ) BEZPEČNOSTI

Kybernetická bezpečnosť patrí medzi najaktuálnejšie výzvy digitálnej doby a predstavuje akýsi „test" pre právo na súkromie. Bezpečnostné opatrenia v kybernetickom priestore – od monitorovania sieťovej prevádzky až po masový zber dát – často narážajú na hranice práva na súkromie a vo všeobecnosti na hranice súkromia, ako hodnoty hodnej právnej ochrany z pohľadu základných práva slobôd.

Tradičný naratív stavia súkromie a bezpečnosť do pozície vzájomného konfliktu (*„privacy vs. security"*) na téze, že posilnenie bezpečnosti nevyhnutne znamenalo oslabenie súkromia. Tento prístup však čelí čoraz silnejšej kritike: moderné právne rámce zdôrazňujú, že súkromie a bezpečnosť nemusia byť v konflikte. Naopak, primerane nastavené bezpečnostné opatrenia dokážu chrániť spoločnosť pred hrozbami bez toho, aby neprimerane obetovali základné práva. Práve kybernetická bezpečnosť testuje, či právny poriadok vie nájsť rovnováhu: zaistiť digitálnu odolnosť a zároveň uchovať podstatu práva na súkromie.[470]

Kybernetický priestor má vlastnosti, ktoré **znásobujú dosah** bezpečnostných zásahov do súkromia. **Škálovateľnosť** technológií umožňuje sledovať a zbierať údaje o miliónoch ľudí takmer v reálnom čase. **Automatizácia** a pokročilé systémy AI dokážu z analyzovaných dát odhaľovať vzorce správania a predikovať citlivé informácie o jednotlivcoch. Osobitnú pozornosť si zaslúžia **metaúdaje** – údaje o komunikáciách (napr. čas, dĺžka a účastníci hovoru či emailu) a o využívaní sietí. Hoci neobsahujú obsah komunikácie, vďaka **agregácii** obrovského množstva záznamov umožňujú zostaviť detailný obraz o živote jednotlivca. Ako zdôraznil Európsky súd pre ľudské práva (ESĽP) aj Súdny dvor EÚ (SDEÚ), **metadáta môžu byť rovnako citlivé a odhaľujúce ako samotný obsah** komunikácie.[471]

V kybernetickom priestore je bežný aj **sieťový efekt**: informácie z rôznych zdrojov sa dajú prepájať a hromadne vyhľadávať, čím stúpa riziko tzv. *profilovania* jednotlivcov. Tieto špecifiká spôsobujú, že opatrenia kybernetickej bezpečnosti (napríklad globálne

[470] K diskusií pozri napríklad https://www.edps.europa.eu/data-protection/data-protection_en#:~:text=The%20rights%20to%20privacy%20and,AFSJ.

[471] SDEÚ, spojené veci C-293/12 a C-594/12, *Digital Rights Ireland Ltd a Kärntner Landesregierung*, rozsudok z 8. 4. 2014.

monitorovanie prevádzky internetu alebo dlhodobá retencia prevádzkových údajov) dokážu zasiahnuť súkromie oveľa širšie a hlbšie než tradičné, analógové formy dohľadu.

6.1 Súkromie a bezpečnosť: klasický konflikt

Ochrana súkromia v súčasnej dobe čelí zásadnej výzve. Technologický rozvoj umožňuje systematické, plošné a preventívne formy sledovania, ktoré presahujú tradičné predstavy o zásahu do súkromia ako o výnimočnom policajnom opatrení voči konkrétnej osobe. Štúdie venujúce sa sledovaniu a dohľadu (tzv. *surveillance studies*) predstavujú interdisciplinárny smer, ktorý analyzuje spoločenské, politické a širšie dôsledky sledovania. Ich význam pre právo spočíva v tom, že:

- identifikujú štrukturálne riziká dohľadu, ktoré nie sú vždy reflektované individuálnymi právnymi prostriedkami v konkrétnych konaniach,
- poukazujú na dlhodobé a systémové účinky sledovania na demokraciu, právny štát a základné ľudské práva a slobody,
- umožňujú lepšie pochopiť, prečo určité zásahy do súkromia ohrozujú samotné základy právneho štátu, aj keď sú formálne odôvodňované bezpečnosťou.

Z právneho hľadiska nejde o nahradenie doktríny základných práv sociologickou analýzou, ale o jej obohatenie. Mnohé závery z predmetných štúdií sa postupne premietli do judikatúry ESĽP a SDEÚ.

Kľúčové poznatky z interdisciplinárnych štúdií menujú nasledujúce riziká a dilemy v kontext bezpečnosti a súkromia:

- Falošný naratív „kompromisu" pri otázkach bezpečnosti a súkromia,
- Odstrašujúce účinky sledovania (chilling effect),
- Sledovanie, profilovanie a sociálny skóring,
- Rozširovanie funkcií: od cieleného používania k hromadnému sledovaniu (*function creep*),
- Spoločné systémy sledovania – prepojene štátu a súkromných firiem, a
- Preventívna bezpečnosť a rizikové sledovanie.

6.1.1 Falošný naratív „kompromisu" pri otázkach bezpečnosti a súkromia

Literatúra v oblasti sledovania deklaruje, že rámcovanie súkromia a bezpečnosti ako kompromisu s „nulovým súčtom" (*zero sum*) je príliš zjednodušujúce a dokonca manipulatívne. Po teroristických útokoch z 11. septembra 2001 vlády propagovali masové sledovanie ako „cenu", ktorú treba zaplatiť za bezpečnosť. Kritici poukazujú na to, že uvedené zjednodušenie ignoruje kľúčové a zložité aspekty vzťahu medzi súkromím a bezpečnosťou. Hrozby ako terorizmus môžu byť obohnané „politikou strachu", ktorá odvádza pozornosť od iných rizík, a prehliada symbiózu verejného a súkromného sledovania, v rámci ktorej sú osobné údaje komodifikované spoločnosťami a využívané štátmi na iné účely. Napríklad komerčný „kapitalizmus sledovania" rutinne sleduje správanie za účelom zisku a často spolupracuje so štátnym sledovaním – priemyselným komplexom sledovania, ktorý stiera hranice medzi bezpečnosťou a obchodom.[472] Známy škandál so špionážnym softvérom Pegasus ukázal, že súkromné spoločnosti umožňujú štátom hackovať aktivistov a novinárov pod záštitou boja proti terorizmu. Štúdie o sledovaní preto odmietajú myšlienku, že musíme „obetovať" súkromie v záujme bezpečnosti, a naliehajú na podrobnejšiu analýzu nákladov a prínosov, ktorá zohľadňuje skutočné náklady na súkromie, neisté bezpečnostné prínosy a komerčné záujmy, ktoré sú v hre.[473]

PRÍKLAD

V kontexte práva na súkromie sa predmetný konflikt prejavuje v prísnych testoch nevyhnutnosti a proporcionality, predstavujúcich protipól akceptovania všeobecného kompromisu. ESĽP aj SDEÚ trvajú na tom, aby zásahy do súkromia boli „nevyhnutné v demokratickej spoločnosti" alebo „prísne nevyhnutné" na uspokojenie naliehavej spoločenskej potreby. Vyžadujú sa konkrétne odôvodnenia, že opatrenie skutočne dosahuje bezpečnostné ciele a nestačia menej invazívne alternatívne prostriedky.

[472] Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (Profile Books 2019).

[473] Bližšie k tejto diskusií pozri napríklad Daniel J Solove, Nothing to Hide: The False Tradeoff between Privacy and Security (Yale University Press 2011) alebo David E Pozen, 'Privacy–Privacy Tradeoffs' (2016) 83(1) University of Chicago Law Review 221.

6.1.2 Odstrašujúce účinky sledovania (chilling effect)

Dobre zdokumentovaným dôsledkom všadeprítomného sledovania je „odstrašujúci účinok" (tzv. *chilling effect*) na individuálne správanie, prejavy a združovanie sa. Štúdie o sledovaní ukazujú, že keď ľudia vedia (alebo tušia), že štát monitoruje ich komunikáciu a činnosti, často sa autocenzurujú a vyhýbajú sa uplatňovaniu svojich práv, čo podkopáva otvorenú diskusiu a demokraciu.[474] Výskum v rôznych kontextoch potvrdzuje, že sledovanie má odstrašujúci účinok na slobodu prejavu. Novinári môžu váhať s kontaktovaním zdrojov, aktivisti sa môžu vyhýbať organizovaniu sa online a bežní občania sa môžu vyhýbať citlivým vyhľadávaniam alebo diskusiám.[475]

Tento účinok môže poškodiť úlohu občianskej spoločnosti a tlače ako „verejného strážcu". Inými slovami, masové sledovanie môže narušiť práve tie slobody, ktoré má pôvodne chrániť.

PRÍKLAD

Právo na súkromie sa prelína so slobodou prejavu a slobodou združovania, osobitne pri sledovaní jednotlivcov. ESĽP výslovne uznáva odstrašujúce účinky ako ujmu, ktorú je potrebné zvážiť. Napríklad v rozsudku *Big Brother Watch a iní proti Spojenému kráľovstvu* (Veľká komora, 25. mája 2021) súd konštatoval porušenie práva na slobodu prejavu, pretože režim sledovania neposkytoval dostatočné záruky pre novinárov, čo ich mohlo odrádzať od komunikácie so zdrojmi. Súd konštatoval, že nedostatočná ochrana dôverných komunikácií novinárov „ohrozuje funkciu verejného strážcu" tlače. Podobne aj skupiny občianskej spoločnosti, ktoré sú predmetom rozsiahleho sledovania, čelia obmedzovaniu slobody prejavu a presadzovania spoločenských záujmov.

6.1.3 Sledovanie, profilovanie a sociálny skóring

Štúdie o sledovaní diskutujú aj sociálny skóring a následnú klasifikáciu jednotlivcov. Tento koncept stojí na myšlienke, že systémy sledovania triedia populáciu do kategórií s

[474] Napríklad Jonathon W Penney, 'Chilling Effects: Online Surveillance and Wikipedia Use' (2016) 31(1) Berkeley Technology Law Journal 117.

[475] K tomu Elizabeth Stoycheff, 'Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring' (2016) 93(2) Journalism & Mass Communication Quarterly 296. Daragh Murray, 'The Chilling Effect of Surveillance under the European Convention on Human Rights' (2024) 26(1) Journal of Human Rights Practice 1. Suneal Bedi, 'The Myth of the Chilling Effect' (2021) 34(3) Harvard Journal of Law & Technolog, Volume 35, Number 1 Fall 2021.

rozdielnou hodnotou alebo rizikom, čím často posilňujú existujúce predsudky. David Lyon a ďalší ukazujú, že moderné sledovanie (od čerpania alebo dolovania údajov po umelú inteligenciu) nezaobchádza so všetkými rovnako. Na základe údajov vytvára profily jednotlivcov, aby bolo rozhodnuté, kto si zaslúži väčšiu pozornosť alebo podozrenie.[476] Táto automatizovaná diskriminácia môže mať hlboký vplyv na šance v živote. Napríklad policajná činnosť založená na údajoch sa môže neprimerane zameriavať na štvrte, kde bývajú národnostné menšiny, alebo AI systémy môžu označiť jednotlivcov za „vysoko rizikových" na základe nejasných kritérií. Sociálne triedenie stiera hranicu medzi sociálnou kontrolou a verejnou bezpečnosťou, čím vyvoláva otázky sociálnej spravodlivosti nad rámec samotného súkromia. Ako poznamenáva Lyon, sledovanie nie je len otázkou osobného súkromia, ale aj sociálnej spravodlivosti, pretože môže vytvárať hlbokú diskrimináciu tým, že rozlišuje, kto je sledovaný alebo komu sa dôveruje.[477] V praxi to znamená, že určité skupiny často znášajú väčšiu mieru zvýšeného sledovania, ak sú klasifikované ako „riziková" časť populácie, zatiaľ čo iné unikajú kontrole.

PRÍKLAD

Z právneho hľadiska sa tieto obavy prejavujú v princípoch antidiskriminácie a ochrany údajov. Hoci právo na súkromie a zákaz diskriminácie výslovne nespomínajú „sociálny skóring", ESĽP v tejto otázke niekoľkokrát judikoval. V rozsudku *S. a Marper proti Spojenému kráľovstvu* (Veľká komora, 4. decembra 2008) súd zrušil plošné uchovávanie profilov DNA podozrivých osôb, ktoré nikdy neboli odsúdené za trestné činy. Okrem porušenia súkromia súd konštatoval, že táto politika vytvárala „nežiaduce stigmy" pre nevinných ľudí, ktorí boli považovaní za večných podozrivých.

6.1.4 Rozširovanie funkcií: od cieleného používania k hromadnému sledovaniu (function creep)

Rozširovanie funkcie a účelov (*function creep*) sa týka postupného rozširovania nástrojov sledovania nad rámec jeho pôvodného účelu . Štúdie o sledovaní poukazujú na to, ako sa opatrenia zavedené na obmedzený, legitímny účel (napr. boj proti terorizmu) často

[476] David Lyon (ed), Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination (Routledge 2003).
[477] David Lyon, 'Surveillance, Security and Social Sorting: Emerging Research Priorities' (2007) 17(1) International Criminal Justice Review 161.

vyvinú do širšieho použitia.[478] Napríklad sieť dopravných kamier určená na zachytávanie vodičov porušujúcich pravidlá povolenej rýchlosti sa neskôr môže použiť na sledovanie nepoistených vodičov, potom na všeobecné presadzovanie práva, pričom každý krok rozširuje rozsah sledovania. Toto rozširovanie môže byť nepostrehnuteľné, avšak podkopáva očakávania v oblasti súkromia. Literatúra poukazuje na to, že v prostredí strachu (napr. z terorizmu alebo zločinu) orgány často využívajú údaje na účel bezpečnosti a nakoniec zaobchádzajú s každým ako s potenciálnym podozrivým. Nebezpečenstvo spočíva v tom, že dočasné mimoriadne právomoci alebo konkrétne zbierky údajov sa menia na trvalú, univerzálnu sledovaciu infraštruktúru. Rozširovanie funkcií narúša dôveru a to takým spôsobom, že údaje zhromaždené z jedného dôvodu sa nakoniec používajú na iné účely bez vedomia verejnosti a bez verejného dohľadu.[479]

PRÍKLAD
Z právneho hľadiska sa funkčné rozširovanie rieši prostredníctvom obmedzenia účelu a požiadaviek predvídateľnosti. Z dikcie ustanovení chrániacich právo na súkromie vyplýva požiadavka „v súlade so zákonom", na základe ktorej musia mať sledovacie opatrenia jasné, predvídateľné pravidlá týkajúce sa rozsahu a používania údajov, čím sa zabráni nekontrolovanému rozširovaniu dôvodov a účelov sledovania.

6.1.5 Spoločné systémy sledovania – prepojene štátu a súkromných firiem

Moderné sledovanie je zriedka len činnosťou štátu, keďže ide skôr o súbor verejných a súkromných opatrení a postupov. Štúdie o sledovaní opisujú „participatívne panoptikum", kde jednotlivci zdieľajú obrovské množstvo údajov prostredníctvom sociálnych médií, ako aj verejno-súkromné partnerstvo v oblasti sledovania, kde štátne bezpečnostné agentúry využívajú tieto údaje.[480] Od telekomunikačných spoločností, ktoré uchovávajú metadáta zákazníkov pre spravodajské služby, až po technologické spoločnosti, ktoré zostavujú podrobné profily, ku ktorým majú prístup vlády, sa hranice medzi štátnym a súkromným dohľadom stierajú. Koncept sledovacieho kapitalizmu, ktorý opísala Shoshana Zuboff,

[478] Bert-Jaap Koops, 'The Concept of Function Creep' (2021) 24(4) Information, Communication & Society 538 alebo Sarah Brayne, 'Big Data Surveillance: The Case of Policing' *American Sociological Review*, *82*(5), 977-1008. https://doi.org/10.1177/0003122417725865 .

[479] Tamže.

[480] Kevin D Haggerty and Richard V Ericson, 'The Surveillant Assemblage' (2000) 51(4) British Journal of Sociology 605.

zdôrazňuje, že spoločnosti sledujú používateľov s cieľom dosiahnuť zisk, čím v podstate vytvárajú úložisko údajov, ktoré štáty radi využívajú.[481]

PRÍKLAD
Zo zákonného hľadiska sa štát nemôže vyhnúť svojim povinnostiam v oblasti ľudských práv tým, že koná prostredníctvom súkromných subjektov alebo v spolupráci s nimi. Podľa článku 8 Dohovoru, ak vláda núti spoločnosti zbierať alebo odovzdávať údaje, tento zásah musí spĺňať rovnaké normy nevyhnutnosti a zákonnosti. Napríklad povinné uchovávanie údajov poskytovateľmi internetových služieb bolo súdmi efektívne považované za štátny dohľad. Súdny dvor Európskej únie vo veci *C-203/15 a C-698/15, Tele2 Sverige a Watson* rozhodol, že vnútroštátne právne predpisy, ktoré vyžadujú, aby telekomunikačné spoločnosti všeobecne uchovávali metadáta používateľov pre prístup orgánov presadzovania práva, porušujú základné práva a slobody.

6.1.6 Preventívna bezpečnosť a rizikové sledovanie

Dominantnou logikou po 11. septembri 2021 je preventívna bezpečnosť v podobe predvídania a predchádzania rizikám skôr, ako sa prejavia. Teória poukazuje na vznikajúci paradigmu „predchádzania zločinu" – orgány využívajú rozsiahle sledovanie a analýzu údajov na proaktívne identifikovanie hrozieb, namiesto čakania na individuálne podozrenia. To zahŕňa hodnotenie rizík, úrovne hrozieb a „vyhľadávanie" informácií prostredníctvom hromadných údajov s cieľom nájsť anomálie[482]. Hoci je táto logika v niektorých prípadoch potenciálne účinná, narúša tradičné chápanie kľúčových inštitútov právneho poriadku. Namiesto toho, aby sa vychádzalo z dôkazov alebo podozrenia z protiprávneho konania, zhromažďujú sa údaje o všetkých osobách pre prípad, že by mohli odhaliť budúcu hrozbu. Lucia Zedner a ďalší varujú, že tento preventívny prístup môže podkopať prezumpciu neviny a normalizovať hromadný dohľad, pretože sa zaoberá tým, že všeobecnú populáciu považuje za podozrivú.[483]

[481] Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (Profile Books 2019).
[482] Claudia Aradau, 'Governing Terrorism Through Risk: Taking Precautions, (Un)Knowing the Future' (2007) 28(1) European Journal of International Relations 89.
[483] Lucia Zedner, 'Pre-Crime and Post-Criminology?' (2007) 11(2) Theoretical Criminology 261.

PRÍKLAD
Preventívne sledovanie testuje hranice proporcionality a demokratickej nevyhnutnosti. ESĽP uznal legitimitu proaktívneho spravodajstva v záujme národnej bezpečnosti, ale vyžaduje dôkladné kontroly. V prípade Klass (1978) súd uznal, že demokratické spoločnosti môžu potrebovať prijať [tajné] opatrenia na boj proti špionáži a terorizmu, čím v podstate podporil prevenciu, ale zároveň varoval, že neobmedzené sledovanie by zničilo demokraciu pod zámienkou jej ochrany. Preto aj v oblasti prevencie vyžaduje právo obmedzenia: predchádzajúce povolenie, transparentnosť, dohľad a následné opravné prostriedky na zabránenie zneužívaniu.

6.2 Právo na súkromie v kontexte kybernetickej bezpečnosti

Základné mantinely ochrany súkromia v kontexte kybernetickej bezpečnosti sú v Európe vymedzené **duálnym právnym rámcom** – systémom Rady Európy (najmä **Európsky dohovor o ľudských právach**, EDĽP) a právom Európskej únie (Charta základných práv EÚ a sekundárne predpisy, napr. GDPR, ePrivacy smernica). Obe tieto roviny poskytujú právo na súkromie, no s určitými špecifikami v rozsahu a teste pri jeho obmedzovaní.

Článok 8 EDĽP garantuje každému právo na **rešpektovanie súkromného a rodinného života, obydlia a korešpondencie**.[484] Ide o široko koncipované právo, ktoré pokrýva okrem iného aj **komunikačné súkromie** (tajomstvo listov, hovorov, elektronickej komunikácie) a **informačné súkromie** (ochranu osobných údajov). Do práva podľa čl. 8 môže štát zasiahnuť len za prísnych podmienok: zásah musí byť **v súlade so zákonom**, sledovať niektorý z vymenovaných **legitímnych cieľov** (napr. národná bezpečnosť, verejná bezpečnosť, predchádzanie zločinnosti atď.) a byť **nevyhnutný v demokratickej spoločnosti** (primeraný). Judikatúra ESĽP tieto kritériá ďalej rozvinula do detailných **doktrinálnych prvkov**.[485]

Lisabonská zmluva a Charta základných práv EÚ výrazne posilnili ochranu súkromia na úrovni Únie. Charta obsahuje **dve samostatné ustanovenia**:

- **článok 7** (právo na súkromný a rodinný život, obydlie, a komunikáciu) a
- **článok 8** (právo na **ochranu osobných údajov**).

[484] EDĽP, článok 8.

[485] Ako príklad možno uviesť požiadavky kvality zákona, test proporcionality a tzv. *margin of appreciation* (v preklade určitá „miera voľnej úvahy" štátov pri napĺňaní Dohovoru).

Čl. 7 je obsahovo rovnocenný s čl. 8 EDĽP; dokonca Charta nahradila pojem „korešpondencia" modernejším slovom „komunikácie." Podľa čl. 52 ods. 3 Charty platí, že význam a rozsah práva podľa čl. 7 sú rovnaké ako podľa EDĽP. Oproti tomu čl. 8 Charty zavádza osobitné právo na ochranu osobných údajov so špecifickými komponentmi: zaručením ochrany osobných údajov jednotlivcov a ich spravodlivého spracúvania, vymedzenie účelu a právneho základu spracúvania, práva jednotlivca na prístup a opravu údajov a požiadavka nezávislého dozoru nad dodržiavaním týchto pravidiel.[486] Toto **dvojkoľajné poňatie** (súkromie vs. ochrana údajov) odráža rozdiely medzi týmito dvoma právami: súkromie (čl. 7) je širší pojem zahŕňajúci aj priestorové a rodinné aspekty, kým ochrana osobných údajov (čl. 8) sa sústredí na pravidlá zaobchádzania s osobnými informáciami.[487] V praxi sú však tieto práva úzko prepojené a navzájom sa posilňujú. SDEÚ preto opakovane zdôrazňuje, že **nezávislý dohľad** je neoddeliteľnou súčasťou práva na ochranu údajov a že obmedzenie týchto práv možno pripustiť len za podmienok čl. 52 ods. 1 Charty.

PRÍKLAD

Všetky obmedzenia výkonu práv podľa Charty musia byť zákonné, rešpektovať podstatu (esenciu) daného práva a pri zachovaní princípu proporcionality môžu byť prijaté len ak sú nevyhnutné a skutočne zodpovedajú cieľom všeobecného záujmu uznaným EÚ alebo potrebe ochrany práv iných.

Uplatnenie tohto testu je v praxi evidentné aj pri posudzovaní kyber-bezpečnostných opatrení. Ak napríklad legislatíva prikazuje hromadné uchovávanie komunikačných údajov, Súdny dvor skúma, či nezasahuje do samotnej podstaty práva napr. či neumožňuje prístup aj k obsahu komunikácie, čo by bolo obzvlášť závažné, a či je takáto plošné uchovávanie údajov skutočne nevyhnutné na dosiahnutie deklarovaného cieľa.

[486] V podmienkach Slovenskej republiky Úrad na ochranu osobných údajov SR.

[487] K vzťahu pozri napríklad EUROPEAN DATA PROTECTION SUPERVISOR. Study on the Essence of the fundamental rights to privacy and to the protection of personal data. https://www.edps.europa.eu/data-protection/our-work/publications/papers/2023-11-08-study-essence-fundamental-rights-privacy-and-protection-personal-data_en alebo Duncan, Jamie (2023). Data protection beyond data rights: governing data production through collective intermediaries . Internet Policy Review,[online] 12(3). Available at: https://policyreview.info/articles/analysis/data-protection-beyond-data-rights [Accessed: 5 Jan. 2026] alebo Alafaa, Princess, Data Privacy and Data Protection: The Right of User's and the Responsibility of Companies in the Digital World. (January 7, 2022). Available at SSRN: https://ssrn.com/abstract=4005750 or http://dx.doi.org/10.2139/ssrn.4005750.

PRÍKLAD

Hoci oba európske súdy uplatňujú podobné testy proporcionality, v praxi existujú rozdiely v ich prístupe. SDEÚ spravidla vykonáva prísnejší prieskum zásahov, najmä ak ide o plošné opatrenia ohrozujúce podstatu práva alebo slobôd viacerých osôb. Zavádza koncept *„strict necessity"* – štát musí preukázať, že dané opatrenie je skutočne nevyhnutné a nemožno ho nahradiť miernejším alternatívnym prostriedkom. Taktiež kladie dôraz na podstatu (*essence*) práva: ak by ho opatrenie porušilo, nie je prípustné vôbec.

Naproti tomu ESĽP tradične priznáva štátom určitú voľnú úvahu, najmä v otázkach národnej bezpečnosti a boja proti terorizmu. To znamená, že do istej miery akceptuje rôzne národné riešenia, pokiaľ však spĺňajú minimálne európske štandardy (napr. existenciu základných záruk proti zneužitiu). Klasickým príkladom je prípad *Klass proti Nemecku* (1978), kde ESĽP uznal, že Nemecko môže nasadiť tajný sledovací systém v záujme národnej bezpečnosti, avšak iba ak je „nevyhnutný v demokratickej spoločnosti" a obsahuje primerané kontroly zneužitia. Inými slovami, národná bezpečnosť nepôsobí ako "magická výnimka", ktorá by zbavovala štáty povinnosti rešpektovať právo na súkromie, ale ESĽP im priznáva širší priestor na uváženie, ako konkrétne tieto požiadavky splniť.

6.2.1 Zásahy do práva na súkromie v kybernetickej bezpečnosti

Ak hovoríme o ochrane súkromia v kontexte kyber-bezpečnostných opatrení, je potrebné vymedziť, čo sa považuje za „zásah do súkromia". Z pohľadu práva (či už EDĽP alebo Charty EÚ) predstavuje zásah do práva na súkromie *akákoľvek* činnosť štátu alebo aj súkromného subjektu, ktorá ovplyvňuje súkromný život jednotlivca alebo spracúva jeho osobné údaje. Z tohto dôvodu musí mať oporu v právnom poriadku a podlieha testu proporcionality. V digitálnej ére sem spadá niekoľko situácií, ktoré načrtneme nižšie.

Monitorovanie sietí a komunikácií je jedným z najčastejších príkladov. Zaradiť do tejto kategórie môžeme odpočúvanie alebo záznam obsahu komunikácie (telefonáty, e-maily), ale aj sledovanie samotnej prevádzky v sieti (network monitoring). Príkladom kyber-bezpečnostného opatrenia je inštalácia sond analyzujúcich dátové toky v sieti za účelom odhalenia útokov. Už samotné zachytávanie a prehliadanie paketov alebo inšpekcia

hlavičkových informácií o spojeniach predstavuje zásah do „korešpondencie" a „súkromia" v zmysle čl. 8 EDĽP.[488]

PRÍKLAD

ESĽP v prípade Copland proti Spojenému kráľovstvu jasne uviedol, že aj monitoring telefonátov, e-mailov či internetovej aktivity zamestnanca (v práci) napĺňa pojem zásahu do súkromia – a to dokonca aj vtedy, ak ide len o sledovanie údajov o komunikácii (napr. čísla volaných účastníkov, dĺžka hovorov) bez monitorovania obsahu Takéto metadáta sú totiž integrálnou súčasťou komunikácie a požívajú rovnakú ochranu ako obsah hovoru.

Logovanie a retencia údajov je ďalším príkladom. Mnohé predpisy v oblasti kybernetickej bezpečnosti alebo elektronických komunikácií ukladajú povinnosť uchovávať prevádzkové a lokalizačné údaje o komunikáciách pre potreby vyšetrovania incidentov či trestných činov. Takéto plošné uchovávanie (napr. archivácia telefónnych záznamov, IP adries, histórie pripojení) bola predmetom viacerých kľúčových rozsudkov.

PRÍKLAD

SDEÚ v *Digital Rights Ireland* konštatoval, že ukladanie údajov o elektronickej komunikácii miliónov osôb predstavuje „široký a obzvlášť závažný zásah" do súkromia, ktorý môže u ľudí vyvolávať pocit neustáleho sledovania. Preto takéto opatrenia podliehajú prísnemu testu nevyhnutnosti. Samotný fakt, že štát nezískava obsah správ, ešte neznamená absenciu zásahu – uchovávanie metadát je zásahom do práva na súkromie aj podľa Charty EÚ (čl. 7 a 8).

Automatizovaná analýza a detekcia hrozieb je ďalšou ilustráciou pnutia medzi ochranou súkromia a kybernetickou bezpečnosťou. Moderné kyberbezpečnostné systémy často fungujú na princípe **automatizovaného vyhodnocovania rizík**. Analyzujú veľké dáta (napríklad z logov, sieťovej prevádzky či z otvorených zdrojov) a hľadajú znaky prieniku, anomálie alebo podozrivé vzorce (tzv. *threat intelligence*). Pokiaľ sú pri tom spracúvané osobné údaje (napr. IP adresy, používateľské účty, komunikačné vzorce konkrétnych osôb), ide opäť o zásah do súkromia. **Profilovanie** osôb na základe automatickej analýzy môže

[488] ESĽP, *Copland proti Spojenému kráľovstvu*, č. 62617/00, rozsudok z 3. 4. 2007.

spadať pod ochranu súkromia aj ochranu údajov súčasne. V praxi sem patria napríklad systémy na **detekciu botnetov** u poskytovateľov internetových služieb (ISP) alebo **skenovanie súborov** pri kyberincidentoch v organizácii – oboje zasahujú do súkromných dát používateľov, hoci je cieľom ochrana systémov.

Osobitnú kategóriu predstavujú **tajné sledovacie opatrenia** (napríklad utajené odpočúvanie, bulk surveillance – hromadné sledovanie medzinárodných dátových tokov spravodajskými službami a pod.).[489] V týchto prípadoch práve absencia vedomia dotknutej osoby o predmetnej aktivite zosilňuje zásah, pretože osoba nemá možnosť sa brániť či prispôsobiť svoje konanie. Hromadné spracúvanie osobných údajov rovnako zvyšuje závažnosť zásahu, najmä ak je plošné a zamerané na všeobecnú populáciu.

PRÍKLAD

ESĽP v konaní *Big Brother Watch a iní proti Spojenému kráľovstvu* (Veľká komora, 25. mája 2021) zdôraznil, že automaticky nemožno považovať metadáta za menej citlivé než obsah – ich masový zber bez rovnakých záruk by bol neakceptovateľný. Vo všeobecnosti teda platí: čím širší a tajnejší zásah, tým vyššie nároky kladie právo na jeho zdôvodnenie a limitáciu.

6.2.2 Legitímne ciele a verejný záujem v oblasti kybernetickej bezpečnosti pri zásahu do práva na súkromie

Každý zásah do súkromia musí slúžiť legitímnemu cieľu – ide o výpočet cieľov uvedený v čl. 8 ods. 2 EDĽP (a podobne v čl. 52 ods. 1 Charty). V kontexte kybernetickej bezpečnosti štáty spravidla odôvodňujú zásahy účelmi diskutovanými nižšie.

Najčastejšie deklarovaným cieľom je **národná bezpečnosť.** Národná bezpečnosť predstavuje ochranu štátu pred kybernetickou špionážou, sabotážou kritických systémov, zahraničnými kybernetickými útokmi či terorizmom v online priestore. Do tejto kategórie legitímneho cieľa patrí napríklad odhaľovanie útočných operácií cudzích mocností, ochrana vojenskej a vládnej komunikačnej infraštruktúry a preventívne sledovanie potenciálnych hrozieb pre bezpečnosť štátu. Národná bezpečnosť je v EDĽP výslovne uvedeným

[489] K tomu napríklad Murray D, Fussey P. Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data. *Israel Law Review*. 2019;52(1):31-60. doi:10.1017/S0021223718000304.

legitímnym cieľom a v kybernetickom priestore nadobúda nový rozmer. Dôležité je však rozlišovať, kedy sa konkrétne opatrenie skutočne týka *národnej* bezpečnosti, a nie len všeobecnej kriminality či verejného poriadku – od toho sa odvíja režim kontroly (napr. zapojenie spravodajských služieb vs. polície) a pôsobnosť práva EÚ. Podľa čl. 4 ods. 2 Zmluvy o EÚ totiž národná bezpečnosť zostáva vo výlučnej zodpovednosti členských štátov; to však neznamená, že ak štát označí opatrenie nálepkou „národná bezpečnosť", uniká akýmkoľvek európskym pravidlám.[490]

PRÍKLAD

Ako rozhodol Súdny dvor EÚ vo veci *C-623/17, Privacy International* (6. októbra 2020), ak štát zaviaže súkromných poskytovateľov uchovávať alebo odovzdávať dáta na účely národnej bezpečnosti, stále sa uplatnia požiadavky práva EÚ (napr. pravidlá e-Privacy smernice a Charty).

Ďalším legitímnym cieľom je **verejná bezpečnosť a predchádzanie kriminalite.** Tento cieľ pokrýva širšie chápanú ochranu spoločnosti a obyvateľstva pred ohrozeniami, ktoré nemusia dosahovať úroveň „existenciálnej" národnej hrozby, ale týkajú sa udržania poriadku a bezpečia. Patria sem zásahy proti **kybernetickej kriminalite** (napr. finančné podvody, útoky ransomvéru na nemocnice), identifikácia páchateľov trestnej činnosti cez digitálne stopy, zabezpečenie verejného poriadku pri rozsiahlych kybernetických incidentoch atď. **Verejná bezpečnosť** je tiež uznaný legitímny cieľ (čl. 8 ods. 2 EDĽP hovorí o „verejnej bezpečnosti" a „predchádzaní neporiadku alebo zločinnosti"[491]). V praxi sa pojem verejnej bezpečnosti v tomto kontexte môže prekrývať s národnou bezpečnosťou – napríklad masívny kyberútok na energetickú sieť môže byť oboma naraz. Avšak z právneho hľadiska je dôležité rozlišovať nasledovné. Opatrenia definované ako súčasť presadzovania práva (*law enforcement*) spadajú pod iný režim (uplatní sa právo EÚ, napr. e-Privacy smernica, a dohľad súdov), kým ak ide čisto o spravodajské operácie pre národnú bezpečnosť, pristupuje sa k nim v EDĽP s väčšou voľnou úvahou štátu.

[490] K tomu bližšie pozri EUROPEAN DATA PROTECTION SUPERVISOR. Study on the Essence of the fundamental rights to privacy and to the protection of personal data. https://www.edps.europa.eu/data-protection/our-work/publications/papers/2023-11-08-study-essence-fundamental-rights-privacy-and-protection-personal-data_en.

[491] Ségolène Barbou des Places. Introduction: Public order and public security in EU law. Time for Reappraisal. European Papers, Vol. 9, 2024, No 3, pp. 1316-1328.

Ochrana práv iných osôb a kritickej infraštruktúry je ďalším z kľúčových legitímnych cieľov pre zásahy do práva na súkromie**.** Kybernetická bezpečnosť často sleduje aj cieľ chrániť **práva a slobody iných** napríklad právo občanov na život a telesnú integritu (ochrana nemocníc pred hackerským útokom), právo na ochranu majetku (prevencia podvodov) či dokonca ochranu súkromia samotných jednotlivcov (zabránenie únikom osobných údajov pri bezpečnostnom incidente). Rovnako ochrana **kritickej informačnej infraštruktúry** môže byť prezentovaná ako súčasť verejného záujmu.

Osobitnou kategóriou môže byť tzv. **kybernetická odolnosť (*resilience*).** Pojem kybernetická odolnosť možno chápať ako schopnosť systémov a spoločnosti odolať kybernetickým hrozbám a rýchlo sa zotaviť. Nie je to priamo definovaný právny termín v judikatúre. V zásade zahŕňa kombináciu vyššie uvedených cieľov. Ide o zabezpečenie kontinuity kritických služieb (verejný záujem) a posilnenie kapacít štátu i súkromných subjektov reagovať na útoky (čo slúži ochrane práv všetkých závislých od týchto služieb).

6.2.3 Požiadavky na zásahy do práva súkromie

6.2.3.1 Test zákonnosti a kvality práva

Podľa čl. 8 ods. 2 EDĽP nesmie byť do práva na súkromie zasahované. Výnimku tvoria prípady, v ktorých je to „v súlade so zákonom". ESĽP toto spojenie vykladá tak, že zásah musí mať oporu v domácom práve, pričom dotknuté právo musí byť pre občana dostatočne prístupné a predvídateľné v tom zmysle, že jednotlivec môže do rozumnej miery vedieť, za akých okolností a podmienok môže dôjsť k zásahu.

V kontexte utajených opatrení (ako je odpočúvanie) ESĽP uznáva, že absolútna predvídateľnosť nie je možná – jednotlivec nemusí vedieť dopredu, kedy konkrétne budú jeho komunikácie odpočúvané. Opačný prístup by popieral samotný účel odpočúvania. Predvídateľnosť sa preto chápe skôr ako požiadavka, aby zákon jasne a detailne vymedzil rozsah a spôsob výkonu sledovacích právomocí.[492] Práve preto ESĽP už v 80. rokoch formuloval potrebu, aby zákon obsahoval jasné pravidlá, vzhľadom na neustále sa zdokonaľujúce technológie sledovania.[493] V rozhodnutí o prijateľnosti *Weber a Saravia proti*

[492] ESĽP, *Weber a Saravia proti Nemecku*, č. 54934/00, rozhodnutie o prijateľnosti z 29. 6. 2006.
[493] Malone v. the United Kingdom, judgment of 2 August 1984, Series A no. 82, pp. 30-31, § 64 a Huvig v. France, judgment of 24 April 1990, Series A no. 176 B, p. 52, § 26.

Nemecku (29. júna 2006)[494] súd definoval minimálne požiadavky, ktoré musí zákon upravujúci tajné sledovanie obsahovať, aby obstál v teste diskutovanej požiadavky. Patria k nim najmä:

- vymedzenie povahy trestných činov alebo hrozieb, pri ktorých možno vydať príkaz na sledovanie;
- definícia kategórií osôb, ktoré môžu byť cieľom sledovania;
- limit trvania sledovania;
- postup pri zhodnocovaní, používaní a uchovávaní získaných dát;
- opatrenia pri poskytovaní údajov iným orgánom; a
- okolnosti, za ktorých sa má nezákonne získaný alebo nepotrebný materiál vymazať alebo zničiť.[495]

Tieto kritériá majú zabezpečiť, že zákon ponúka dostatočné záruky proti zneužitiu: ak by chýbali, hrozí „svojvoľný" zásah do súkromia, čo je v rozpore s princípmi právneho štátu.

ESĽP takisto trvá na **nezávislej kontrole** dodržiavania zákona. Už v požiadavke „kvality zákona" zdôrazňuje, že zákon musí predvídať mechanizmy kontroly nad vykonávaním tajných opatrení, aby nedochádzalo k excesom. Ak napríklad zákon zveruje právomoc povoliť odpočúvanie výlučne exekutíve bez účinného dohľadu, v takom prípade nemusí spĺňať štandardy „v súlade so zákonom" a takáto právna úpravav by bola nedostatočná. V rozsudku *Roman Zakharov proti Rusku* (Veľká komora, 4. decembra 2015) sa ESĽP v celom rozsahu venoval auditu ruských zákonov o sledovaní a dospel k záveru, že ruská legislatíva *ako celok* neposkytovala dostatočné záruky proti svojvôli a preto porušovala čl. 8.[496] Súd opakovane prízvukoval, že v prostredí, kde technológia umožňuje masový zásah, má mimoriadny význam, aby zákon jasne určoval rozsah oprávnení a aby nad ich výkonom bol nezávislý dohľad – či už *ex ante* (súdne povolenie) alebo aspoň *ex post* (kontrola komisiou alebo súdom).

Aj právo EÚ (najmä cez výklad e-Privacy smernice a Charty) stanovuje obdobné podmienky. Podľa Súdneho dvora musia opatrenia obmedzujúce súkromie a ochranu údajov byť ustanovené zákonom a tento zákon musí byť dostatočne presný a jasný, aby ľudia pochopili jeho dosah. Navyše, v oblastiach patriacich pod právo EÚ (ako spracúvanie

[494] ESĽP, *Weber a Saravia proti Nemecku*, č. 54934/00, rozhodnutie o prijateľnosti z 29. 6. 2006.
[495] Pre zhrnutie pozri napríklad ECtHR: When not backed by strong safeguards, mass surveillance violates privacy. Dostupné na: https://ccdcoe.org/incyder-articles/ecthr-when-not-backed-by-strong-safeguards-mass-surveillance-violates-privacy/.
[496] ESĽP, *Roman Zakharov proti Rusku*, č. 47143/06, rozsudok Veľkej komory z 4. 12. 2015.

osobných údajov alebo elektronické komunikácie) úniové právo explicitne vyžaduje, aby do ochrany súkromia zasahovali len zákony, ktoré obsahujú primerané záruky. Napríklad SDEÚ vo veci *C-203/15 a C-698/15, Tele2 Sverige a Watson* priamo uviedol, že právna úprava povoľujúca uchovávanie či prístup k údajom musí stanovovať jasné a precízne pravidlá, vymedzovať kategórie údajov, dotknuté osoby, trvanie uchovávania atď., a to všetko obmedziť na to, čo je striktne nevyhnutné.[497] Taktiež musí obsahovať bezpečnostné garancie proti zneužitiu – napr. povinnosť uchovávať dáta na území EÚ a po uplynutí lehoty ich nezvratne zničiť, obmedzenie prístupu len na boj proti závažnej kriminalite, presný postup vybavovania žiadostí o prístup, ako aj zavedený systém nezávislého dohľadu (*ex ante* alebo *ex post*) nad tým, ako sa k uchovaným údajom pristupuje.[498]

Súdny dvor EÚ vo spojených veciach *C-293/12 a C-594/12, Digital Rights Ireland* anuloval celú smernicu o uchovávaní údajov práve preto, že bola príliš vágna a neobsahovala potrebné limity. Právo EÚ teda kladie dôraz na to, aby právny základ nebol všeobecný a neobmedzený, ale precízny a cielený, inak opatrenie nie je v súlade s predmetnou požiadavkou.

6.2.3.2 Proporcionalita a nevyhnutnosť

Najnáročnejším krokom testu je posúdenie, či zásah do súkromia je primeraný a nevyhnutný vzhľadom na sledovaný legitímny cieľ. Práve tento aspekt predstavuje skutočné „jadro sporu" v debate o súkromí a kybernetickej bezpečnosti. Práve tu nachádzame najvýraznejšie rozdiely medzi prístupom ESĽP a SDEÚ, hoci základné princípy zdieľajú.

ESĽP skúma, či zásah odpovedá „naliehavej spoločenskej potrebe" a či je proporcionálny vo vzťahu k legitímnemu cieľu, pričom zvažuje aj existenciu menej rušivých prostriedkov. Zohľadňuje pritom voľnú úvahu štátov, pričom v oblasti národnej bezpečnosti je táto voľná úvaha štátov pomerne široká, no nie neobmedzená. Súd posudzuje celý kontext napríklad ak ide o plošné a cielené rozhranie. V rozsudku *Klass a iní proti Nemecku* (6. septembra 1978) súd toleroval tajné odpočúvanie komunikácií členov extrémistických skupín, pretože bolo cielené, viazané na legitímny cieľ ochrany demokracie a podliehalo nezávislým

[497] SDEÚ, spojené veci C-203/15 a C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen a Secretary of State for the Home Department v. Watson a i.*, rozsudok z 21. 12. 2016.
[498] Tamže.

kontrolám. Zároveň však varoval, že tajné sledovanie môže „podkopať samotnú demokraciu, ktorú má chrániť", ak by nebolo držané v medziach nevyhnutnosti.

V súčasnej dobe ESĽP čelil výzve masového sledovania. Rozsudok *Big Brother Watch a iní proti Spojenému kráľovstvu (Veľká komora, 25. mája 2021)* potvrdil, že hromadné zachytávanie medzinárodnej internetovej prevádzky nie je porušením EDĽP, pričom uznal, že v súčasnom prostredí môže byť pre národnú bezpečnosť významné. Súd však detailne skúmal záruky a vytkol Veľkej Británii nedostatky v zacielení, chýbajúcu nezávislú autorizáciu výberu cielenej komunikácie a nedostatočné pravidlá pre prístup k sekundárne získaným dátam, najmä metadátam. ESĽP tak trvá na tom, že aj v režime hromadného sledovania treba posúdiť proporcionalitu aj *ex post* a to v podobe, či mala implementácia dostatočné filtre, minimalizáciu zhromaždených údajov, odstraňovanie nepotrebných dát atď. Tam, kde chýbajú tzv. „minimálne požiadavky", spravidla deklaruje porušenie, lebo zásah nemožno považovať za nevyhnutný v demokratickej spoločnosti. Napríklad ESĽP v prípade *Szabó a Vissy proti Maďarsku*, č. 37138/14, rozsudok z 12. 1. 2016 rozhodol, že mimoriadne široké protiteroristické sledovacie právomoci v Maďarsku bez súhlasu súdu a s všeobecným povoľovaním od vlády porušili čl. 8, pretože nebolo preukázané, že by boli využívané v nevyhnutnej miere. V tomto prípade absentoval test nevyhnutnosti ako aj nezávislý dohľad. Hoci ochrana národnej bezpečnosti bol legitímnym cieľom, chýbali minimálne záruky proti zneužitiu, a ESĽP teda považoval opatrenie za neprimerané.

Súdny dvor EÚ zaujal vo veciach kyberbezpečnosti, najmä v otázke uchovávania a sprístupňovania telekomunikačných údajov, mimoriadne prísny meter. Vo veci *C-203/15 a C-698/15, Tele2 Sverige a Watson* SDEÚ jasne vyslovil, že všeobecná a nerozlišujúca povinnosť uchovávať dáta preventívne je v rozpore s požiadavkou nevyhnutnosti. Zdôraznil, že hoci uchovávané metadáta neodhaľujú obsah komunikácií, umožňujú vyvodiť veľmi presné závery o súkromnom živote osôb, a preto ani boj proti vážnej kriminalite sám osebe neospravedlňuje taký vážny zásah voči osobám, u ktorých nie je žiadne podozrenie. Inými slovami, neohraničené zásahy (bez cielenia na podozrivých či definované skupiny) porušujú princíp proporcionality.

Po rozsudkoch z roku 2020 (La Quadrature du Net a ďalšie) SDEÚ síce pripustil výnimky pre situácie vážnej hrozby národnej bezpečnosti, kde dočasne možno nariadiť plošné uchovávanie, avšak len pre prípady, ak ide o skutočnú a aktuálnu alebo predvídateľnú hrozbu, opatrenie je prísne časovo obmedzené a schváli ho nezávislý orgán. Rovnako

spresnil, že štáty môžu zaviesť cielené uchovávanie údajov na účely boja proti závažnej kriminalite, ak je ohraničené na objektívne vymedzené kategórie osôb alebo geografické oblasti a trvá len nevyhnutný čas.

Pri posudzovaní, či je konkrétne opatrenie proporcionálne, sa v rozhodnutiach opakovane objavujú určité kľúčové faktory, ktoré uvádzame nižšie v tabuľke.

Faktor	Charakteristika
Plošnosť vs. cielenosť	Zásadná otázka je, či opatrenie dopadá na všetkých (resp. veľmi široko) alebo je úzko mierené na konkrétnu hrozbu/osoby. Plošné, všeobecné opatrenia (napr. hromadná retencia všetkých komunikácií, masový odposluch podmorského kábla) sú z pohľadu súdov takmer vždy neproporcionálne, ak neexistuje výnimočná situácia ohrozenia štátu. Cielené opatrenia (napr. sledovanie konkrétneho podozrivého, uchovávanie údajov len v určitom regióne s vysokým výskytom terorizmu) majú väčšiu šancu obstáť, ak sa preukáže ich nutnosť.
Závažnosť ohrozenia a účelové obmedzenie	Posudzuje sa, či opatrenie slúži skutočne vážnemu účelu (napr. boju proti závažným hrozbám). SDEÚ vyžaduje, aby napr. uchovávanie a využívanie dát bolo limitované len na boj proti závažnej trestnej činnosti alebo obdobne významným cieľom. Ak zákon umožňuje prístup k údajom aj pre relatívne malé prečiny, považuje sa to za neprimerané cieľu. Pred povolením sledovania by malo existovať podozrenie voči konkrétnej osobe, inak to neprejde testom nevyhnutnosti.
Trvanie uchovávania a rozsah dát	Čím dlhšie sú údaje uchovávané a čím väčší objem/podrobnosť informácií sa zhromažďuje, tým prísnejšie treba skúmať nevyhnutnosť. Napr. SDEÚ vytkol dátovej smernici fixnú lehotu min. 6 mesiacov pre všetky dáta bez rozlíšenia, čo nebolo preukázané ako striktne nevyhnutné.

	Očakáva sa, že lehota bude čo najkratšia potrebná a založená na objektívnych kritériách (napr. štatistická vyťažiteľnosť). Podobne ESĽP berie do úvahy, či zákon nestanovuje možnosť uchovávať dáta pridlho bez priebežného preverovania potreby.
Prístup orgánov a následné použitie údajov	Hodnotí sa režim, za akého môžu kompetentné orgány (polícia, spravodajské služby) pristúpiť k získaným/uchovaným dátam a ako ich môžu použiť. Ak chýba predchádzajúce povolenie nezávislým orgánom (súdom) na prístup, SDEÚ to považuje za problematické. SDEÚ zdôraznil, že prístup polície k uchovaným telekomunikačným dátam musí podliehať predchádzajúcej kontrole súdom alebo nezávislým administratívnym orgánom. ESĽP síce nevyžaduje vždy *ex ante* povolenie (ak to kompenzuje silná *ex post* kontrola), ale tiež považuje nezávislý dohľad za významný. Tiež sa skúma, na aké účely sa získané dáta môžu použiť ďalej – prísne viazanie na pôvodný účel je plus (napr. ak boli dáta získané pre boj s terorizmom, nemali by byť voľne použiteľné na iné ciele).
Bezpečnostné opatrenia pri uchovávaní a preposielaní dát	Keď už sa zhromažďujú citlivé dáta, musia byť chránené pred neoprávneným prístupom, únikom či zneužitím. SDEÚ v *Digital Rights Ireland* kritizoval chýbajúce záruky v smernici – nebola garantovaná dostatočná bezpečnosť týchto mega-archívov dát, ani nezávislý dohľad nad tým, kto k nim pristupuje

Tabuľka č. 2: Faktory proporcionality.

6.2.3.3 Procesné záruky, dohľad a opravné prostriedky

Silné procedurálne záruky sú nevyhnutné, aby sa riziko zneužitia obmedzujúcich opatrení minimalizovalo. V kontexte zásahov v oblasti kybernetickej bezpečnosti ide predovšetkým o tri oblasti:

- nezávislé povolenie alebo dohľad nad aplikáciou opatrenia,
- transparentnosť a notifikácia, a
- efektívne opravné prostriedky pre dotknuté osoby.

Optimálnym štandardom základných práv je, ak každý zásah (najmä tajný) vopred schvaľuje nezávislý orgán, ideálne súd. V kyberbezpečnosti však nastávajú situácie, kde *ex ante* povolenie nie je praktické (napr. automatizované zachytávanie veľkého toku dát spravodajskou službou). ESĽP preto akceptuje, že v niektorých režimoch môže namiesto predchádzajúcej autorizácie fungovať robustná následná kontrola. Podmienkou ale je, že kontrolný orgán je skutočne nezávislý a má právomoci prípadný zásah limitovať, prípadne zakázať. SDEÚ je prísnejší, nakoľko v kontexte uchovávaných dát rozhodol, že prístup orgánov k údajom musí v zásade schváliť súd alebo nezávislý orgán *ex ante*, okrem špecifických urgentných situácií.

Nezávislý dohľad môže mať viacero foriem: špecializovaný sudca, nezávislý správny orgán, ombudsman alebo iné subjekty. Podstatné je, aby bol nezávislý od výkonnej moci a mal dostatočné právomoci a kapacity vykonávať účinnú a nepretržitú kontrolu. Tento orgán by mal mať prístup k utajovaným informáciám, možnosť preveriť konkrétne prípady, zastaviť neoprávnené konania a podobne. ESĽP aj Benátska komisia odporúčajú, aby existoval aspoň orgán, ktorý ex post garantuje., že aj tajné opatrenia sú "držané na uzde".

Transparentnosť v oblasti kybernetickej bezpečnosti je zložitá, lebo mnohé opatrenia sú utajované, inak by stratili efektivitu. Napriek tomu sa vyžaduje určitá forma transparentnosti, minimálne vo forme verejne dostupných správ dohliadajúcich orgánov (koľko sledovaní prebehlo, koľko zamietnutých žiadostí, aké záruky sa uplatňujú). Rovnako je dôležitá vnútorná transparentnosť v podobe jasných interných pravidiel a dokumentovania procesov pre kontrolný orgán.

Kľúčovou zárukou je notifikácia dotknutej osoby *ex post*, akonáhle je to možné bez ohrozenia účelu opatrenia. ESĽP opakovane uviedol, že ak má byť dostupný účinný prostriedok nápravy, jednotlivec by sa mal dozvedieť o zásahu v momente, keď už nehrozí, že by to znemožnilo jeho účel.

Článok 13 EDĽP (a čl. 47 Charty EÚ) garantujú právo na účinný prostriedok nápravy. To znamená, že jednotlivec musí mať možnosť obrátiť sa na nezávislý orgán (súd) so sťažnosťou, ak sa domnieva, že jeho právo bolo porušené, a domôcť sa vyšetrenia a nápravy.

V kybernetickej bezpečnosti môže predmetná požiadavka predstavovať výraznú komplikáciu, nakoľko dotknutý subjekt často nevie o zásahu pre jeho utajenie. Preto sa do popredia dostávajú špeciálne mechanizmy ako napr. tzv. tribunály pre kontrolu sledovania (ako *Investigatory Powers Tribunal* v UK),[499] kam môžu ľudia poslať sťažnosť, aj keď nemajú dôkaz, pričom tento orgán má prístup k utajeným informáciám a môže rozhodnúť o nezákonnosti sledovania.

ESĽP takýto model akceptoval, hoci posudzoval, či tribunál spĺňa nezávislosť a kontradiktórnosť. Ďalším prípustným modelom je dať kompetenciu dozornému orgánu. V EÚ majú práve dozorné orgány podľa GDPR (a e-Privacy) silnú rolu.

[499] Dostupné na: https://investigatorypowerstribunal.org.uk/.

7. KYBERNETICKÁ BEZPEČNOSŤ A OCHRANA OSOBNÝCH ÚDAJOV

Právna úprava kybernetickej bezpečnosti prirodzene nie je „osamelým pustovníkom," ale jej ustanovenia častokrát dopĺňajú iné právne rámce, ktoré s touto problematikou nevyhnutne súvisia. V rámci tejto kapitoly sa preto stručne pozrieme na legislatívu, ktorá odzrkadľuje úzky vzťah s otázkami kybernetickej bezpečnosti – ochrana osobných údajov, ktorú reflektuje všeobecné nariadenie o ochrane údajov, známe pod skratkou GDPR (General Data Protection Regulation).[500] Spracúvanie osobných údajov je častokrát nevyhnutnou súčasťou kybernetických bezpečnostných opatrení, ako napríklad preventívne monitorovanie siete alebo detekcia incidentov, a z toho dôvodu sa na tieto aktivity bude vzťahovať všeobecný právny rámec ochrany osobných údajov.

Ochrana osobných údajov už dávno prestala byť izolovaným regulačným rámcom. Na úrovni Európskej únie bol prijatý nový balík právnych predpisov upravujúcich kybernetickú bezpečnosť, najmä smernica NIS 2 a nariadenie DORA. Tieto predpisy významne dopĺňajú bezpečnostné požiadavky podľa článku 32 GDPR (viď nižšie), pričom v mnohých prípadoch ukladajú detailnejšie a sektorovo špecifické povinnosti.

Je však potrebné zdôrazniť, že GDPR zostáva všeobecným rámcom ochrany osobných údajov a jeho povinnosti sa aplikujú paralelne s osobitnými bezpečnostnými predpismi.

7.1 Úvod a pôsobnosť

Na úrovní Európskej únie bola viac ako 20 rokov v platnosti smernica Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov. Nakoľko však išlo o smernicu, členské štáty si povinnosti uvedené v nej implementovali do svojich národných právnych poriadkov odlišným spôsobom.

Od roku 2012 prebiehali odborné diskusie a debaty v rámci európskych štruktúr, týkajúce sa modernizácie daného právneho rámca. Výsledkom spoločnej snahy viacerých aktérov bolo prijatie nového legislatívneho rámca regulujúceho ochranu osobných údajov

[500] 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). Ú. v. EÚ 119, 4.5.2016, s. 1–88.

v podobe nariadenia 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 alebo GDPR); a tzv. Policajnej smernice.[501]

Zároveň je potrebné dodať, že GDPR v určitých otázkach ponechalo voľnosť pre členské štáty a tie a tak v národných právnych poriadkoch mohli upraviť napr. vyváženie práva na ochranu osobných údajov a slobodu prejavu či právo na informácie, otázky mlčanlivosti, vek maloletých pri používaní služieb informačnej spoločnosti a ďalšie otázky.[502] Otázky bezpečnosti však v rámci týchto tzv. „otvorených klauzúl" nefigurujú, preto sa na nich bude vzťahovať všeobecná právna úprav v podobe GDPR.[503]

Kľúčové je aspoň v stručnej miere načrtnúť, kedy sa GDPR aplikuje vzhľadom na svoju pôsobnosť.

Vecná pôsobnosť GDPR je upravená v článku 2 ods. 1 GDPR.[504] Daný článok upravuje pozitívnu vecnú pôsobnosť GDPR. V zmysle dikcie predmetného článku sa GDPR aplikuje na spracúvanie osobných údajov, ktoré je vykonávané (i) automatizovanými prostriedkami, (ii) čiastočne automatizovanými prostriedkami alebo (iii) manuálne, ak osobné údaje tvoria súčasť informačného systému.

Samotné spracúvanie osobných údajov je definované v článku 4 bode 1 GDPR a to demonštratívnymi výpočtom spracovateľských operácií, ktoré možno subsumovať pod definíciu spracúvania osobných údajov. V zmysle daného článku sa pod spracúvaním osobných údajov rozumie:

---

[501] 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. Policajná smernica bola do slovenského právneho poriadku implementovaná v rámci 3. časti zákona č. 18/2018 Z. z. o ochrane osobných údajov. Dané ustanovenia regulujú spracúvanie osobných údajov tzv. kompletnými orgánmi (ako napr. Policajný zbor SR alebo Zbor väzenskej a justičnej stráže SR) pri trestnoprávnych účeloch, čiže vyšetrovanie, odhaľovanie prípadne výkon a ďalšie aktivity pred, pri a po trestnom stíhaní.

[502] K tomu pozri kapitolu IX GDPR.

[503] Ku vzťahu slovenského zákona č. 18/2018 Z. z. a GDPR pozri Úrad na ochranu osobných údajov SR: Kedy nariadenie a kedy zákon? Dostupné na: https://dataprotection.gov.sk/uoou/sk/content/kedy-nariadenie-kedy-zakon-o-ochrane-osobnych-udajov.

[504] *„Toto nariadenie sa vzťahuje na spracúvanie osobných údajov vykonávané úplne alebo čiastočne automatizovanými prostriedkami a na spracúvanie inými než automatizovanými prostriedkami v prípade osobných údajov, ktoré tvoria súčasť informačného systému alebo sú určené na to, aby tvorili súčasť informačného systému.*"

„operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, ***napríklad*** *získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami.*"

O čisto automatizované spracúvanie by išlo v prípade, ak by napríklad banka spracúvala údaje o žiadateľovi o úver a túto žiadosť by následne automatizovane posúdil algoritmus, ktorý by zároveň rozhodol o tom, či banka úvery poskytne alebo nie. V prípade čiastočne automatizovaného spracúvania by vo vyššie uvedenom prípade nakoniec o poskytnutí úveru rozhodol človek a v procese by bol prítomný ľudský zásah. Manuálne spracúvanie osobných údajov predstavuje napr. kartotéka pacientov u lekára zoradená podľa abecedy.[505]

Ústredným pojmom GDPR je však definícia osobného údaju. Osobným údajom

„je akékoľvek informácia týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby."[506]

Identifikovateľná fyzická osoba je taká osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä prostredníctvom odkazu na identifikátor, akým je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby. Pojem identifikovateľnosti ďalej vykladá recitál 26 GDPR.[507] Tento recitál reprezentuje tzv. test primeranej pravdepodobnosti, ktorý odpovedá

[505] Informačný systém je v zmysle článku 4 bod 6 GDPR definovaný ako *„akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe.*" Je nutné poznamenať, že v rámci slovenskej právnej kultúry došlo k dezinterpretácii tohto pojmu, avšak v zmysle staršej smernice a aj GDPR ide o manuálne spracúvanie údajov v rámci systému, v ktorom sa dá vyhľadávať podľa určitého kľúča.

[506] Článok 4 bod 1 GDPR.

[507] *„Na určenie toho, či je fyzická osoba identifikovateľná, by sa mali brať do úvahy všetky prostriedky, pri ktorých existuje primeraná pravdepodobnosť, že ich prevádzkovateľ alebo akákoľvek iná osoba využije, napríklad osobitným výberom, na priamu alebo nepriamu identifikáciu fyzickej osoby. Na zistenie toho, či je primerane pravdepodobné,*

na to, či je konkrétna dotknutá osoba skutočne identifikovateľná. Predmetným testom sa zaoberal aj Súdny dvor Európskej únie vo veci *C-582/14, Breyer.*[508] Skutkovo sa prípad týkal otázky, či dynamická IP adresa predstavuje osobný údaje v zmysle staršej legislatívy na ochranu osobných údajov. Prevádzkovateľ webového sídla mal k dispozícii IP adresa užívateľa, avšak nemal priamo informáciu, na koho je táto IP adresa registrovaná. Tieto informácie má zvyčajne k dispozícii poskytovateľ internetového pripojenia. Otázka teda bola, či pre prevádzkovateľa webového sídla predstavuje IP adresa osobný údaj v zmysle legálnej definície. Luxemburský súd judikoval:

> *„...že dynamická IP adresa, ktorú poskytovateľ online mediálnych služieb uchováva v súvislosti s prehliadaním si určitou osobou internetovej stránky, ktorú tento poskytovateľ sprístupnil verejnosti, predstavuje pre tohto poskytovateľa osobný údaj v zmysle tohto ustanovenia,* ***ak má k dispozícii právne prostriedky****, na základe ktorých dokáže identifikovať dotknutú osobu vďaka ďalším informáciám, ktorými disponuje poskytovateľ internetového pripojenia tejto osoby.*"

Toto rozhodnutie tak znamená, že ak existujú právom dovolené prostriedky na identifikáciu jednotlivca, pôjde o osobné údaje.

PRÍKLAD
Ilustráciou je situácia, ak dôjde ku kybernetickému útoku na webstránku orgánu verejnej moci a ten má k dispozícii iba IP adresu útočníka. V tomto prípade je IP adresa taktiež osobným údajom a to z toho dôvodu, že orgán verejnej moci má k dispozícii právne prostriedky na zistenie totožnosti útočníka (prostredníctvom orgánov činných v trestnom konaní, ktoré môžu požiadať prevádzkovateľa internetového pripojenia o stotožnenie IP adresy s konkrétnym páchateľom).

že sa prostriedky použijú na identifikáciu fyzickej osoby, by sa mali zohľadniť všetky objektívne faktory, ako sú náklady a čas potrebný na identifikáciu so zreteľom na technológiu dostupnú v čase spracúvania, ako aj na technologický vývoj."

[508] SDEÚ, vec C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, rozsudok z 19. 10. 2016.

K pojmu osobný údaj teda možno záverom dodať, že nie každá informácia je automaticky osobným údajom. Vždy bude záležať od konkrétnych okolností a kontextu, či je daná osoba identifikovateľná alebo nie.

GDPR upravuje v článku 2 ods. 2 negatívnu pôsobnosť nariadenia. To predstavuje situácie, v ktorých sa GDPR neaplikuje. Ide predovšetkým o prípady, na ktoré sa neaplikuje právo Európskej únie, otázky národnej bezpečnosti a tajných služieb či otázky patriace do pôsobnosti Policajnej smernice. Osobitne zaujímavou otázkou je výnimka z pôsobnosti, ktorá sa aplikuje v prípade, že spracúvanie osobných údajov prebieha fyzickou osobou v rámci výlučne osobnej alebo domácej činnosti.[509] GDPR však nedefinuje, o aké situácie konkrétne ide. Judikatúra SDEÚ však naznačuje určitý smer, ktorý ukazuje na prípady, kedy sa GDPR vzhľadom na negatívnu pôsobnosť nevzťahuje. O spracúvanie v rámci výlučne osobnej alebo domácej činnosti nepôjde vtedy, ak sú osobné údaje zverejnené na internete,[510] prípadne ak ide o monitorovanie ulice kamerovým systémom umiestneným nad dverami domu.[511]

GDPR upravuje územnú pôsobnosť v rámci článku 3. Je faktom, že nariadenie sa aplikuje v rámci spracúvania osobných údajov v prevádzke, ktorá má sídlo v EÚ (tzv. intra-teritoriálny režim), ale zároveň aj na prevádzkovateľov, ktorí majú sídlo mimo EÚ (tzv. extra-teritoriálny režim) za predpokladu, že ponúkajú osobám v EÚ tovary a služby alebo sledujú ich správanie, napríklad prostredníctvom webovej aktivity.

PRÍKLAD

Ak slovenská firma so sídlom v Bratislave spracúva osobné údaje za účelom bezpečnosti, robí tak v rámci režimu prevádzkarne v EÚ a bude sa na ňu vzťahovať GDPR.

Rovnaké konštatovanie ale platí pre elektronický obchod, ktorý v EÚ sídlo nemá, ale ponúka tovary a služby zákazníkom s možnosťou doručenia do EÚ.

Z hľadiska osobnej pôsobnosti je potrebné rozlišovať 5 typov entít v zmysle GDPR. Najdôležitejšími pojmami sú dotknutá osoba, prevádzkovateľ a sprostredkovateľ. Pre kompletnosť uvádzame aj definíciu pojmov príjemcov a tretej strany.

[509] Článok 2 ods. 2 písm. c) GDPR.
[510] Rozhodnutie Súdneho dvora Európskej únie, C-101/01- Lindqvist.
[511] Rozhodnutie Súdneho dvora Európskej únie, C-212/13-Ryneš.

Dotknutá osoba znamená identifikovanú alebo identifikovateľnú osobu, ktorej sa osobné údaje týkajú. GDPR nedefinuje termín dotknutá osoba, ale jej vymedzenie možno odvodiť z ustanovení týkajúcich sa pojmu osobný údaj (článok 4 bod 1 GDPR).

Prevádzkovateľ[512] je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov, pričom platí, že ak sa účely a prostriedky tohto spracúvania stanovujú v práve Únie alebo v práve členského štátu, možno prevádzkovateľa alebo konkrétne kritériá na jeho určenie určiť v práve Únie alebo v práve členského štátu. Najdôležitejším aspektom definície prevádzkovateľa je „určenie účelu." Entita, ktorá určí účel spracúvania osobných údajov (dôvod, prečo sú osobné údaje spracúvané) je prevádzkovateľom.

PRÍKLAD

Univerzita monitoruje bezpečnosť svojej siete a z tohto dôvodu v nevyhnutnej miere spracúva aj osobné údaje. Nakoľko tento účel vymedzila univerzita, bude prevádzkovateľom.

Spoloční prevádzkovatelia[513] sú dvaja alebo viacerí prevádzkovatelia, ktorí spoločne určia účely a prostriedky spracúvania.

Sprostredkovateľ[514] je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa. To znamená, že v tomto prípade je nevyhnutné mať poverenie a pokyny od prevádzkovateľa o tom, ako spracúvať osobné údaje v jeho mene. Nie je vylúčené, že jedna entita môže figurovať aj ako prevádzkovateľ a aj ako sprostredkovateľ.

PRÍKLAD

Ak univerzita na príklade uvedenom vyššie využíva na splnenie účelu dodávateľa špecifického softwaru, tento dodávateľ má postavenie sprostredkovateľa, keďže koná v mene univerzity za účelom vymedzeným univerzitou.

Ak by však dodávateľ softwaru spracúval osobné údaje na vlastné účely, napríklad na štatistiky, účel vymedzil sám a bude v tomto postavení prevádzkovateľom.

[512] Článok 4 bod 7 GDPR.
[513] Článok 26 ods. 1 GDPR.
[514] Článok 4 bod 8 GDPR.

Príjemca[515] je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorému sa osobné údaje poskytujú bez ohľadu na to, či je treťou stranou. Orgány verejnej moci, ktoré môžu prijať osobné údaje v rámci konkrétneho zisťovania v súlade s právom Únie alebo právom členského štátu, sa však nepovažujú za príjemcov.

Tretia strana[516] je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt než dotknutá osoba, prevádzkovateľ, sprostredkovateľ a osoby, ktoré sú na základe priameho poverenia prevádzkovateľa alebo sprostredkovateľa poverené spracúvaním osobných údajov.

7.2 Základné zásady spracúvania

GDPR stojí a padá na siedmych zásadách, ktoré sú upravené v článku 5. Zásady spracúvania osobných údajov slúžia predovšetkým ako interpretačné pravidlá. To znamená, že ak nariadenie určitú aplikačnú otázku priamo nerieši, adresáti právnych noriem by mali zohľadniť uplatnenie a výklad noriem spôsobom súladným so základnými zásadami. Zároveň, každá zásada predstavuje všeobecné pravidlo pre špecifickejšie inštitúty upravujúce konkrétne povinnosti v zmysle nariadenia.

Alfou a omegou spracúvania sú zásada zákonnosti a zásada vymedzenia účelu. Tieto zásady zásadne obmedzujú dôvody spracúvania osobných údajov a tzv. právne základy alebo právne tituly, na ktorých je spracúvanie možné vykonávať.

Zásada zákonnosti ustanovuje:

> *„Osobné údaje musia byť…spracúvané zákonným spôsobom, spravodlivo a transparentne vo vzťahu k dotknutej osobe („zákonnosť, spravodlivosť a transparentnosť").*"

Predmetná zásada vyžaduje zákonné spracúvanie osobných údajov, ktoré je bližšie upravené v článku 6 GDPR. Ten upravuje šesť právnych základov (titulov), na základe ktorých

[515] Článok 4 bod 9 GDPR.
[516] Článok 4 bod 10 GDPR.

je možné osobné údaje spracúvať. Týmito titulmi sú súhlas, plnenie zmluvy, zákonná povinnosť, životne dôležitý záujem, verejný záujem a oprávnený záujem. Najčastejšie využívaným právnym základom je zákonná povinnosť, nakoľko množstvo osobitných právnych predpisov priamo vyžaduje spracúvanie osobných údajov na plnenie určitých povinností.

Súdny dvor vo veci C-252/21 Meta Platforms[517] zdôraznil, že oprávnený záujem nemožno vykladať extenzívne tak, aby legitimizoval systematické profilovanie používateľov bez riadneho vyváženia práv a slobôd dotknutých osôb. Test proporcionality musí byť konkrétny a dokumentovaný z dôvodu kontroly dozornými orgánmi.

Súčasťou tejto zásady sú aj požiadavky na spravodlivosť a transparentnosť. Spravodlivosť spočíva v požiadavke, že spracovateľské operácie sa majú vykonávať pôvodným spôsobom. Transparentnosť je prítomná v konkrétnych inštitútoch GDPR ako informačná povinnosť prevádzkovateľa (články 12 až 14 GDPR), transparentnosti práv dotknutých osôb a komunikovanie bezpečnostných incidentov, ktorým je venovaná osobitná stať tejto kapitoly.

Na zásadu zákonnosti priamo nadväzuje zásada vymedzenia účelu. Každý právny základ musí byť previazaný s konkrétnym dôvodom – účelom spracúvania.

> *„Osobné údaje musia byť… získavané na konkrétne určené, výslovne uvedené a legitímne účely a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi; ďalšie spracúvanie na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či štatistické účely sa v súlade s článkom 89 ods. 1 nepovažuje za nezlučiteľné s pôvodnými účelmi („obmedzenie účelu").*"

Predmetná zásada prakticky znamená, že prevádzkovateľ sa musí vopred zamyslieť, na aké účely osobné údaje reálne potrebuje a tieto dôvody komunikovať navonok dotknutým osobám. Dané ustanovenie zároveň upravuje aj súladnosť nových účelov s pôvodnými, kde za automaticky kompatibilné považujú účely archivácie vo verejnom záujme, účely vedeckého alebo historického výskumu či štatistické účely.

[517] SDEÚ, vec C-252/21, *Meta Platforms a i.*, rozsudok z 4. 7. 2023.

Ak vezmeme do úvahy účely týkajúce sa bezpečnosti z pohľadu účelu a právneho základu, môžeme vymedziť dané účely a právne základy napríklad takto:

Účel	Právny základ	Vysvetlenie
Bezpečnosť informačných technológií alebo iba „Bezpečnosť"	Plnenie zákonných povinností podľa článku 6 ods. 1 písm. c) GDPR Alternatívne oprávnený záujem podľa článku 6 ods. 1 písm. f) GDPR	Vzhľadom na to, že pri činnosti prevádzkovateľa je potrebné dbať na bezpečnosť zamestnancov alebo pri poskytovaní služieb na bezpečnosť užívateľov, je nevyhnutné vymedziť aj účel bezpečnosti, ktorý zahŕňa spracovateľské operácie ako monitorovanie siete alebo detekciu kybernetických incidentov. Právnym základom môže byť buď plnenie zákonných povinnosti s odkazom na požiadavky GDPR, kybernetickej bezpečnosti alebo národnej právnej úpravy. Alternatívne sa v praxi využíva aj oprávnený záujem, ktorý pokrýva spracúvanie údajov na účely bezpečnosti mimo osobitných právnych predpisov. Samotným

		oprávneným záujmom môže byť napríklad „bezpečnosť informačných technológií a sietí." Ak by prevádzkovateľ daný účel nemal, hrozili by ekonomické ale aj neekonomické škody ako napríklad únik údajov a ohrozenie práv a záujmov fyzických osôb.

Tabuľka č. 3: Účel a právny základ.

Ďalšou zásadou v zmysle GDPR je zásada minimalizácie údajov:

„Osobné údaje musia byť…primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú („minimalizácia údajov")."

Prevádzkovateľ tak zjednodušene nemôže spracúvať viac osobných údajov, ako je na daný účel vhodné. Pri bezpečnostných opatreniach je však veľmi náročné určenie hranice toho, čo je potrebné a čo nie.

PRÍKLAD
Prevádzkovateľ implementuje bezpečnostné logovanie všetkej aktivity zamestnancov vrátane zaznamenávania obsahu komunikácie. Takéto opatrenie môže byť neprimerané, pokiaľ postačuje zaznamenávanie metaúdajov (čas, identifikátor používateľa, IP adresa). Minimalizácia údajov sa aplikuje aj pri bezpečnostných opatreniach.

Zásada správnosti vyžaduje, že:

„Osobné údaje musia byť… správne a podľa potreby aktualizované; musia sa prijať všetky potrebné opatrenia, aby sa zabezpečilo, že sa osobné údaje, ktoré sú

nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bezodkladne vymažú alebo opravia („správnosť")."

Prevádzkovateľ tak musí objektívne zabezpečiť čo najväčšiu presnosť údajov v kontexte účelu spracúvania.

Dobu uchovávania osobných údajov reflektuje zásada minimalizácie uchovávania:

„Osobné údaje musia byť... uchovávané vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac dovtedy, kým je to potrebné na účely, na ktoré sa osobné údaje spracúvajú; osobné údaje sa môžu uchovávať dlhšie, pokiaľ sa budú spracúvať výlučne na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely v súlade s článkom 89 ods. 1 za predpokladu prijatia primeraných technických a organizačných opatrení vyžadovaných týmto nariadením na ochranu práv a slobôd dotknutých osôb („minimalizácia uchovávania")."

Prevádzkovateľ je povinný vymedziť dobu uchovávania údajov na jednotlivé účely. Môže tak urobiť číselne alebo s naviazaním na konkrétnu udalosť, napr. uplynutie premlčacej doby či zánik nároku.

Samotnú bezpečnosť rámcuje zásada integrity a dôvernosti, ku ktorej sa ešte v rámci tejto kapitoly vrátime:

„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 („integrita a dôvernosť")."

Veľmi dôležitou zásadou je aj zásada zodpovednosti:

„Prevádzkovateľ je zodpovedný za súlad s odsekom 1 a musí vedieť tento súlad preukázať („zodpovednosť").

Zásada zodpovednosti je jednou z najdôležitejších, napriek tomu, že jej legislatívne vyjadrenie zvádza k pochybnostiam. Jej zmysel spočíva v tom, že prevádzkovateľ by mal nielen prijať potrebné dokumenty na zabezpečenie súladu s GDPR (ako napríklad internú politiku alebo bezpečnostnú politiku), ale zároveň tieto opatrenia aktívne implementovať do praxe. Ochrana osobných údajov totiž nie je otázkou, ktorú je možné vyriešiť jednorazovo. Ide o dlhodobú uvedomelú činnosť, ktorá si vyžaduje pravidelnú starostlivosť a riešenie. Podobné konštatovanie možno uviesť vo vzťahu ku kybernetickej bezpečnosti.

7.3 Bezpečnosť

7.3.1 Všeobecná klauzula bezpečnosti

Samotná bezpečnosť a jej požiadavky v zmysle spracúvania osobných údajov sú upravené v článku 32 GDPR. Práve tento článok nadväzuje už na spomínanú zásadu integrity a dôvernosti uvedenú vyššie, ktoré reflektuje bezpečnostné požiadavky na spracúvanie osobných údajov.

Článok 32 ods. 1 upravuje všeobecnú klauzulu bezpečnosti:

> *„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…"*

Diskutovaný článok explicitne ustanovuje požiadavky triády kybernetickej bezpečnosti (CIA) uvedené v úvode tejto učebnice. Zachováva tak konzistentnosť požiadaviek na kybernetickú bezpečnosť v rámci právnych rámcov. Zároveň daný článok vymedzuje demonštratívny výpočet bezpečnostných opatrení, ktoré môže prevádzkovateľ alebo sprostredkovateľ prijať. Konkrétne ide o:

- pseudonymizáciu a šifrovanie osobných údajov;
- schopnosť zabezpečiť trvalú dôvernosť, integritu, dostupnosť a odolnosť systémov spracúvania a služieb;
- schopnosť včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu;

- proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania.

Článok 32 opakovane zdôrazňuje požiadavku primeranosti bezpečnostných opatrení. Prakticky to znamená, že prevádzkovatelia a sprostredkovatelia musia identifikovať konkrétne riziká v konkrétnych situáciách a zohľadniť špecifiká spracúvania osobných údajov ako napr. citlivosť údajov, prípadne ďalší kontext.

> *„Pri posudzovaní primeranej úrovne bezpečnosti sa prihliada predovšetkým na riziká, ktoré predstavuje spracúvanie, a to najmä v dôsledku náhodného alebo nezákonného zničenia, straty, zmeny, neoprávneného poskytnutia osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávneného prístupu k takýmto údajom.*"

Samotná referencia na primeranosť znamená aj úzke prepojenie na princíp proporcionality, ktorý je všeobecne známy a preferovaný v práve EÚ. Proporcionalita vo všeobecnosti znamená, že je potrebné merať vhodnosť použitých prostriedkov vzhľadom na účel a zamýšľaný výsledok.

PRÍKLAD

Odlišné bezpečnostné opatrenia sa budú javiť ako vhodné pre sociálnu sieť s miliardou užívateľov a pre malého podnikateľa s úzkou klientelou. Použitie biometrického skenovania očných sietnic ako bezpečnostného opatrenia za účelom vstupu do priestoru chovu poľnohospodárskych zvierat je zjavne neproporcionálne zamýšľanému dôsledku.

Z ROZHODNUTÍ DOZORNÝCH ORGÁNOV

Porušenie článku 32 GDPR býva jedným z najčastejšie penalizovaných porušení nariadenia od účinnosti GDPR. Najvyššia pokuta za nedostatočné bezpečnostné opatrenia bola uložená v Taliansku vo výške 27 800 000 €. Jeden z najväčších telekomunikačných

operátorov v Taliansku (TIM) dostal pokutu v uvedenej výške za viacero porušení GDPR pri marketingovej komunikácií vrátane článku 32 GDPR.[518]

Zaujímavé sú aj dva prípady v Spojenom kráľovstve. Britský dozorný orgán uložil leteckej spoločnosti British Airways pokutu 22 046 000 € 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.[519] V druhom prípade bola uložená pokuta vo výške 20 450 000 € sieti hotelových zariadení Marriott International za nedostatočné bezpečnostné opatrenia a únik údajov týkajúci sa 339 miliónov zákazníkov.[520] Pre porovnanie slovenský dozorný orgán uložil zatiaľ najvyššiu pokutu 50 000 € Sociálnej poisťovni za porušenie článku 32 GDPR tým, že došlo k strate žiadostí o sociálne poistenie, ktoré boli zaslané poisťovňou do zahraničia klasickým doručením (nie do vlastných rúk) a následne stratené.[521]

Súdny dvor Európskej únie vo veci C-340/21 (Natsionalna agentsia za prihodite) rozhodol, že samotná existencia kybernetického útoku neznamená automaticky, že prevádzkovateľ nesplnil požiadavky článku 32 GDPR. Prevádzkovateľ musí byť schopný preukázať, že prijaté technické a organizačné opatrenia boli primerané riziku.

Nemožno sa zbaviť zodpovednosti len poukazom na konanie tretej osoby (hackera). Dôkazné bremeno o primeranosti opatrení nesie prevádzkovateľ.

Sankčná prax dozorných orgánov sa po roku 2022 výrazne sprísnila. Pokuty presahujúce stovky miliónov eur sa stali realitou najmä v prípadoch nedostatočného zabezpečenia prenosov do tretích krajín alebo systematického porušovania zásad zákonnosti a minimalizácie údajov.

[518] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9256486 (dostupné 12.12.2025).

[519] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/ (dostupné 12.8.2025).

[520] 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 12.8.2025).

[521] https://www.etrend.sk/ekonomika/socialna-poistovna-porusila-gdpr-pokutu-50-tisic-eur-nechce-zaplatit.html (dostupné 12.8.2025).

PRÍKLAD

Írsky dozorný orgán uložil v roku 2023 spoločnosti Meta Platforms Ireland Ltd. pokutu vo výške 1,2 miliardy eur za porušenie pravidiel prenosu osobných údajov do Spojených štátov amerických. Dozorný orgán dospel k záveru, že samotné použitie štandardných zmluvných doložiek nepostačovalo na zabezpečenie primeranej úrovne ochrany po rozsudku Schrems II[522] keďže neboli prijaté dostatočné doplnkové technické a organizačné opatrenia. Rozhodnutie zároveň obsahovalo príkaz na pozastavenie ďalších prenosov údajov.

Uvedený prípad ilustruje, že porušenie povinností podľa GDPR môže mať nielen reputačné, ale aj zásadné finančné a prevádzkové dôsledky.

7.3.2 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 nasledovne:

> *„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.[523]

[522] SDEÚ, vec C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd a Maximillian Schrems*, rozsudok z 16. 7. 2020.

[523] K tomu pozri aj Article 29 Working Party Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01.

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**.

> *„V prípade porušenia ochrany osobných údajov prevádzkovateľ bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín po tom, čo sa o tejto skutočnosti dozvedel, oznámi porušenie ochrany osobných údajov dozornému orgánu príslušnému podľa článku 55 s výnimkou prípadov, keď nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb. Ak oznámenie nebolo dozornému orgánu predložené do 72 hodín, pripojí sa k nemu zdôvodnenie omeškania.*" (Článok 33 GDPR)

> *„V prípade porušenia ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ bez zbytočného odkladu oznámi porušenie ochrany osobných údajov dotknutej osobe.*" (Článok 34 GDPR).

Proces nahlasovania vyhodnocovania porušení ochrany osobných údajov možno zadeliť do viacerých etáp alebo fáz.

V prvom rade, ak všeobecne dôjde k bezpečnostnému incidentu 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 organizácii 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.

PRÍKLAD
Zamestnancovi sa 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, nie je riziko pre práva a slobody dotknutých osôb žiadne resp. je minimálne.

V prípade, ak sa porušenie ochrany osobných údajov stane na strane sprostredkovateľa, je o tom povinný informovať prevádzkovateľa bez zbytočného odkladu.[524] Pri komplexnejších situáciách je možné dozorný orgán informovať postupne s vysvetlením, prečo informuje postupne. Úrad na ochranu osobných údajov Slovenskej republiky má na svojom webe zverejnený formulár, prostredníctvom ktorého je možné porušenia ochrany osobných údajov nahlasovať.[525] 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.[526] Kritéria na posúdenie vysokého rizika vymedzila Pracovná skupina čl. 29 vo svojom usmernení.[527] Konkrétne ide o

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

[524] Viď článok 33 ods. 2 GDPR.
[525] https://dataprotection.gov.sk/uoou/sk/dp/dp-breach (512.8.2021).
[526] Článok 34 ods. 1 GDPR.
[527] Article 29 Working Party Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01.

- počet zasiahnutých osôb, prípadne ďalšie faktory.[528]

PRÍKLAD

Nemocnica v krajskom meste sa stane obeťou kybernetického útoku, pri ktorom sú kompromitované údaje zamestnancov a pacientov. Údaje sú riadne zálohované a šifrované. Vyšetrovanie ukáže, že útočník osobné údaje iba videl, ale nestiahol si ich. Záloha údajov a nastavenie systémov do pôvodnej prevádzky ale trvalo dva dni, počas ktorých bolo limitované poskytovanie zdravotnej starostlivosti.

Napriek tomu, že nedošlo k veľkej škode čo sa týka samotných osobných údajov, činnosť nemocnice bola obmedzená, a z toho dôvodu by mal byť tento prípad klasifikovaný ako nesúci vysoké riziko.

V prípade, ak prevádzkovateľ vysoké riziko pri porušení ochrany osobných údajov vyhodnotí, nemusí automaticky dotknuté osoby informovať. GDPR totiž ustanovuje tri výnimky, v rámci ktorých prevádzkovateľ takéto incidenty nemusí oznamovať 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 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.[529]

PRÍKLAD

Firemná databáza s údajmi klientov je kompromitovaná po ransomware útoku na informačné technológie. Databáza je šifrovaná a spĺňa kritéria najvyššieho štandardu šifrovacích metód (*state of the art)*. Prevádzkovateľtak nemusí dotknuté osoby informovať, nakoľko je minimálne pravdepodobné rozšifrovanie danej databázy.

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.[530]

[528] Tamže.
[529] Článok 34 ods. 3 a) GDPR.
[530] Článok 34 ods. 3 b) GDPR.

PRÍKLAD

Firma zistí, že pred niekoľkými sekundami jeden z jej zamestnancov neoprávnene pristúpil k niektorým osobným údajom klientom. Do niekoľkých minút je priamo pri zamestnancovi na mieste zodpovedná osoba s ochrankou a IT špecialistom. Zistí sa, že zamestnanec údaje nikam neodoslal a ani ich nijakým spôsobom nereplikoval. V takom prípade je možné spoľahnúť sa na výnimku komunikácie porušenia uvedenú vyššie.

Poslednou výnimkou je prípad, v ktorom 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.[531]

PRÍKLAD

Orgán verejnej moci zistí porušenie ochrany osobných údajov, pri ktorom boli kompromitované údaje dvoch miliónov občanov. Oznam o takomto incidente zverejní na svojom webovom sídle a zároveň v celoštátnych médiách.

Ak prevádzkovateľ túto povinnosť nesplní, dozorný orgán si môže notifikačnú povinnosť vynútiť.[532] Aj v tomto prípade je prevádzkovateľ povinný predmetný incident zdokumentovať.

Zároveň si dovoľujeme zvýrazniť, že vo veci C-300/21 Österreichische Post[533] SDEÚ vyslovil, že na priznanie nemajetkovej ujmy podľa článku 82 GDPR nie je potrebná vysoká intenzita zásahu. Samotné porušenie GDPR však automaticky neznamená vznik nároku na náhradu škody – dotknutá osoba musí preukázať existenciu ujmy a príčinnú súvislosť. Tento rozsudok je tak relevantný v kontexte ujmy spôsobenej pri kybernetických incidentoch.

7.3.3 Zodpovednosť a náhrada škody

Osobitný význam v systéme ochrany osobných údajov má ustanovenie článku 82 GDPR, ktoré upravuje právo na náhradu škody. Ide o ustanovenie, ktoré výrazne posilňuje

[531] Článok 34 ods. 3 c) GDPR.
[532] Viď článok 34 ods. 4 GDPR.
[533] SDEÚ, vec C-300/21, *Österreichische Post AG*, rozsudok z 4. 5. 2023.

súkromnoprávny rozmer ochrany osobných údajov a zároveň predstavuje významný faktor právneho rizika pre prevádzkovateľov a sprostredkovateľov.

Podľa článku 82 ods. 1 GDPR:

„Každá osoba, ktorá utrpela majetkovú alebo nemajetkovú ujmu v dôsledku porušenia tohto nariadenia, má právo na náhradu škody od prevádzkovateľa alebo sprostredkovateľa za utrpenú škodu."

Zodpovednosť podľa článku 82 GDPR má v zásade objektívny charakter. Článok 82 ods. 2 stanovuje, že každý prevádzkovateľ zapojený do spracúvania zodpovedá za škodu spôsobenú spracúvaním, ktoré porušuje GDPR. Sprostredkovateľ zodpovedá v prípade, ak nesplnil povinnosti, ktoré sa na neho vzťahujú priamo podľa GDPR alebo ak konal mimo zákonných pokynov prevádzkovateľa.

Možnosť exkulpácie upravuje článok 82 ods. 3 GDPR, podľa ktorého:

„Prevádzkovateľ alebo sprostredkovateľ je zbavený zodpovednosti, ak preukáže, že nijakým spôsobom nezodpovedá za udalosť, ktorá spôsobila škodu."

Súdny dvor Európskej únie vo veci C-340/21 Natsionalna agentsia za prihodite zdôraznil, že samotná existencia kybernetického útoku nepostačuje na zbavenie sa zodpovednosti. Prevádzkovateľ musí preukázať, že prijal primerané technické a organizačné opatrenia podľa článku 32 GDPR a že porušenie nebolo dôsledkom jeho pochybenia.

Z judikatúry SDEÚ vyplýva, že vznik zodpovednosti podľa článku 82 GDPR predpokladá kumulatívne splnenie troch podmienok:

1. porušenie GDPR,
2. vznik škody (majetkovej alebo nemajetkovej),
3. príčinná súvislosť medzi porušením a škodou.

Vo veci C-300/21 Österreichische Post Súdny dvor rozhodol, že samotné porušenie GDPR automaticky nezakladá nárok na náhradu škody. Dotknutá osoba musí preukázať existenciu ujmy a príčinnú súvislosť. Zároveň však Súdny dvor odmietol požiadavku minimálnej intenzity nemajetkovej ujmy, čo znamená, že aj menej závažné zásahy môžu byť odškodniteľné.

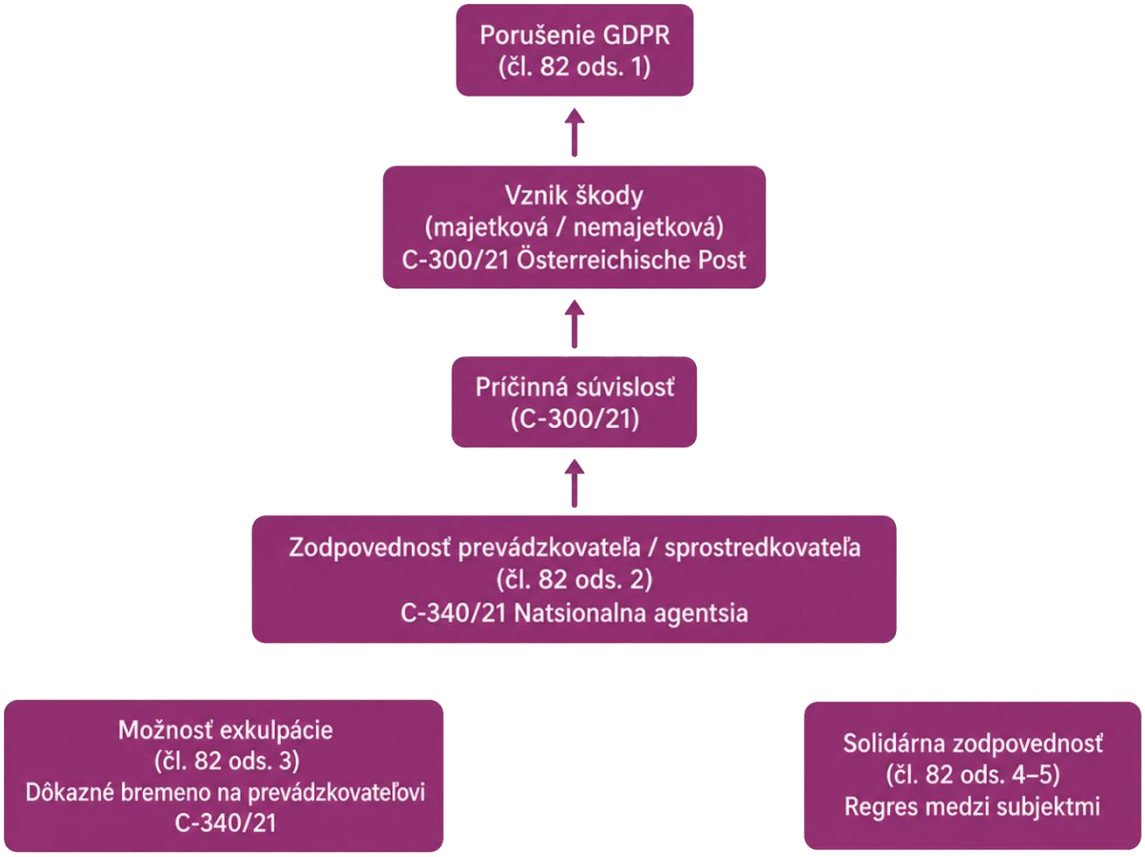
Pokiaľ ide o dôkazné bremeno, žalobca nesie dôkazné bremeno vo vzťahu k existencii škody a príčinnej súvislosti. Naopak, podľa článku 82 ods. 3 GDPR nesie prevádzkovateľ dôkazné bremeno v prípade, ak sa chce zbaviť zodpovednosti.

Článok 82 ods. 4 GDPR ustanovuje solidárnu zodpovednosť, ak je do toho istého spracúvania zapojených viacero prevádzkovateľov alebo sprostredkovateľov. Dotknutá osoba môže požadovať náhradu celej škody od ktoréhokoľvek z nich. Následné vyrovnanie medzi zodpovednými subjektmi prebieha podľa článku 82 ods. 5 GDPR formou regresu.

Významný posun priniesol článok 80 GDPR, ktorý umožňuje dotknutej osobe poveriť neziskový subjekt, aby uplatňoval jej práva vrátane práva na náhradu škody. Tento mechanizmus bol ďalej posilnený prijatím smernice (EÚ) 2020/1828 o zástupných žalobách na ochranu kolektívnych záujmov spotrebiteľov.

Súdny dvor vo veci C-319/20 Meta Platforms Ireland potvrdil, že spotrebiteľské združenia môžu za určitých podmienok podať žalobu aj bez individuálneho splnomocnenia konkrétnej dotknutej osoby, ak to umožňuje vnútroštátne právo.

Kolektívne uplatňovanie nárokov tak významne zvyšuje procesné riziko pre prevádzkovateľov, najmä v prípadoch rozsiahlych bezpečnostných incidentov.



Obrázok č. 12: Zodpovednosť prevádzkovateľa/sprostredkovateľa.

8. ETIKA KYBERNETICKEJ BEZPEČNOSTI

Regulácia a osobitne regulácia nových technológií v dnešnej dobe už nie je doménou iba legislatívy. Predmetná myšlienka nie je nová, podobné tézy prezentoval už Lawrence Lessig z Harvard Law School vo svojej slávnej eseji a následne knihe Code v2.0 na konci 20. storočia.[534] Lessig už dávnejšie upozorňoval, že osobitne v kyberpriestore pôsobia štyri modality regulácie, ktoré sa navzájom dopĺňajú pri regulovaní spoločenských vzťahov. Konkrétne hovoril o práve, morálke (etike), trhu a architektúre alebo kóde. Legislatíva tak nie je jediná možnosť ako upraviť pravidlá správania sa a toto konštatovanie platí aj pre oblasť kybernetickej bezpečnosti.

PRÍKLAD

Vyššie uvedené modality regulácie spoločenských vzťahov môžu spolupôsobiť aj v oblasti kybernetickej bezpečnosti. Právo určuje základný rámec bezpečnostných opatrení alebo nahlasovania bezpečnostných incidentov. Etika alebo morálka zohráva výraznú úlohu napríklad pri tzv. etickom hackingu a jeho prevedení. Trh určuje cenu a hodnotu aktív, ktoré kybernetická bezpečnosť chráni. Architektúra alebo kód predstavuje pravidlá „stmelené" do dizajnu bezpečnostných technických opatrení. Napríklad šifrovaný súbor je možné otvoriť iba so zodpovedajúcou technológiou a kľúčom.

V rámci tejto kapitoly sa budeme venovať etike. Kým prejdeme ku konkrétnym otázkam etiky kybernetickej bezpečnosti, považujeme za nevyhnutné načrtnúť základné východiská etického rámca a jeho vzťahu ku právu. Následne budeme diskutovať konkrétne etické hodnoty kybernetickej bezpečnosti, ich konflikty a vzájomné vzťahy a možnosti praktického využitia etických posúdení pri analýze rizík v oblasti kybernetickej bezpečnosti.

8.1 Etika, právo, hodnoty a dilemy pre začiatočníkov

Na úvod tejto kapitoly je potrebné vymedziť niekoľko základných pojmov a vzťahov. Čo je vlastne etika? Etika je filozofická disciplína, ktorá sa zaoberá otázkami ako by sme mali

[534] Pozri LESSIG, L.: The Laws of Cyberspace. Draft 3. 1998. Dostupné na: https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf. HUSOVEC, M. – MESARČÍK, M. – ANDRAŠKO, J.: Právo informačných a komunikačných technológií 1. TINCT, 2020, s. 15 – 21.

žiť, myšlienkami dobra a pracuje s pojmami ako „správne" a „nesprávne."[535] Podobným spôsobom definuje etiku slovenská teória práva: *„..pojmom „etika" sa označuje teória morálky, veda o mravnosti, čiže filozofická disciplína, ktorá sa venuje skúmaniu morálky, jej pôvodu, podstaty a obsahu morálnych kategórií."*[536] Etika v zásade skúma racionálnu a praktickú reflexiu toho, čo je dobré a zlé; a zároveň skúma na inej úrovni čo je správne a nesprávne. Štúdiu etiky možno diferencovať na tri kľúčové častí:

1) *Deskriptívnu etiku* – táto oblasť skúma tradície, zvyky a princípy ľudí a kultúr;
2) *Etickú teóriu*, (alebo normatívna etika ktorá sa snaží systematicky pochopiť a odôvodniť morálne koncepty a princípy prostredníctvom toho, čo je dobré a zlé spolu s analýzou zdroja daných myšlienok. Cieľom je formulovať princípy správneho správania v podobe usmernení pre jednotlivcov a skupiny.
3) *Aplikovaná etika* sa venuje skúmaniu konkrétnych kontroverzných etických problémov v praxi ako napríklad umelé prerušenie tehotenstva, trest smrti alebo eutanázia.[537] V tejto kapitole sa budeme venovať práve aplikovanej etike pri konkrétnej oblasti a v konkrétnom kontexte (kybernetická bezpečnosť).

Kľúčové pri aplikovanej etike je riešenie tzv. etických dilem a konfliktu hodnôt.[538] Hodnoty sú spájané s tým, čo je dobré alebo žiadané a poskytujú ľuďom návod ako sa správať. Na účely tejto kapitoly ich môžeme definovať ako hodnotiaci rámec, v ktorom posudzujeme dobré a správne správanie v konkrétnej situácií. Navyše, hodnoty napomáhajú riešeniu a pochopeniu problematických etických otázok.[539] Tieto hodnoty prirodzene nefungujú vo vákuu, ale častokrát sa ocitajú v konflikte. Konflikt hodnôt alebo morálna dilema je situácia, v ktorej nie je možné rôzne relevantné hodnoty rešpektovať simultánne a je potrebné ich vyvažovať.[540]

---

[535] POJMAN, L. – FIESER, J.: Ethics: Discovering Right and Wrong. Cengage Learning, 2011, s. 1 – 2.
[536] KOLEKTÍV AUTOROV: Aktuálne otázky teórie práva. 1. vydanie. Bratislava: Wolters Kluwer, 2018, s. 258.
[537] POJMAN, L. – FIESER, J.: Ethics: Discovering Right and Wrong. Cengage Learning, 2011, s. 2. Iní autori do delenia zahŕňajú aj metaetiku. Pozri napr. KOLEKTÍV AUTOROV: Aktuálne otázky teórie práva. 1. vydanie. Bratislava: Wolters Kluwer, 2018.
[538] VAN, DEM HOVEN a kol.: Engineering and the Problem of Moral Overload. In Sci Eng Ethics. 2012; 18(1), s. 143–155.
[539] VAN DE POEL, I.: Core Values and Value Conflicts in Cybersecurity: Beyond Privacy versus Security. In CHRISTEN, M. et al. (eds): The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology, 21. Dordrecht: Springer, 2020, s. 46.
[540] V slovenskej spisbe pozri napríklad MARKOŠ, J.: Medzi dobrom a zlom. 16 etických dilem, pred ktorými môžete stáť raz i vy. Bratislava: N PRESS, 2020.

PRÍKLAD

Typickým prípadom konfliktu hodnôt v oblasti kybernetickej bezpečnosti je etický hacking. Ak etický hacker odhalí, že v štátnom informačnom systéme je zraniteľnosť, musí opatrne vyvážiť hodnoty transparentnosti a bezpečnosti. Na jednej strane občanom musí záležať na tom, aby ich údaje a verejné služby boli z pohľadu technického zabezpečenia bezpečné. Na strane druhej, zverejnením zraniteľnosti môže odhalenú zraniteľnosť ktokoľvek zneužiť. Zároveň, občania majú právo na informácie o zabezpečení svojich údajov orgánmi verejnej moci.

Druhú otázku, ktorú sme si pri tomto stručnom exkurze položili je, aký je vzťah medzi právom a etikou? Už z úvodného slova pri tejto kapitole je zjavné, že pôjde o modality, ktoré sú schopné regulovať správanie jednotlivcov. V teórií a súčasných diskusiách existujú tri názory na vzťah etiky a práva. Prvý názor prezentuje tézu, že právo a etika reflektujú *úplnú jednotu* a teda právo spolu s etikou predstavuje univerzálny morálny rámec. Druhá názorová skupina akademikov prezentuje opačný názor – právo a etika sú podľa nich *úplne odlišné* fenomény, ktoré pochádzajú z odlišného zdroja. Medzi spomínanými dvoma prúdmi pôsobí tretí, ktorý reprezentuje pohľad *prieniku a vzájomného ovplyvňovania* medzi právom a etikou.[541] Typické otázky prieniku etiky a práva predstavujú základné ľudské práva a slobody, právne princípy, Radbruchova formula či rešpektovanie hodnoty ľudskej dôstojnosti.[542] K týmto prezentovaným tézam možno ešte dodať, že vzťah práva a etiky nie je čiernobiely. V niektorých situáciách idú etické pravidlá ďalej ako právo. Taktiež existujú situácie, keď je konanie v súlade s právnym poriadkom, ale v konflikte s etickými pravidlami.

V ostatnom období sa v odbornej literatúre vyskytuje pojem „etifikácia" práva (*ethification*), hlavne v oblasti práva informačných a komunikačných technológií na úrovní Európskej únie. Etifikáciou možno rozumieť šírenie odvolávania sa na „etiku" a „etické princípy a hodnoty" v právnych, politických, akademických a diskusiách pri podnikaní o riadení technológií a rastúci inštitucionálny význam etickej expertízy prostredníctvom poradných orgánov ako aj prostredníctvom postupov zakotvených v metodických

[541] Pozri viac KOLEKTÍV AUTOROV: Aktuálne otázky teórie práva. 1. vydanie. Bratislava: Wolters Kluwer, 2018, s. 261 a nasl.
[542] Tamže, s. 264 a nasl.

dokumentoch.[543] Typickým príkladom je oblasť ochrany osobných údajov a regulácie umelej inteligencie. V rámci riadiacich orgánov EÚ pôsobí Expertná skupina na vysokej úrovni pre umelú inteligenciu, ktorej najvýznamnejším výstupom sú Etické usmernenia pre dôveryhodnú umelú inteligenciu,[544] neskôr pretavených do praktického *Assessment List for Trustworthy AI* (ALTAI).[545]

V rámci EÚ autori citovaného článku vidia prenikanie etických pravidiel v troch oblastiach:

1) Etický výskum – vyžadovanie etických pravidiel pri výskume financovanom z prostriedkov EÚ;
2) Etické inovácie a správa – podpora a správa inovatívnych nových technológií by mala rešpektovať zaužívané etické pravidlá na úrovní celej spoločnosti a predmetné pravidlá by mali byť prirodzenou brzdou určitých inovácií;
3) Etický priemysel – priemysel pri vývoji nových technológií musí rešpektovať etické pravidlá. Tento cieľ dosahuje EÚ prostredníctvom štandardizácie a certifikácie.[546]

Zároveň autori prezentujú aj niektoré závery ohľadom vzťahu práva a etiky v kontexte regulácie IT. Výhodou etických pravidiel je, že sú flexibilnejšie a prijaté rýchlejšie ako legislatíva.[547] Podobný prístup vidieť pri otázkach regulácie dezinformácií, kde EÚ ako prvý krok rozhodla o prijatí kódexu správania pre veľké online platformy a následne sa diskutuje o legislatívnych pravidlách v tejto oblasti. Dôležitým bodom je, že etika môže obohatiť legislatívny proces a to takým spôsobom, že rešpektovanie etických hodnôt a dôraz na nich pri tvorbe práva by mal rezultovať v podobe dobrých zákonov.[548] Zároveň, ako už bolo naznačené vyššie, etické pravidlá idú častokrát mimo rozsah práva a preto je nevyhnutné

[543] VAN DIJK, N. – CASIRAGHI, S. – GUTWIRTH, S.: The 'Ethification' of ICT Governance. Artificial Intelligence and Data Protection in the European Union. In Computer law & security review 43 (2021), s. 2.
[544] Expertná skupina na vysokej úrovni pre umelú inteligenciu: Etické usmernenia pre dôveryhodnú umelú inteligenciu. Dostupné na: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_SK.pdf.
[545] AI HLEG - Assessment List for Trustworthy Artificial Intelligence (ALTAI) . Dostupné na: https://futurium.ec.europa.eu/en/european-ai-alliance/document/ai-hleg-assessment-list-trustworthy-artificial-intelligence-altai?language=sk.
[546] VAN DIJK, N. – CASIRAGHI, S. – GUTWIRTH, S.: The 'Ethification' of ICT Governance. Artificial Intelligence and Data Protection in the European Union. In Computer law & security review 43 (2021), s. 4 – 5.
[547] Tamže, s. 7.
[548] Tamže.

rešpektovať obe modality.[549] Autori taktiež uvádzajú, že diskusia o etických pravidlách obohacuje verejnú diskusiu ohľadom prijatia pravidiel správania sa.[550]

Môžeme teda zhrnúť, že etika je filozofická disciplína, ktorá skúma otázky dobra a toho čo je správne a nesprávne. Zároveň je ale etika aj modalitou regulácie spoločenských vzťahov. Aplikovaná etika rieši etické dilemy alebo konflikty hodnôt v konkrétnom kontexte a prípade. V poslednej dobe je evidentné prenikanie etických pravidiel do legislatívy, či už vo forme vyžadovania etickej expertízy pri prijímaní legislatívy alebo dohľade nad jej dodržiavaním či prostredníctvom vyžadovania súladu s etickými pravidlami pri určitých činnostiach.

V nasledujúcich častiach sa budeme venovať už konkrétne oblasti kybernetickej bezpečnosti, kde si zadefinujeme špecifické etické hodnoty a charakterizujeme typické etické dilemy a konflikty. Zároveň prezentujeme riešenie pre včasnú detekciu etických rizík v oblasti kybernetickej bezpečnosti.

8.2 Etické hodnoty v kybernetickej bezpečnosti

Kybernetická bezpečnosť nie je oblasťou, ktorej by bola z hľadiska etiky venovaná v literatúre špecifická pozornosť.[551] Výnimkou sú výstupy projektu CANVAS.[552] Kybernetická bezpečnosť však neuniká etickým dilemám a konfliktom medzi rôznymi hodnotami. Na jednej strane, prílišné zdôrazňovanie kybernetickej bezpečnosti môže porušovať základné ľudské práva a slobody a hodnoty v podobe rovnosti, spravodlivosti a súkromia. Naopak, zanedbanie kybernetickej bezpečnosti môže viesť ku nedôvere občanov v digitálnu infraštruktúru, tvorcov politík a štát. Kybernetická bezpečnosť sa nevyhýba etickým dilemám.

PRÍKLAD

Najčastejšie prezentovanou dilemou je súkromie verzus bezpečnosť. Na jednej strane kybernetická bezpečnosť je požiadavkou na ochranu údajov o jednotlivcoch. Na strane

[549] Tamže.
[550] Tamže, s. 8.
[551] Výnimka napríklad MACNISH, K. – VAN DER HAM, J.: Ethics in Cybersecurity research and practice. In *Technology in Society* 63 (2020).
[552] Project CANVAS. Dostupné na: https://cyberwatching.eu/projects/1267/canvas. CHRISTEN, M. et al. (eds): The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology, 21. Dordrecht: Springer, 2020, s. 49 – 50.

druhej, dostupnosť údajov pre rôzne osoby v rámci technických a organizačných opatrení znamená viac rizík pre dôvernosť údajov.

Ďalšími typickými etickými dilemami v oblasti kybernetickej bezpečnosti sú otázky prevedenia etického hackingu, zneužitie zraniteľnosti pred jej odstránením, vyvažovanie prístupu k údajom a súkromia pri citlivých dátach či využívanie šifrovania a vyšetrovanie trestných činoch.

Tieto konflikty stoja a padajú na stretnutí rôznych hodnôt, ktoré je potrebné vyvážiť a vzájomne rešpektovať. Van de Poel definuje základné hodnoty kybernetickej bezpečnosti a konceptualizuje ich do štyroch skupín:

- Bezpečnosť (*security*);
- Súkromie (*privacy*);
- Spravodlivosť (*fairness*); a
- Zodpovednosť (*accountability*).[553]

Prvou spomínanou skupinou hodnôt je samotná **bezpečnosť**. Bezpečnosť reflektuje situáciu, keď sú počítačové systémy bez kybernetických hrozieb. V rámci tejto skupiny môžeme hovoriť o bezpečnosti jednotlivca, ale aj v intenciách národnej bezpečnosti. Cieľ je totiž rovnaký: zabezpečiť počítačové systémy pred kybernetickými hrozbami. Van de Poel do tejto skupiny zahŕňa bezpečnosť ako ochranu proti náhodným nebezpečenstvám ako sú prírodné katastrofy (*safety*) a aj bezpečnosť pred úmyselnými útokmi (*security*). Kľúčové pri bezpečnosti je zachovanie hodnoty informačnej bezpečnosti, ktorá v súlade s už prezentovanými závermi spočíva v zachovaní dôvernosti, integrity a dostupnosti informačných aktív.[554]

Druhou skupinou hodnôt je **súkromie**. V literatúre zatiaľ neexistuje konsenzus pri definovaní a konceptualizácií súkromia. Ak ale hovoríme o kybernetickej bezpečnosti, dôraz je predovšetkým na informačnom súkromí, to znamená aké informácie o konkrétnom jednotlivcovi sa zdieľajú. Vhodnosť vyžadovania informácií o súkromí jednotlivca odzrkadľuje

[553] VAN DE POEL, I.: Core Values and Value Conflicts in Cybersecurity: Beyond Privacy versus Security. In CHRISTEN, M. et al. (eds): The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology, 21. Dordrecht: Springer, 2020, s. 49 – 50.
[554] Tamže, s. 50 – 53.

autonómiu jednotlivca a jeho rozhodovanie. Nie je tomu však vždy tak. Spracúvanie údajov bez súhlasu musí rešpektovať hodnoty dôstojnosti a dôvernosti, zachovávať anonymitu ak je to vhodné a taktiež uznávať ochranu osobnosti a identitu jednotlivca.[555]

Spravodlivosť predstavuje tretiu skupinu hodnôt. Najviditeľnejšie sa daná skupina hodnôt predstavuje v situácií, keď zvýšenie kybernetickej bezpečnosti nezasahuje všetkých jednotlivcov rovnakým spôsobom, čo samozrejme naráža na hodnoty spravodlivosti, rovnosti a nediskriminácie. Zároveň, niektoré opatrenia na zvýšenie kybernetickej bezpečnosti vyžadujú silnú legitimitu v demokratickom zriadení. Ilustrovať to možno na prípade trasovania kontaktov osôb pozitívne testovaných na COVID-19 a spracúvanie ich lokalizačných údajov. Dôležitým faktorom pri hodnote spravodlivosti je detekcia a prechádzanie skresleniam (tzv. *bias*) pri využívaní automatizovaných riešení. Rovina ochrany demokracie je osobitne dôležitá pri volebných procesoch a volebnej kampani.[556]

Poslednou skupinou hodnôt je **zodpovednosť**. Zodpovednosť je relevantná predovšetkým v oblasti kybernetickej bezpečnosti v dvoch situáciách. Prvá situácia sa týka vyvodzovania následkov pri spôsobení škody a ide tak o typickú kategóriu zodpovednosti v podobe *liability* alebo *responsiblity*. Ak niekto úmyselne poškodí počítačový systém, mal by byť braný na zodpovednosť. Druhá situácia sa týka vyžadovania zodpovedného prístupu (*accontability*) pri správe informačných aktív, ak je prítomný mocensky nevyvážený vzťah. Občania a užívatelia očakávajú od orgánov verejnej moci a poskytovateľov služieb, že budú chrániť a zabezpečovať poskytnuté údaje adekvátnym spôsobom. Predmetný aspekt zároveň reflektuje aj potrebu transparentnosti zo strany orgánov verejnej moci a poskytovateľov služieb voči jednotlivcom napríklad pri notifikácií bezpečnostných incidentov.[557]

[555] Tamže, s. 53 – 55.
[556] Tamže, s. 55 – 58.
[557] Tamže, s. 58 – 59.

Skupina hodnôt	Špecifikácia
BEZPEČNOSŤ	- Bezpečnosť jednotlivca - Národná bezpečnosť - Informačná bezpečnosť - Dôvernosť, integrita, dostupnosť
SÚKROMIE	- Autonómia - Dôstojnosť - Identita - Osobnosť - Anonymita - Dôvernosť
SPRAVODLIVOSŤ	- Spravodlivosť - Nediskriminácia - Rovnosť - Demokracia
ZODPOVEDNOSŤ	- *Accountability* - *Liability* - Transparentnosť - Vysvetliteľnosť

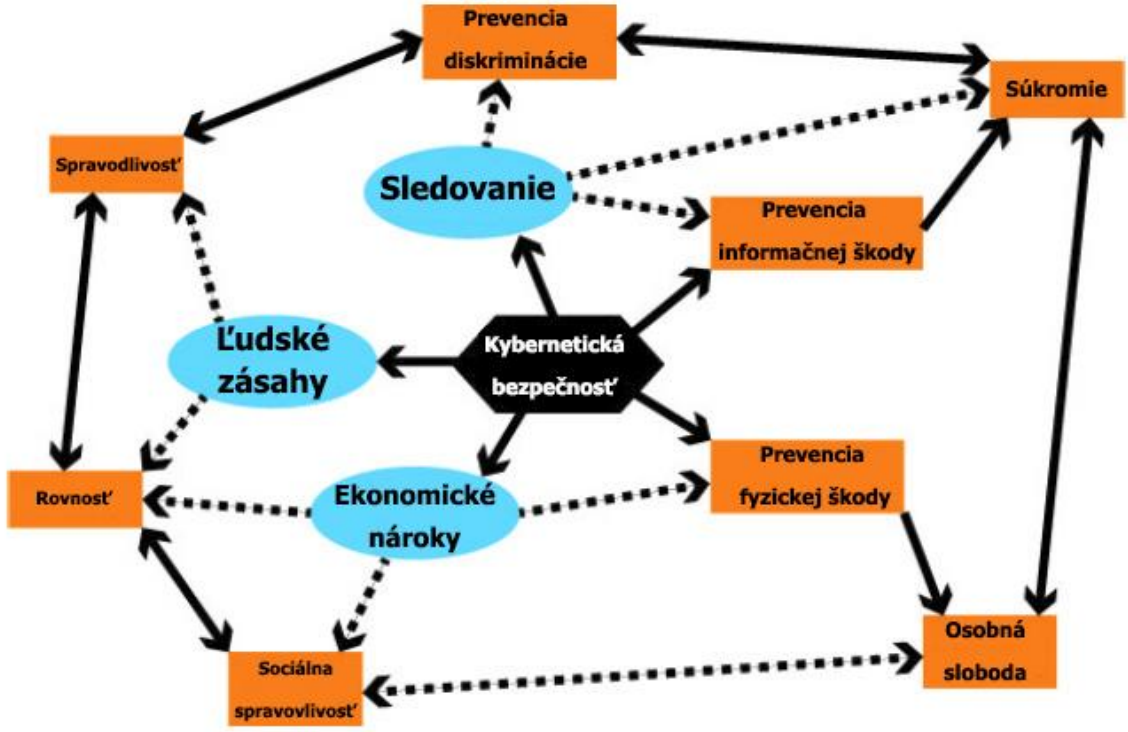
Tabuľka č. 4: Skupiny hodnôt a ich špecifikácia.[558]

8.3 Etické dilemy v kybernetickej bezpečnosti

Etické dilemy predstavujú situácie, keď sa etické hodnoty dostávajú do konfliktu. To znamená, že ich rešpektovanie by viedlo k protichodným záverom. Ak chceme v kybernetickej bezpečnosti rešpektovať hodnoty transparentnosti a dôvernosti, automaticky sa vylučujú, keďže ak je niečo transparentné, nemožno to považovať za dôverné a naopak. Dôležitú rolu pri etických dilemách v kybernetickej bezpečnosti hrá aj hlbšia špecifikácia hodnôt, nakoľko ako sme uviedli v predchádzajúcej stati, skupina hodnôt obsahuje viacero hodnôt, pričom nie vždy sa všetky dostávajú do konfliktných situácií. Zároveň je potrebné zohľadniť špecifický kontext.

[558] VAN DE POEL, I.: Core Values and Value Conflicts in Cybersecurity: Beyond Privacy versus Security.

Vzájomné vzťahy a konflikty pri etických hodnotách v kybernetickej bezpečnosti ilustrujeme na nasledujúcom obrázku prebratom z odbornej literatúry. Oranžové obdĺžniky reprezentujú hodnoty (chýba tu zodpovednosť, nakoľko pôvodný autor obrázka ju považuje za procedurálnu hodnotu). Plné šípky reprezentujú posilňujúci vzťah, prerušované šípky potenciálne konflikty.[559]



Obrázok č. 13: Konflikty etických hodnôt v kybernetickej bezpečnosti. [560]

Ako príklady konfliktu hodnôt v kybernetickej bezpečnosti sme z literatúry vybrali 5 konfliktov:

1) Súkromie verzus bezpečnosť;
2) Súkromie verzus spravodlivosť;
3) Súkromie verzus zodpovednosť;
4) Bezpečnosť verzus zodpovednosť;
5) Bezpečnosť verzus spravodlivosť (a demokracia).

[559] CHRISTEN, M. et al.: A Review of Value-Conflicts in Cybersecurity: An assessment based on quantitative and qualitative literature analysis. In *The ORBIT Journal*, Volume 1, Issue 1, 2017, s. 18 - 19.
[560] CHRISTEN, M. et al.: A Review of Value-Conflicts in Cybersecurity: An assessment based on quantitative and qualitative literature analysis. In *The ORBIT Journal*, Volume 1, Issue 1, 2017, s. 1-19.

Pre výklad a aplikáciu rôznych hodnôt v kybernetickej bezpečnosti dávame do pozornosti aj pomerne známy „*Menlo Report*" od Ministerstva obrany USA, ktorý poskytuje návod v oblasti výskumu informačných a komunikačných technológií. Predmetný dokument stojí na princípoch rešpektu k jednotlivcovi, prospešnosti, spravodlivosti a rešpektovaniu práva a verejného záujmu.[561]

Konflikt 1: Súkromie verzus bezpečnosť

Konflikt medzi hodnotami súkromia a bezpečnosti je najviac pertraktovaný v literatúre. Je však potrebné poznamenať, že dané hodnoty môžu byť v konflikte v rôznych situáciách a s rôznymi závermi. Uveďme niekoľko príkladov. V niektorých situáciách je bezpečnosť na úkor súkromia – napríklad pri všeobecnom monitorovaní počítačovej siete bez limitov, čo predstavuje invazívny zásah do súkromia. Zároveň, bezpečnosť môže pomôcť pri dosahovaní väčšieho súkromia – limitované sledovanie dátových tokov pôsobí preventívne voči bezpečnostným incidentom a týmto spôsobom chráni súkromie užívateľov. Taktiež platí, že kybernetická bezpečnosť je podmienkou súkromia, nakoľko bezpečnostné opatrenia zabezpečujú rešpektovanie vôle jednotlivca pri nastavení toho, čo chce zdieľať a čo už nie. V iných situáciách sa súkromie dosahuje na úkor bezpečnosti – anonymita a úplná dôvernosť môže byť zneužitá pre páchanie protiprávneho konania. V neposlednom rade súkromie prispieva k bezpečnosti – ak určitá informácia je považovaná za dôvernú, pri phisingových útokoch už nemôžu útočníci využiť nadmerné množstvo dostupných informácií o používateľovi pre výber ďalšieho útoku.[562]

Ako je z vyššie uvedených situácií zrejmé, hodnoty súkromia a bezpečnosti sa nie vždy nevyhnutne musia dostať do konfliktu. Dilema nastáva spravidla pri dvoch situáciách: (i) všeobecnom monitorovaní siete za účelom bezpečnosti, ale s invazívnym narušením súkromia a (ii) úplná anonymita a dôvernosť ide na úkor bezpečnosti. Z tohto dôvodu pri riešení týchto konfliktov je absolútne nevyhnutné klásť si otázky týkajúce sa kvantity

[561] US DEPARTMENT OF HOMELAND SECURITY: The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research. 2012. Dostupné na: https://www.dhs.gov/sites/default/files/publications/CSD-MenloPrinciplesCORE-20120803_1.pdf.

[562] VAN DE POEL, I.: Core Values and Value Conflicts in Cybersecurity: Beyond Privacy versus Security. In CHRISTEN, M. et al. (eds): The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology, 21. Dordrecht: Springer, 2020, s. 62.

a kategórií spracúvaných údajov na účely bezpečnosti, dostupnosť údajov pre konkrétne osoby, doby uchovávania či efektívne využívanie súhlasu dotknutých osôb.[563] Na riešenie týchto otázok je však nevyhnutné využívanie tzv. Privacy Enhancing Technologies (PETs), čiže adekvátnej infraštruktúry.

Konflikt 2: Súkromie verzus spravodlivosť

Vzťah medzi hodnotami súkromia a spravodlivosti môže byť podporný (dopĺňajúci sa) alebo konfliktný. Súkromie a spravodlivosť sa dopĺňajú v dvoch prípadoch. Prvým prípadom je, že súkromie limituje rozsah spracúvaných údajoch o jednotlivcoch a tým bráni nespravodlivému zaobchádzaniu s nimi. Druhým prípadom je, že určitý stupeň súkromia sa vyžaduje aj pre politických reprezentantov vo fungujúcej demokracii.

Zároveň, hodnoty súkromia a spravodlivosti môžu byť konfliktné a predmetom dilem. Ilustrovať to možno na príkladoch povinného poskytovania údajov občanov orgánom verejnej moci nerovnomerným spôsobom napríklad pri daňových priznaniach. Zároveň, je určitý stupeň transparentnosti dôležitý pri rozhodnutiach orgánoch verejnej moci, čo môže narušiť súkromie verejných funkcionárov.[564]

Konflikt 3: Súkromie verzus zodpovednosť

Hodnoty súkromia a zodpovednosti sú častokrát v konflikte. Ak chceme jednotlivca alebo určitý orgán brať na zodpovednosť, potrebujeme na to penzum informácií, ktoré sa môžu týkať súkromia a rozhodovania. Predmetný konflikt je najviac viditeľný v prípadoch rozhodnutí verejných funkcionárov alebo orgánov verejnej moci, za ktorý vždy niekto musí zodpovedať bez ohľadu na etickú, právnu alebo politickú rovinu zodpovednosti. Pri tomto konflikte je kľúčové determinovať a opatrne vyvážiť rozsah zverejňovaných informácií.[565]

Konflikt 4: Bezpečnosť verzus zodpovednosť

Nedostatok opatrení na zabezpečenie kybernetickej bezpečnosti by malo mať za následok vyvodenie zodpovednosti. Opačným prípadom je, ak transparentnosť a zodpovednosť vyžaduje publikáciu zavedených opatrení na prevenciu kybernetických rizík

[563] Tamže, s. 63-64.
[564] Tamže, s. 64.
[565] Tamže, s. 65 -66.

a tým riziko ohrozenia *de facto* zvyšuje. Podobným prípadom je odhalenie zraniteľností etickými hackermi, ktorý sa rozhodnú zraniteľnosť zverejniť pred spoluprácou a odstránením chýb zo strany orgánu verejnej moci.

Riešením na vhodné vybalansovanie týchto hodnôt je kreovanie fór, ktoré budú efektívne schopné situáciu riešiť. Ako príklad možno uviesť parlamentné výbory alebo expertné skupiny a komisie.[566]

Konflikt 5: Bezpečnosť verzus spravodlivosť (a demokracia)

Bezpečnosť a spravodlivosť môžu byť typicky v konflikte, ak sa štát rozhodne implementovať rôzne sledovacie mechanizmy na monitorovanie svojich obyvateľov pre účely národnej bezpečnosti alebo ochrany života a zdravia. Spomínané nástroje je vždy potrebné vyvážiť zárukami proti zneužitiu.[567]

8.4 Posúdenia etických rizík v kybernetickej bezpečnosti

Po predstavení základných etických hodnôt a potenciálnych konfliktov v oblasti kybernetickej bezpečnosti je na mieste úvaha, ako opatrenia a postupy v oblasti kybernetickej bezpečnosti vykonávať „eticky."

Podľa nášho názoru je vhodné vykonanie posúdenia etických rizík (*ethics assessment*) a následná implementácia jeho záverov do organizácie. Posudzovanie rizík nie je v oblasti kybernetickej bezpečnosti ničím novým. Odlišnosťou etického posúdenia je však sústredenie a etické hodnoty a dilemy namiesto hodnotenia iba bezpečnostných opatrení a ich súladu s legislatívou či technickými štandardmi.

Prirodzene, existuje viacero metodológií prístupu k posúdeniu etických rizík.[568] Vhodné posúdenie etických rizík by podľa nášho názoru malo obsahovať viacero fáz a konkrétnych krokov. Ilustrujeme to na nasledujúcom postupe.

[566] Tamže, s. 66.
[567] Tamže, s. 67.
[568] Pozri napríklad LOI, M. – CHRISTEN, M.: Ethical Frameworks for Cybersecurity. In CHRISTEN, M. et al. (eds): The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology, 21. Dordrecht: Springer, 2020, s. 73 – 95.

PRÍKLAD

1. FÁZA: Uvedomenie si potreby etického posúdenia a jeho príprava

- Etické posúdenie by nemali byť reaktívne t.j. nasledovať až po bezpečnostnom incidente alebo identifikácií zásadnej zraniteľnosti;
- Etické poúdenie nie je kontrolný zoznam, ktorý sa odškrtá a problém je vyriešený. Ide skôr o kontinuálnu činnosť a zmenu myslenia nad etickými dilemami, ktoré v oblasti kybernetickej bezpečnosti môžu nastať;
- Etické posúdenie by mal vykonať dostatočne odborne pripravená skupina ľudí vrátane etikov, inžinierov, právnikov či informatikov. Vhodná skladba tímu je základom pre získanie relevantných výsledkov.

2. FÁZA: Posúdenie etických rizík

- Za vhodný úvodný krok považujeme zasadenie do etického a legislatívneho rámca. To znamená preskúmanie, či sa na organizáciu vzťahujú niektoré etické usmernenia, kódexy alebo legislatíva a posúdenie rámcovať týmito požiadavkami;
- Etické posúdenie by malo obsahovať aj identifikáciu zainteresovaných strán (*stakeholders*), ktorých sa hodnotená technológia alebo proces dotýka.
- Vymedzili sme si základné etické hodnoty a dilemy v kybernetickej bezpečnosti. Tieto hodnoty a dilemy je potrebné preskúmať a diskutovať v konkrétnom kontexte a situácií s posudzovaným subjektom.
- Výsledkom by malo byť definovanie tzv. *red flags* a etických rizík, ktoré je potrebné v organizácií vyriešiť.

3. FÁZA: Implementácia záverov

- Závery etického posúdenia je potrebné pretaviť do praxe. Možností je niekoľko a vždy budú závisieť od konkrétnej organizácie a jej možností. Ako príklady možno uviesť kreovanie etickej komisie alebo určenie etického experta v organizácií, zavedenie dodatočných záruk pre jednotlivcov, etických pravidiel alebo zvýšenie informovanosti verejnosti a dotknutých jednotlivcoch. Ideálnym je systematická zmena v dizajne produktov alebo procesoch pri vytváraní nových technológií.

9. ADMINISTRATÍVNOPRÁVNA ZODPOVEDNOSŤ V KYBERNETICKEJ BEZPEČNOSTI - VŠEOBECNÁ ČASŤ

Táto kapitola je vystavaná ako teoreticko-právny základ pre ďalší výklad administratívnoprávnej zodpovednosti v oblasti kybernetickej bezpečnosti. Jej cieľom je systematicky vymedziť základné pojmy, princípy, druhy správnych deliktov, všeobecné podmienky zodpovednosti a procesné východiská správneho trestania tak, aby čitateľ získal ucelený rámec potrebný na porozumenie osobitnej právnej úprave vyvodzovania administratívnoprávnej zodpovednosti. Výklad sa sústreďuje na všeobecné inštitúty správneho práva trestného, no zároveň sa neobmedzuje len na abstraktnú rovinu. Priebežne pracuje aj s príkladmi a odkazmi na sektorové predpisy kybernetickej bezpečnosti, čím sa všeobecná teória prepája s osobitnou reguláciou. Význam tejto časti spočíva v ustálení metodologického a pojmového aparátu, ktorý bude v nasledujúcej osobitnej časti aplikovaný na konkrétne právne predpisy tvoriace jadro právnej úpravy kybernetickej bezpečnosti. Konkrétne na ZoKB a ZoITVS.[569]

9.1 Pojem a funkcie administratívnoprávnej zodpovednosti

Fenomén zodpovednosti siaha k počiatkom spoločnosti. Slovník k heslu **zodpovednosť** poskytuje výklad, v ktorého v zmysle ide *o vedomie o následkoch činu, konania* resp. *povinnosť niesť následky za nejaký čin.*[570] Zužujúci pojem **právna zodpovednosť** patrí medzi základné právne inštitúty. V najširšom zmysle znamená povinnosť niesť právne následky vlastného konania alebo opomenutia konania. V rámci právnej zodpovednosti tieto následky nastupujú vtedy, keď sa poruší právna povinnosť alebo vznikne stav, s ktorým zákon spája nepriaznivý následok napr. nesplnenie povinnosti nahlásiť kybernetický bezpečnostný incident alebo uvedenie nepravdivých informácií pri zápise do registra PZS. Ak by právo

[569] Informácia o využívaní nástrojov umelej inteligencie: Pri spracovaní tejto kapitoly bol použitý nástroj umelej inteligencie ChatGPT (GPT-5.4 Thinking) ako pomocný nástroj v rámci autorom riadeného pracovného postupu. Jeho použitie malo podporný charakter a uskutočňovalo sa na základe pokynov autora, jeho priebežnej spätnej väzby, kontroly a následnej autorskej úpravy. Za koncepciu kapitoly, jej štruktúru, metodologické východiská, výber zdrojov, odbornú argumentáciu, právne závery a výslednú podobu textu zodpovedá výlučne autor.

[570] *Slovník slovenského jazyka.* V. V – Ž. Red. Š. Peciar. 1. vyd. Bratislava: Vydavateľstvo SAV 1965. 848 s.(kolektív autorov: V. Budovičová, K. Buzássyová, J. Kačala, O. Kajanová, V. Šulcová, F. Kočiš, Š. Peciar, Š. Michalus, M. Pisárčiková, V. Slivková, E. Smiešková, M. Šalingová, M. Urbančok, J. Kačala, Š. Vragaš).

nebolo tvorené inštitútom zodpovednosti, jeho normy by sa oslabili. V mnohých prípadoch by ostali iba formálnym príkazom bez skutočnej vynútiteľnosti. Z hľadiska štruktúry právnej normy je vynútiteľnosť tvorená jednou z jej častí v rámci trichotomickej výstavbou. Obsahuje hypotézu, dispozíciu a **sankciu.** Právna zodpovednosť však nie je len otázkou postihu. Je aj prostriedkom ochrany **zákonnosti**[571], rešpektu k právu a zárukou plynulého výkonu verejnej správy.

V systéme verejného práva má **administratívnoprávna zodpovednosť** osobitné postavenie. Ide o taký druh zodpovednosti, ktorý sa spája s porušením povinností upravených normami **správneho práva – administratívnoprávnymi normami resp. administratívnymi normami**. Uplatňuje ju orgán verejnej správy. Jej zmyslom je chrániť **verejný záujem** a zabezpečiť účinnosť správnoprávnej regulácie.[572] Administratívnoprávnu zodpovednosť nemožno chápať výlučne ako technický nástroj sankcionovania. Ide o širší právny mechanizmus, prostredníctvom ktorého štát presadzuje dodržiavanie právnych povinností v oblastiach dôležitých pre **verejný poriadok** (dodržanie povinnosti vykonať nápravné opatrenie uložené správnym orgánom), **bezpečnosť** (kybernetická bezpečnosť – predchádzanie, potláčanie, a evidencia kybernetických bezpečnostných incidentov) a **riadny výkon verejnej správy** (v našom prípade vynútiteľnosť noriem, dohľad nad vedením registrov, participáciou s orgánmi verejnej správy).[573]

Administratívnoprávna zodpovednosť je vnútorne diferencovaná. Zahŕňa viacero foriem, ktoré sa odlišujú svojím účelom aj spôsobom uplatnenia. Pre základný výklad treba rozlišovať najmä **deliktuálnu administratívnoprávnu zodpovednosť, disciplinárnu zodpovednosť** a v širšom metodologickom rámci aj **zodpovednosť za výkon verejnej správy**[574].

Deliktuálna zodpovednosť označovaná aj ako **zodpovednosť za správne delikty**[575] sa viaže na porušenie správnoprávnej povinnosti. Jej typickým prejavom je uloženie sankcie za **správny delikt**. Práve táto forma zodpovednosti tvorí jadro **správneho trestania**. V praxi ide o najviditeľnejší prejav represívnej právomoci verejnej správy voči spravovaným

[571] *Vrabko, M. a kol.* Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava : Ch. H. Beck, 2025, s. 197 – 198.
[572] *Horvat, M.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 18.
[573] *Prášková, H.* Základy odpovědnosti za správní delikty. 1. vydání. Praha : C. H. Beck, 2013, s. 17.
[574] *Vrabko, M. a kol.* Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava : Ch. H. Beck, 2025, s. 198.
[575] *Vrabko, M. a kol.* Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava : Ch. H. Beck, 2025, s. 200.

subjektom. Delikty a sankcie s nimi spojené tvoria osobitnú časť právnej úpravy kybernetickej bezpečnosti. Sú označované ako priestupky, alebo správne delikty.

Disciplinárna zodpovednosť má odlišný základ. Uplatňuje sa tam, kde existuje osobitný služobný, pracovný alebo profesijný vzťah. Jej cieľom je chrániť riadny výkon služby, funkcie alebo povolania. Zároveň slúži na udržiavanie vnútornej disciplíny v určitom organizačnom alebo profesijnom prostredí. Je typická napr. pre výkon súdnictva ale aj výkon verejnej správy a to najmä v prípade porušenia interných predpisov, alebo nerešpektovania pokynov nadriadeného. Veľmi úzko je previazaná najmä s vnútornými zodpovednostnými vzťahmi naviazanými na plnenie povinnosti orgánu verejnej správy v súvislosti s aplikáciou ZoITVS. Má vnútroorganizačný charakter. V tomto smere sa odlišuje od všeobecnej deliktuálnej zodpovednosti. Nie je určená pre neurčitý okruh osôb, ale pre osoby viazané osobitným právnym režimom.

Osobitné miesto má aj **zodpovednosť za výkon verejnej správy**. Tá sa netýka postihu adresáta povinnosti vyplývajúcej z noriem správneho práva. Týka sa následkov postupu samotnej verejnej správy. Nastupuje najmä vtedy, keď orgán verejnej moci rozhoduje nezákonne alebo postupuje nesprávne. V takom prípade nenesie následky spravovaný subjekt, ale spravujúci subjekt. Následkom je povinnosť spravujúceho subjektu (správneho orgánu) nahradiť škodu spravovanému subjektu (účastníkovi konania). Deje sa tak napr. v prípade, kedy správny orgán vydá rozhodnutie, (napr. prijatie opatrenia na nápravu) ktorým zamedzí činnosť PZS, čím zasiahne do jeho ekonomickej aktivity a neskôr sa preukáže, že rozhodnutie orgánu verejnej správy bolo nezákonné. To v konečnom dôsledku vedie k stavu, v ktorom rozhodnutím orgánu verejnej správy vznikla PZS škoda, ktorú je potrebné nahradiť. Aj keď nejde o správne trestanie, z metodologického hľadiska ide stále o dôležitú súčasť širšieho rámca administratívnoprávnej zodpovednosti osobitne v prípade regulácie kybernetickej bezpečnosti, kedy rozhodnutie správneho orgánu môže mať pre účastníka konania nedozierne následky. Aj tu totiž právo reaguje na porušenie pravidiel výkonu verejnej správy. Do popredia vystupuje reparačná funkcia vyvodzovania zodpovednosti vo forme náhrady škody za nezákonný výkon verejnej správy.[576]

S pojmom **zodpovednosť** sa nutne spája aj pojem **zavinenie**. Zavinenie je vnútorný psychický vzťah páchateľa k protiprávnemu konaniu a k jeho následku. Vyjadruje, či osoba

[576] Bližšie pozri: zákon č. 514/2003 Z. z. o zodpovednosti za škodu spôsobenú pri výkone verejnej moci a o zmene niektorých zákonov

konala úmyselne alebo z nedbanlivosti. Tento pojem je dôležitý najmä pri **subjektívnej zodpovednosti**. Teda tam, kde zákon vyžaduje, aby sa pri posudzovaní zodpovednosti skúmal aj vnútorný vzťah osoby k jej konaniu.[577] Je založené na vôľovej (chcieť) a intelektuálnej zložke (vedieť).[578]

V kontexte zavinenia možno rozlišovať dva základné modely zodpovednosti. **Subjektívnu** a **objektívnu zodpovednosť**.

I. Subjektívna zodpovednosť

Pri subjektívnej zodpovednosti sa **vyžaduje zavinenie**. Nestačí, že vznikol protiprávny výsledok. Treba skúmať aj to, či osoba konala úmyselne alebo z nedbanlivosti. Pre tento model sú typické tieto predpoklady:

1. **porušenie právnej povinnosti**,
2. **škodlivý alebo protiprávny následok**,
3. **príčinná súvislosť** medzi konaním a následkom,
4. **zavinenie**.

Tento model sa uplatňuje najmä pri **trestných činoch, priestupkoch** a vo viacerých prípadoch **zodpovednosti za škodu** v súkromnom práve. Je postavený na myšlienke, že právny poriadok spravidla reaguje prísnejšie tam, kde možno osobe vytknúť aj jej vnútorný vzťah ku konaniu.

II. Objektívna zodpovednosť

Pri objektívnej zodpovednosti sa **zavinenie nevyžaduje**. Rozhodujúce je najmä to, že vznikol **protiprávny stav** alebo že boli naplnené znaky deliktu určené zákonom. Tento model je častý tam, kde právna úprava sleduje vysokú mieru ochrany verejného záujmu alebo potrebu efektívnej regulácie. Tieto kritéria napĺňa ZoKB ale aj ZoITVS. V mnohých prípadoch zákon pripúšťa **liberačné dôvody**. To znamená, že zodpovedný subjekt sa môže zodpovednosti zbaviť, ak preukáže zákonom určené okolnosti. Niekedy sa však uplatňuje aj prísnejší model, pri ktorom sa oslobodenie od zodpovednosti nepripúšťa. Deje sa tak v prípade skutkových podstát opísaných v ZoKB a ZoITVS, ktoré sú vo svojej architektúre veľmi striktné, čo je logické vzhľadom na povahu regulácie. Pre potrebu našej učebnice je ďalším argumentom v prospech

[577] Bližšie pozri: *Horvat, M.* § 3 [Zavinenie]. In: *Srebalová, M. a kol.* Zákon o priestupkoch. 2. vydanie. Bratislava: C. H. Beck, 2020, s. 16–23.

[578] *Hamuľáková, Z.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 96 s.

vyvodzovania objektívnej zodpovednosti aj skutočnosť, že ZoKB ale aj ZoITVS spravidla regulujú špeciálne subjekty (v tomto prípade ich môžeme označiť aj ako profesionálne subjekty), pri ktorých je vysoká naliehavosť znalosti a správnej aplikácie sektorovej regulácie. Objektívna zodpovednosť je typická najmä pre **správne delikty právnických osôb** a **správne delikty podnikajúcich fyzických osôb**. Vyskytuje sa aj v niektorých oblastiach súkromného práva.[579]

S administratívnoprávnou zodpovednosťou úzko súvisí pojem **správne právo trestné**. Ide o tú časť správneho práva, ktorá upravuje **správne delikty, sankcie za ne, zásady ukladania sankcií** a **konanie o správnom delikte**.

Na pojem **správne právo trestné** bezprostredne nadväzuje pojem **správne trestanie** – ten predstavuje proces, v ktorom príslušný orgán zisťuje, či bol spáchaný správny delikt, a následne rozhoduje o sankcii. Medzi týmito pojmami treba rozlišovať. [580] **Správne právo trestné** predstavuje širší normatívny rámec. **Správne trestanie** je praktická a procesná realizácia správneho práva trestného. Jeden pojem označuje právnu úpravu. Druhý označuje rozhodovaciu činnosť orgánu verejnej moci.

Práve v oblasti správneho práva trestného sa výrazne prejavuje **represívny charakter verejnej správy**. Verejná správa neplní len organizačné a kontrolné úlohy. Má aj právomoc autoritatívne reagovať na porušenie právnych povinností. Túto právomoc vykonáva najmä ukladaním sankcií. **Represívny charakter verejnej správy** však nemožno chápať ako samoúčelný. Represia nie je cieľom verejnej správy. Je iba **prostriedkom**, ktorý má zabezpečiť ochranu verejného záujmu (zabezpečenie a udržateľnosť kybernetickej bezpečnosti), vynútiteľnosť právnych povinností (určenie manažéra kybernetickej bezpečnosti, alebo určenie zástupcu poskytovateľa s trvalým pobytom, alebo sídlom na území SR) a rešpekt k zákonu (uloženie poriadkovej pokuty za neplnenie povinností podľa ZoKB počas výkonu kontroly). Pre potrebu ich zabezpečenia je spravujúci orgán **dotovaný verejnomocenskými oprávneniami** – ukladá sankcie a vyžaduje resp. vynucuje si ich plnenie – nútený výkon. **Správne právo trestné nastupuje najmä vtedy, keď iné nástroje, ako prevencia, kontrola alebo nápravné opatrenia, nepostačujú.**

[579] *Vrabko, M. a kol.* Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava : Ch. H. Beck, 2025, s. 200.
[580] *Horvat, M.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 19 - 20.

Z funkčného hľadiska slúži inštitút administratívnoprávnej zodpovednosti na plnenie viacerých úloh spojených s ochranou verejného a individuálneho záujmu a výkonom verejnej správy. Sú to:

1. **regulatívna funkcia** – určuje, ktoré správanie je možné považovať za deliktuálne,
2. **preventívna funkcia** – pôsobí odstrašujúco a vedie k dodržiavaniu pravidiel,
3. **ochranná funkcia** – chráni verejný záujem, verejný poriadok a zákonnosť,
4. **represívna funkcia** – reaguje na porušenie povinnosti uložením sankcie,[581]
5. **stabilizačná funkcia** – posilňuje istotu a predvídateľnosť vo verejnoprávnych vzťahoch,
6. **reparačná funkcia** – odstraňuje alebo zmierňuje následky protiprávnych činov.

Tieto funkcie sa navzájom dopĺňajú. Administratívnoprávnu zodpovednosť preto nemožno chápať len ako nástroj postihu. Opätovne zdôrazňujeme, že je aj prostriedkom, ktorým štát udržiava riadne fungovanie verejnej správy a podporuje rešpekt k právnym pravidlám.

9.2 Správne právo trestné a správne trestanie

V slovenskej teórii sa **správne právo trestné** označuje ako subsystém správneho práva, pre ktorý je typický zodpovednostný právny vzťah vo verejnej správe. Rozdeľ medzi správnym právom a správnym právom trestným spočíva najmä **v represívnom charaktere** správneho práva trestného. Z hľadiska právnych vzťahov správne právo trestné upravuje vzťahy medzi správnym orgánom [spravujúci subjekt – napr. NBÚ, MIRRI SR (orgán vedenia)] a obvineným zo spáchania správneho deliktu [spravovaný subjekt – napr. PZS, alebo orgán riadenia] a to v kontexte rozhodovania o vine a sankcii za spáchané protiprávne konanie nesúce znaky správneho deliktu.[582] Okrem týchto dvoch subjektov v konaní môže ešte vystupovať rad subjektov ako napr. poškodený, osoba povinná vydať vec ale aj zúčastnené osoby, ako svedok či súdny znalec. Správne právo trestné predstavuje subsystém, v ktorom správne orgány vyvodzujú administratívnoprávnu zodpovednosť voči spravovaným subjektom za účelom poskytnutia mocenskej ochrany riadneho, plynulého a nerušeného fungovania verejnej správy (vedenia príslušných registrov, dodržiavania protokolov, hlásenia

[581] *Horvat, M.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 16 - 17.
[582] *Vrabko, M. a kol.* Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava : Ch. H. Beck, 2025, s. 200.

určitých skutočností, poskytovania súčinnosti a pod.). Správne právo trestne spravidla nadväzuje na iné činnosti správnych orgánov ako je napr. výkon kontroly alebo dozoru.[583] Čo je veľmi prítomné v ZoKB najmä v kontexte novelizácie pod vplyvom smernice NIS2, kde sa posilňujú kontrolné a dozorové kompetencie NBÚ.

Správne právo trestné sa nevyčerpáva iba uložením sankcie. Nemožno ho zužovať ani na samotné konanie o správnom delikte. Jeho obsah je širší. Zahŕňa právnu úpravu:

1. **princípov správneho práva trestného,**
2. **zásad ukladania sankcií,**
3. **správnych deliktov,**
4. **subjektov administratívnoprávnej zodpovednosti,**
5. **predpokladov vzniku zodpovednosti,**
6. **sankcií a ochranných opatrení,**
7. a tiež **procesných pravidiel,** podľa ktorých sa o správnom delikte rozhoduje.

V tomto zmysle predstavuje správne právo trestné **ucelený normatívny rámec,** ktorý určuje:

1. **čo je správny delikt** – neudržiavanie bezpečnostnej dokumentácie;
2. **kto zaň môže zodpovedať** – PZS;
3. **za akých podmienok možno zodpovednosť vyvodiť** – ak sa stane bezpečnostná dokumentácia neaktuálna a
4. **aký právny následok môže správny orgán uložiť** – sankcia od 300 do 500 000 eur.

Obsah právnych vzťahov upravených týmto subsystémom správneho práva je súhrn práv a povinností, ktoré určujú či je osoba obvinená zo spáchania správneho deliktu páchateľom deliktu a ak je páchateľom tak aj to aká sankcia ju za jej deliktuálne konanie postihne.[584]

Z dogmatického hľadiska tak správne právo trestné vystupuje ako osobitný subsystém správneho práva, ktorého predmetom nie je len represia. Jeho predmetom je predovšetkým **právna regulácia verejnoprávnej reakcie** na porušenie administratívnoprávnych povinností. Táto reakcia musí byť zákonná, predvídateľná a viazaná

[583] *Prášková, H.* Základy odpovědnosti za správní delikty. 1. vydání. Praha : C. H. Beck, 2013, s. 17.
[584] *Horvat, M.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 15.

na splnenie zákonných podmienok. Sankcia je len jedným z jej prejavov. Prioritu predstavuje udržiavanie zákonného stavu.

Predmet správneho práva trestného tvoria spoločenské vzťahy vo verejnej správe, ktoré vznikajú v súvislosti s vyvodzovaním administratívnoprávnej zodpovednosti.[585] Sú tvorené vymedzením **správnych deliktov**, určením **subjektov zodpovednosti**, úpravou a uložením **sankcií a ochranných opatrení** a právnou úpravou ich **prejednávania**. Ide o tú časť správneho práva, ktorá upravuje verejnoprávnu reakciu na porušenie administratívnoprávnych povinností.

Správny delikt je charakterizovaný ako *protiprávne konanie, ktorého znaky ustanovuje zákon, a za ktoré orgán verejnej správy ukladá sankcie ustanovené administratívnou normou.*[586]

Medzi všeobecné pojmové znaky správneho deliktu zaraďujeme:

1. **protiprávne konanie** – aktívny alebo pasívny prejav ľudskej vôle vo vonkajšej realite smerujúci proti právom chránenému záujmu;
2. **sankcionovateľnosť** – hrozba uloženia sankcie vychádzajúca zo spáchania deliktu;
3. **zodpovedná osoba** – subjekt správneho deliktu – subjekt, ktorý je spôsobilý niesť zodpovednosť[587];
4. **zavinenie** (okrem prípadov správneho deliktu, kde sa nevyžaduje zavinenie) – vnútorný psychický stav páchateľa k svoju protiprávnemu konaniu a jeho následku. Môže ísť o:
    a. **úmyselné konanie** – priamy / nepriamy úmysel,
    b. **nedbanlivostné konanie** – vedomá / nevedomá nedbanlivosť;
5. **spoločenská škodlivosť činu** – nebezpečnosť činu pre spoločnosť vo forme porušenia alebo ohrozenia verejného záujmu, alebo právom chráneného záujmu;

[585] *Horvat, M.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 19.

[586] *Trellová, L. (ed.)* Nový správny súdny poriadok: návrh. Zborník z medzinárodnej konferencie konanej v dňoch 25. až 27. septembra 2014 v Dunajskej Strede. Bratislava Univerzita Komenského Právnická fakulta, 2014, s. 305. poznámka pod čiarou prebratá z *Vrabko, M. a kol.* Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava : Ch. H. Beck, 2025, s. 204.

[587] Pozn.: Znak **zodpovedná osoba** je previazaný s inštitútom **deliktuálnej spôsobilosti** – k schopnosti byť subjektom povinností, ktoré vzniknú v dôsledku porušenia povinností ale tiež v schopnosti tieto povinnosti právne relevantne porušiť. Pozri: *Prášková, H.* In *Hendrych, D. a kol.* Správni právo Obecná část. Praha : C. H. Beck, 2009, s. 173. Informácia a odkaz prevzatý z: *Vrabko, M. a kol.* Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava : Ch. H. Beck, 2025, s. 207.

6. **ustanovenie znakov skutkovej podstaty v zákone** – súhrn typových znakov konania, ktoré vyjadrujú jeho spoločenskú škodlivosť a odlišujú jednotlivé druhy správnych deliktov navzájom. Znaky skutkovej podstaty sú:
    a. **objekt –** právom chránený záujem,
    b. **objektívna stránka –** vonkajšia charakteristika deliktu: **konanie → následok = príčinná súvislosť** tzv. *kauzálny nexus*,
    c. **subjekt** – zodpovedná osoba,
    d. **subjektívna stránka –** zavinenie.[588]

9.3 Znaky skutkovej podstaty

Pri vyvodzovaní administratívnoprávnej zodpovednosti sa osobitný význam kladie na tzv. znaky skutkovej podstaty. Ich naplnenie je predpokladom pre úspešné vyvodenie administratívnoprávnej zodpovednosti za spáchaný delikt. Táto podkapitola všeobecnej časti je osobitne dôležitá v kontexte osobitnej časti, v ktorej skúmame znaky skutkovej podstay v súvislosti s jednotlivými deliktmi upravenými v ZoKB a ZoITVS. Skutková podstata je definovaná **štyrmi obligatórnymi znakmi**:

1. **Objektom,**
2. **objektívnou stránkou,**
3. **subjektom a**
4. **subjektívnou stránkou.**

I. Objekt ako znak skutkovej podstaty spočíva v skutočnosti, že ak má byť nejaké konanie trestné musí proti niečomu smerovať. Pri definovaní objektu **rozlišujeme:**

1. **všeobecný objekt,**
2. **druhový objekt a**
3. **individuálny objekt.**

Všeobecným objektom sa rozumie súhrn chránených spoločenských vzťahov, záujmov a právnych hodnôt. Pri definovaní objektu dochádza k rozlišovaniu skutku, ktorý je trestným činom od skutku, ktorý je správnym deliktom. Vo všeobecnosti platí, že **všeobecným objektom trestných činov** je ochrana základných ľudských práv a hodnôt –

[588][588] Bližšie pozri: *Vrabko, M. a kol.* Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava : Ch. H. Beck, 2025, s. 204 - 2011.

život, zdravie, majetok. V prípade **všeobecného objektu správnych deliktov** je to **nerušený výkon verejnej správy**. Definovanie a skúmanie objektu správneho deliktu je dôležité pre ujasnenie toho čo má byť predmetom ochrany prostredníctvom správneho práva trestného ako aj pre náležitú formuláciu skutkových podstát správnych deliktov. Správne právo trestné nechráni všetky spoločenské záujmy. Chráni ich fragmenty odvoditeľné zo správnych noriem.[589] Všeobecný objekt správnych deliktov môžeme čiastočne odvodiť z úvodného ustanovenia Zákona o priestupkoch spočívajúci v **ochrane plnenia úloh verejnej správy, verejného poriadku a občianskeho spolunažívania**.[590] To platí aj v kotnexte ZoKB a ZoITVS.

Druhový objekt predstavuje širšiu kategóriu chráneného záujmu, ktorá vyjadruje to, čo je spoločné pre individuálne objekty jednotlivých správnych deliktov. Nejde teda o konkrétny záujem dotknutý pri jednom delikte, ale o spoločný okruh hodnôt a vzťahov, ktoré sú chránené v určitej vecnej oblasti verejnej správy. Práve tento spoločný základ umožňuje, aby sa jednotlivé skutkové podstaty správnych deliktov systematicky zoskupovali a vnútorne triedili. **Druhový objekt plní významnú systematizačnú funkciu**, keďže vytvára základ pre členenie a usporiadanie jednotlivých kategórií deliktov. Na tomto princípe je postavená napríklad aj osobitná časť Zákona o priestupkoch[591], ktorá zoskupuje priestupky podľa toho, aký druh verejnoprávne chráneného záujmu je ich spáchaním porušený alebo ohrozený.[592] PriesZ definuje priestupky proti poriadku v správe a priestupky proti verejnému poriadku. Ostatné priestupky a iné správne delikty nie sú kodifikované a sú obsiahnuté v osobitných právnych predpisoch upravujúcich jednotlivé vecné oblasti verejnej správy. Druhový objekt nekodifikovaných správnych deliktov je možné odvodiť primárne z úvodných ustanovení vecne príslušných osobitných predpisov.[593] Druhovým objektom je v prípade ZoKB a ZoITV napr. ochrana kybernetickej bezpečnosti a s ňou spojená funkčnosť informačných systémov verejnej správy, či dodržiavanie administratívnych postupov a compliance circle postupov.

[589] *Prášková, H.* Základy odpovědnosti za správní delikty. 1. vydání. Praha : C. H. Beck, 2013, s. 233 - 234.
[590] Bližšie pozri: § 1 PriesZ a *Srebalová, M.* § 1 [Základné ustanovenie]. In: *Srebalová, M. a kol.* Zákon o priestupkoch. 2. vydanie. Bratislava: C. H. Beck, 2020, s. 1–5. alebo *Košičiarová, S.* Zákon o priestupkoch. Podrobný komentár s judikatúrou. Praha : Leges, 2020. s. 78 – 83.
[591] Bližšie pozri: Časť II – osobitná časť PriesZ.
[592] *Vrabko, M. a kol.* Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava : Ch. H. Beck, 2025, s. 210.
[593] *Prášková, H.* Základy odpovědnosti za správní delikty. 1. vydání. Praha : C. H. Beck, 2013, s. 234 - 235.

Individuálny objekt sa spája s konkrétnym priestupkom a so zákonom presne vymedzeným protiprávnym konaním. Individuálny objekt musí mať každá skutková podstata správneho deliktu. Ide o konkrétny jednotlivý záujem proti, ktorému smeruje správny delikt a na, ktorého ochranu je príslušné ustanovenie určené.[594] Individuálny objekt nie je v zákone vyslovene uvedený a je potrebné ho odvodiť z úvodných ustanovení prípadne z dikcie právneho predpisu a z ostatných znakov skutkovej podstaty.[595] Vybrané správne delikty môžu mať aj viacero objektov. Vtedy musia byť deliktuálnym správaním páchateľa zasiahnuté všetky definované objekty skutkovej podstaty administratívneho deliktu.[596] V ZoKB a ZoITVS, je individuálny objekt odvoditeľný kombináciou úvodných ustanovení s časťami regulujúcimi správne delikty a v prípade ZoKB aj priestupky, v spojení s konkrétnymi povinnosťami upravenými naprieč zákona. Identifikácia objektu v týchto predpisoch má prevažne blanketový charakter – príslušné ustanovenie definujúce správny delikt odkazuje na konkrétne povinnosti v jednotlivých ustanoveniach sektorového predpisu, prípadne európskeho aktu.

II. Objektívna stránka zachytáva vonkajší priebeh správneho deliktu, teda to, ako sa deliktuálne konanie prejaví navonok. Práve prostredníctvom nej sa jednotlivé skutkové podstaty správnych deliktov od seba odlišujú najvýraznejšie, pretože vyjadruje konkrétnu podobu protiprávneho správania. V jej jadre stoja tri základné prvky:

1. **konanie,**
2. **následok** a
3. **príčinná súvislosť** medzi nimi.

Až ich spoločné naplnenie umožňuje uzavrieť, že je objektívna stránka deliktu daná.

Prvým prvkom je **konanie,** teda správanie osoby, ktoré sa prejaví vo vonkajšej realite. Môže ísť o aktívny zásah, keď osoba niečo vykoná, alebo naopak o nečinnosť, ak nekoná tam, kde konať mala. V právnej úprave môžeme identifikovať ustanovenia, ktoré vyslovene

[594] *Horvat, M.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 28.
[595] Napríklad v zmysle § 30 ods. 1 písm. b) ZoKB sa priestupku dopustí ten, kto správnemu orgánu poskytne nepravdivé údaje v oznámení o prevádzkovaní základnej služby. Objektom v tomto prípade je celospoločenský záujem na vedení registra PZS, ktorý obsahuje úplné, pravdivé a aktuálne údaje.
[596] *Prášková, H.* Základy odpovědnosti za správní delikty. 1. vydání. Praha : C. H. Beck, 2013, s. 233 - 236.

nevymedzujú konanie, ale odkazuje na porušenie inde stanovených povinností.[597] Čo je typické pre ZoKB a ZoITVS. Spravidla ide o osobitnú, sektorovú právnu úpravu.[598] Druhým prvkom je **následok**, ktorým sa rozumie zásah do právom chráneného záujmu, či už vo forme jeho porušenia, poškodenia alebo aspoň ohrozenia. Tretím prvkom je **kauzálny vzťah**, teda vzťah príčiny a následku. Práve kauzálny nexus predstavuje vyjadrenie myšlienky, že každá akcia má svoju reakciu. Nestačí len existencia konania a škodlivého výsledku; musí byť zároveň zrejmé, že práve konkrétne konanie bolo príčinou daného následku.[599]

Pri niektorých správnych deliktoch zákon viaže vznik zodpovednosti aj na ďalšie okolnosti. Môže ísť napríklad o **miesto**, kde k deliktu došlo, o **čas**, v ktorom bol spáchaný, alebo o osobitný **spôsob vykonania**. Tieto znaky nemusia byť prítomné pri každom delikte, no ak ich zákon výslovne uvádza, stávajú sa súčasťou objektívnej stránky. Objektívna stránka nevyjadruje iba samotné protiprávne správanie, ale aj konkrétne podmienky, za ktorých nadobúda právny význam. Dobrým príkladom je priestupok proti majetku, pri ktorom zákon opisuje objektívnu stránku prostredníctvom konania smerujúceho k spôsobeniu škody na cudzom majetku, prípadne aj pokusu o takéto konanie.[600]

III. Subjekt správneho deliktu predstavuje okruh osôb, voči ktorým možno v konkrétnom prípade vyvodiť administratívnoprávnu zodpovednosť. S pojmom subjekt sa bezprostredne spája aj pojem **páchateľ**. Tieto dva pojmy je však potrebné od seba odlíšiť.[601] Zatiaľ čo pojem subjekt je pojmom teoreticko-právnym, pojem páchateľ je pojmom administratívno-právnym a trestno-právnym. Administratívno-právne normy legálnu definíciu pojmu páchteľ neobsahujú. Správny delikt **nemožno** posudzovať bez väzby na právne relevantný subjekt, keďže zodpovednosť sa vždy spája s konkrétnou osobou, nie s okolnosťou, udalosťou alebo pôsobením vyššej moci. V rámci administratívnoprávnej zodpovednosti pritom môže ísť o **fyzickú osobu** aj **právnickú osobu**, avšak rozhodujúce je vždy to, aký druh správneho deliktu zákon upravuje. Práve konkrétny režim spájajúci sa s konkrétnym druhom správneho deliktu určuje, kto môže byť nositeľom zodpovednosti. Kým pri priestupkoch je subjektom

[597] *Prášková, H.* Základy odpovědnosti za správní delikty. 1. vydání. Praha : C. H. Beck, 2013, s. 233 - 241.
[598] Napríklad pozri: § 78 ods. 1 písm. a) zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov alebo § 30 ods. 1 písm. a) – c) ZoKB.
[599] *Horvat, M.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 28.
[600] *Vrabko, M. a kol.* Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava : Ch. H. Beck, 2025, s. 210.
[601] Bližšie pozri: *Prášková, H.* Základy odpovědnosti za správní delikty. 1. vydání. Praha : C. H. Beck, 2013, s. 265.

zásadne len fyzická osoba, pri iných správnych deliktoch môže zákon viazať zodpovednosť aj na právnické osoby alebo podnikajúce fyzické osoby. Z hľadiska miery konkretizácie možno rozlišovať:

1. **všeobecný,**
2. **špeciálny a**
3. **individuálny subjekt**.[602]

Všeobecný subjekt je vymedzený široko a označuje každú osobu, ktorá spĺňa základné podmienky deliktuálnej spôsobilosti; v zákonnom texte sa preto spravidla vyjadruje všeobecnými pojmami, ako sú *„kto*", *„fyzická osoba*" alebo *„právnická osoba*". Takéto vymedzenie znamená, že zákon nevyžaduje nijakú ďalšiu osobitnú vlastnosť, postavenie alebo právny status nad rámec všeobecnej spôsobilosti niesť administratívnoprávnu zodpovednosť. Všeobecný subjekt je preto typický pre tie skutkové podstaty, pri ktorých zákonodarca sleduje čo najširší okruh potenciálne zodpovedných osôb.

Špeciálny subjekt[603] je už užšie určený. Popri všeobecných podmienkach spôsobilosti sa pri ňom vyžaduje ešte ďalší osobitný znak, ktorý subjekt bližšie konkretizuje. Môže ísť napríklad o:

1. **určité právne postavenie** – PZS, orgán riadenia, člen štatutárneho orgánu;
2. **osobitnú funkciu** – certifikovaný audítor kybernetickej bezpečnosti;
3. **oprávnenie** – vykonávanie samohodnotenia manažérom kybernetickej bezpečnosti;
4. **povolanie** – manažér KB, osoba so sídlom v SR zastupujúca PZS so sídlom mimo EÚ;
5. **služobný pomer** – príslušník NBÚ, alebo
6. **inú vlastnosť**, ktorú zákon považuje za rozhodujúcu pre vznik zodpovednosti – akreditácia, certifikácia, zápis v príslušnom registri.

Ak osoba tento osobitný znak nespĺňa, nemôže byť subjektom konkrétneho správneho deliktu, hoci by inak všeobecnú deliktuálnu spôsobilosť mala. Pri špeciálnom subjekte teda zákon viaže zodpovednosť na užší okruh osôb, ktoré sa nachádzajú v osobitnom právnom alebo faktickom postavení vo vzťahu k chránenému záujmu.

[602] *Horvat, M.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 29.

[603] Napríklad PZS v zmysle ZoKB, alebo kritický subjekt v zmysle zákona č. 367/2024 Z. z. o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov.

Individuálny subjekt predstavuje najvyšší stupeň konkretizácie. Ide o taký subjekt, pri ktorom je zákonná skutková podstata naviazaná na natoľko určité postavenie alebo funkciu, že zodpovednosť môže niesť len presne určená osoba alebo veľmi úzko vymedzený okruh osôb. V tomto prípade už nejde len o všeobecnú alebo osobitnú deliktuálnu spôsobilosť, ale o právne postavenie, ktoré je svojou povahou jedinečné alebo nezameniteľné. Individuálny subjekt sa preto vyskytuje najmä tam, kde je porušenie povinnosti späté s výkonom konkrétnej verejnej funkcie, zákonom určenej právomoci alebo osobitného druhu zodpovednosti, ktorú nemožno preniesť na neurčitý okruh osôb – štatutárny orgán.[604]

IV. Subjektívna stránka správneho deliktu predstavuje vnútornú zložku deliktuálnej zodpovednosti. Vyjadruje psychický vzťah páchateľa k vlastnému konaniu a k následku, ktorý jeho konanie vyvolalo alebo mohlo vyvolať. V právnej rovine sa táto zložka spravidla stotožňuje so **zavinením**. Nejde teda o to, ako sa delikt prejavil navonok, ale o to, ako sa páchateľ k svojmu konaniu staval z hľadiska vedomia a vôle. Práve z tohto dôvodu má subjektívna stránka význam len tam, kde právna úprava viaže vznik zodpovednosti na subjektívny princíp.

Zavinenie sa tradične vysvetľuje prostredníctvom dvoch zložiek:

1. **Vedomostná zložka** – zahŕňa vedomie rozhodujúcich okolností a predstavu páchateľa o možnom následku jeho konania.
2. **Vôľová zložka** – vyjadruje vzťah páchateľa k tomuto následku, teda či ho chcel vyvolať, prípadne či bol aspoň uzrozumený s tým, že následok môže nastať.

Na základe kombinácie týchto dvoch zložiek sa rozlišujú základné formy zavinenia, a to **úmysel** a **nedbanlivosť**. **Úmysel** *(dolus)* môže mať podobu **priameho** *(dolus directus)* **alebo nepriameho** *(dolus indirectus)* úmyslu; **nedbanlivosť** *(culpa)* sa rozlišuje na **vedomú** *(culpa lata)* **a nevedomú** *(culpa levis)*.[605] Toto členenie má význam najmä pri posúdení intenzity zavinenia a následne aj pri individualizácii sankcie.

Ak právna úprava neustanovuje niečo osobitné, na vznik zodpovednosti spravidla postačuje už **nedbanlivostná forma zavinenia**. Ak však zákon výslovne vyžaduje úmyselné

[604] Napríklad štatutárny orgán v zmysle ZoKB alebo oprávnená osoba kritického subjektu v zmysle zákona č. 367/2024 Z. z. o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov.
[605] *Vrabko, M. a kol.* Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava : Ch. H. Beck, 2025, s. 208.

konanie, zodpovednosť nemožno vyvodiť len na základe nedbanlivosti. Naopak, ak skutková podstata vyžaduje len nedbanlivosť, nevylučuje to, aby bol delikt spáchaný úmyselne; takáto okolnosť sa následne prejaví najmä pri výmere sankcie, keďže **úmysel predstavuje závažnejšiu formu zavinenia.** V niektorých prípadoch môže zákon pracovať aj s ďalšími vnútornými znakmi, najmä s **pohnútkou, cieľom alebo účelom**. Tie však spravidla nevystupujú ako pravidelný znak skutkovej podstaty, ale len vo výnimočných prípadoch, ak ich zákon výslovne vyžaduje.[606] Na rozdiel od trestného práva vo všeobecnosti nie je pri správnych deliktoch možné hovoriť o tom, že niektoré znaky subjektívnej stránky sú obligatórne a iné fakultatívne. Toto určenie je možné realizovať výlučne pri jednotlivých druhoch správnych deliktov.[607] Výrazne sa to prejavuje najmä pri správnych deliktoch v zmysle ZoKB alebo ZoITVS.

Pre potreby správneho trestania je rozhodujúce rozlíšenie medzi deliktmi založenými na **subjektívnej zodpovednosti – zodpovednosti za zavinené protiprávne konanie** a deliktmi založenými na **objektívnej zodpovednosti – zodpovednosti za výsledok**.[608] **Priestupky** sú bez výnimky konštruované na subjektívnom princípe, čo znamená, že správny orgán pri nich musí skúmať a preukazovať zavinenie. Bez zistenia subjektívnej stránky nemožno uzavrieť, že skutková podstata priestupku bola naplnená. Naproti tomu **správne delikty právnických osôb a fyzických osôb – podnikateľov** sú typicky budované na princípe **objektívnej zodpovednosti**. V týchto prípadoch sa zavinenie neskúma; rozhodujúce je, či došlo k naplneniu zákonných znakov deliktu a k vzniku protiprávneho stavu (napr. porušenie povinnosti spočívajúce v neuzatvorení zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností) alebo následku (zvýšený rozsah škôd spôsobený nenahlásením závažného kybernetického bezpečnostného incidentu bezodkladne). Pre správny orgán má toto rozlíšenie zásadný význam, pretože určuje samotný rozsah dokazovania. Kým pri priestupkoch je potrebné dokazovanie rozšíriť aj o vnútorný vzťah páchateľa ku skutku, pri objektívne koncipovaných deliktoch sa posudzovanie sústreďuje na naplnenie ostatných znakov skutkovej podstaty. V tom spočíva aj praktický

[606] *Horvat, M.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 32 – 33.
[607] *Prášková, H.* Základy odpovědnosti za správní delikty. 1. vydání. Praha : C. H. Beck, 2013, s. 297.
[608] *Vrabko, M. a kol.* Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava : Ch. H. Beck, 2025, s. 199.

význam subjektívnej stránky pre rozhodovaciu činnosť orgánov verejnej správy.[609] Táto skutočnosť opodstatňuje veľké rozpätie možnosti uloženia pokuty v zmysle ZoKB, ktoré je v niektorých prípadoch naviazané na obrat povinnej osoby.

9.4 Princípy správneho trestania

V právnej teórii možno nájsť prístupy, ktoré sa usilujú rozlišovať medzi pojmami **princíp, zásada a pravidlo**; na túto potrebu upozorňovali aj niektorí autori.[610] Pre účely tejto učebnice však nebudeme stavať na tomto terminologickom rozlíšení. V ďalšom výklade budeme vychádzať z toho, že spoločným menovateľom princípov aj zásad je ich funkcia vedúcej idey a interpretačného východiska, ktoré usmerňuje chápanie aj aplikáciu práva, a to tak v hmotnoprávnej, ako aj v procesnoprávnej rovine. Z hľadiska nášho výkladu nie je rozhodujúce, či konkrétnu kategóriu označíme ako princíp, zásadu alebo pravidlo, ale aký význam má pre systematiku administratívnoprávnej zodpovednosti a správneho práva trestného. Z tohto dôvodu budeme v ďalšom texte používať pojmy, ktoré sa v teórii vzťahujú na jednotlivý princíp resp. zásadu.

9.4.1 Základné zásady správneho konania

Nakoľko je správne trestanie subsystém v rámci správneho konania je samo o sebe ovplyvnené základnými zásadami správneho konania, ktoré sú vo všeobecnosti vyjadrené v Správnom poriadku, ktorý explicitne ustanovuje týchto osem zásad:

1. **Zásada zákonnosti** – označovaná aj ako **princíp legality** v našom kontexte znamená, že administratívnoprávnu zodpovednosť **možno vyvodzovať len na základe zákona a v jeho medziach, a to v hmotnoprávnej aj procesnoprávnej rovine**. Jej ústavný základ vyplýva z čl. 2 ods. 2 a 3 Ústavy SR, v zmysle, ktorého správny orgán môže konať len v rozsahu zákonom zverenej právomoci a pri ochrane len takého záujmu, ktorý zákon výslovne uznáva. V správnom trestaní to znamená, že zodpovednosť možno vyvodiť iba za zákonom vymedzený delikt, voči zákonom určenému subjektu a pri preukázaní zákonných znakov skutkovej podstaty. Z hľadiska administratívnoprávnej zodpovednosti v kontexte

[609] *Horvat, M.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 34.
[610] Bližšie pozri: *Vrabko, M. a kol.* Správne právo procesné. Všeobecná časť. 1. vydanie. Bratislava : C. H. Beck, 2013, s. 61 – 62.

kybernetickej bezpečnosti sa prejavuje prostredníctvom konkrétnych ustanovení upravujúcich priestupky či iné správne delikty a procesné inštitúty ich aplikácie. Napr. ZoKB v ustanovení upravujúcom priestupky okrem jednotlivých priestupkov odkazuje na aplikáciu zákona o priestupkoch. Hmotnoprávnu rovinu aplikácie zásady zákonnosti predstavuje ustanovenie, ktoré upravuje konkrétne priestupky a sankcie za priestupky a procesnoprávnu rovinu upravuje ustanovenie odkazujúce na správny poriadok a určujúce príslušnosť NBÚ.

2. **Zásada aktívnej súčinnosti** – vyjadruje požiadavku **vzájomnej spolupráce medzi správnym orgánom a ostatnými subjektmi konania** pri dosahovaní jeho cieľa. Jej podstata spočíva v tom, že správny orgán má vytvárať podmienky na riadne uplatnenie procesných práv účastníkov, najmä ich poučiť o ich procesných oprávneniach a povinnostiach tak, aby pre neznalosť procesných pravidiel neutrpeli na svojich hmotnoprávnych právach. V konaniach týkajúcich sa vyvodzovania administratívnoprávnej zodpovednosti **musí mať obvinený zabezpečené také procesné postavenie, ktoré mu umožní účinne vykonávať obhajobu**; zároveň však aj **ostatné subjekty** konania musia správnemu orgánu poskytovať **potrebnú a včasnú súčinnosť**, aby bolo možné vydať zákonné rozhodnutie. Aplikácia tejto zásady a jej dodržiavanie vynucované hrozbou sankcie je osobitne prítomné v ZoKB, kde zákon určuje rad povinností pre spravované subjekty (napr. PZS či správca TLD), ktorých nesplnenie je považované za deliktuálne správanie postihnuteľné sankciou. Spravované subjekty sú tak motivované poskytovať správnemu orgánu aktívnu súčinnosť nakoľko za jej neposkytnutie im hrozí sankcia.
3. **Zásada rýchlosti a hospodárnosti** – vyjadruje požiadavku, aby správny orgán konal bez zbytočných prieťahov, v primeranom čase a s použitím takých prostriedkov, ktoré vedú k zákonnému rozhodnutiu bez nadmerného zaťažovania účastníkov. **Rýchlosť** sa v správnom konaní prejavuje najmä prostredníctvom lehôt, v ktorých má správny orgán vykonávať procesné úkony a rozhodnúť vo veci; ich neodôvodnené prekročenie môže viesť k stavu nečinnosti, proti ktorému sa účastník môže brániť aj právnymi prostriedkami ochrany. V ZoKB sa zásada rýchlosti prejavuje napr. vo forme určenia trojdňovej poriadkovej lehoty na rozhodnutie riaditeľa NBÚ o zaujatosti zamestnanca NBÚ alebo rozhodnutie NBÚ o akreditácii jednotky CSIRT do 90 dní ale aj povinnosťou NBÚ bezodkladne oznámiť PZS zapísanie do registra PZS. **Hospodárnosť** zároveň znamená, že

správny orgán má šetriť nielen čas, ale aj náklady spojené s konaním a preto nesmie ukladať zbytočné úkony ani zaťažovať účastníkov viac, než je potrebné na riadne zistenie skutkového stavu. Zásada rýchlosti a hospodárnosti zaväzuje aj spravované subjekty, ktorým ZoKB ukladá aby vybrané povinnosti splnili v stanovenom čase určenom časovým úsekom (dni, mesiace, roky) alebo bezodkladne.

4. **Zásada materiálnej pravdy** – vyjadruje povinnosť správneho orgánu rozhodovať **na základe presne, úplne a spoľahlivo zisteného skutkového stavu veci**. Správny orgán preto musí z úradnej povinnosti zistiť všetky právne významné okolnosti, a to bez ohľadu na to, či svedčia v prospech alebo neprospech účastníka konania. V konaniach týkajúcich sa vyvodzovania administratívnoprávnej zodpovednosti má táto zásada **osobitný význam, pretože sa v nich rozhoduje o vine a treste za administratívny delikt.** Jej obsah je úzko spojený s dokazovaním a s obstarávaním podkladov na rozhodnutie. Len spoľahlivo zistený skutkový stav vytvára predpoklad pre zákonné a spravodlivé rozhodnutie.
5. **Zásada materiálnej rovnosti** – vychádza z **ústavného princípu rovnosti pred zákonom** a vyžaduje, aby správny orgán posudzoval **rovnaké alebo porovnateľné prípady rovnako**, pokiaľ sa nezmenili rozhodné okolnosti. V jej obsahu sa prirodzene prejavuje aj **princíp legitímneho očakávania**, teda požiadavka, aby účastník mohol pri splnení zákonných podmienok očakávať rozhodnutie zodpovedajúce ustálenej rozhodovacej praxi v obdobných veciach. Osobitný význam má táto zásada tam, kde zákon priznáva správnemu orgánu **diskrečnú právomoc** (pripustenie správnej úvahy), v našom prípade najmä pri ukladaní sankcie za správny delikt v rámci zákonného rozpätia. Práve v správnom trestaní preto pôsobí ako korektív proti svojvôli, klientelizmu a neodôvodneným rozdielom v rozhodovaní.
6. **Zásada informovanosti verejnosti** – vychádza z **princípov dobrej správy**, jej uplatnenie v oblasti administratívnoprávnej zodpovednosti je však skôr **obmedzené**. V konaniach o správnych deliktoch totiž spravidla **prevažuje ochrana procesných práv účastníka** nad požiadavkou verejnej informovanosti o priebehu konania. Aj v kontexte **zásady ústnosti trestného konania**, ktorým je aj správne trestanie, Správny poriadok vo všeobecnosti upravuje, že **ústne pojednávanie je neverejné** pokiaľ zákon neustanoví inak. Táto zásada sa preto v správnom trestaní prejavuje napr. tam, kde osobitná právna úprava pripúšťa

alebo vyžaduje **zverejnenie výsledku konania,** najmä informácie o uloženej sankcii.[611] V takom prípade nejde o všeobecnú verejnosť konania, ale o **osobitný zákonný prostriedok,** ktorým sa zabezpečuje informovanie verejnosti o výsledku rozhodovacej činnosti správneho orgánu.[612]

7. **Zásada spolupráce** – vyjadruje požiadavku, aby **správny orgán** aj **ostatné subjekty konania** svojím postupom **prispievali k zákonnému a riadnemu vybaveniu veci**. Správny orgán má vytvárať priestor na uplatnenie procesných práv, účastníci a ďalšie osoby majú poskytovať potrebnú súčinnosť. V správnom trestaní táto zásada **napomáha objasneniu skutku** a vydaniu preskúmateľného rozhodnutia.
8. **Zásada procesnej rovnosti** – vyjadruje požiadavku, aby správny orgán zabezpečil všetkým subjektom konania **rovnaké procesné možnosti pri uplatňovaní ich práv a právom chránených záujmov**. Prejavuje sa najmä v povinnosti správneho orgánu poskytovať **poučenie,** vytvoriť **priestor na vyjadrenie** sa k podkladom rozhodnutia a postupovať tak, aby žiadny z účastníkov **nebol procesne znevýhodnený**. V konaniach o administratívnoprávnej zodpovednosti prispieva k **spravodlivému procesnému postaveniu obvineného** aj **ostatných dotknutých subjektov**.

Okrem vyššie spomenutých všeobecných zásad explicitne ustanovených Správnym poriadkom, je zo všeobecného predpisu o správnom konaní odvoditeľná aj:

1. **Zásada dvojinštančnosti konania** – vyjadruje, že proti prvostupňovému rozhodnutiu má účastník spravidla právo podať **riadny opravný prostriedok,** o ktorom rozhoduje nadriadený orgán. Správny poriadok tým vytvára vnútorný **kontrolný mechanizmus na zabezpečenie zákonnosti a vecnej správnosti rozhodnutia**. Význam tejto zásady spočíva aj v umožnení preskúmať výrok rozhodnutia ešte v rámci mechanizmov vo verejnej správe, skôr než sa vec dostane pred súd. Z hľadiska účinkov riadnych opravných prostriedkov, osobitne **odvolania** sa pri tejto zásade prejavuje tzv. **devolutívny účinok**[613]. Vo veciach,

[611] *Martvoň, A.* Vplyv európskeho práva na slobodný prístup k informáciám a na zásadu informovanosti v konexte správneho trestania. In. *Lenhart, M., Hapčová, I., Hamuľák, J. (ed).* 2016. Vplyv európskeho práva na kreovanie princípov a zásad správneho trestania: Zborník príspevkov z medzinárodnej vedeckej konferencie Bratislavské právnické fórum 2016 organizovanej Univerzitou Komenského v Bratislave, Právnickou fakultou v dňoch 21. – 22. októbra 2016. Bratislava : Univerzita komenského v Bratislave, právnická fakulta, vydavateľské oddelenie, s. 133 – 134.

[612] Napríklad Čl. 54 Nariadenia DORA upravuje uverejnenie rozhodnutí o uložení administratívnych sankcií na oficiálnych webových sídlach príslušných orgánov.

[613] Bližšie pozri: *Vrabko, M. a kol.* Správne právo procesné. Všeobecná časť. 1. vydanie. Bratislava : C. H. Beck, 2013, s. 177.

kde na prvom stupni rozhoduje ústredný orgán štátnej správy je dvojinštančnosť suplovaná tzv. konaním o **rozklade**. Na druhom stupni v rámci rozkladu rozhodne v vedúci ústredného orgánu štátnej správy na návrh **rozkladovej komisie**. Jej rozhodnutím však nie je viazaný. V ZoKB a ZoITVS je práve konanie o rozklade alternatívou k odvolaciemu konaniu, keďže na prvom stupni rozhoduje buď NBÚ, ako ostatný ústredný orgán štátnej správy alebo MIRRI SR, ako ministerstvo. Prakticky to znamená, že na prvom stupni rozhoduje úrad alebo ministerstvo prostredníctvom príslušnej organizačnej zložky, na základe splnomocnenia riaditeľom, resp. ministrom a na druhom stupni rozhoduje sám riaditeľ resp. minister na základe odporúčania rozkladovej komisie, ktorú si sám kreuje.

2. **Dispozičná zásada a zásada oficiality** – tieto dve zásady sa navzájom dopĺňajú. **Dispozičný prvok** sa prejavuje tam, kde sa konanie začína **na návrh účastníka**, kým **oficialita** tam, kde sa začína **na podnet správneho orgánu**. V správnom trestaní spravidla prevažuje oficialita, pretože správny orgán sleduje porušenie zákona z úradnej povinnosti; dispozičný prvok sa uplatní len výnimočne, najmä pri návrhových deliktoch, ak to ustanovuje osobitná úprava. V ZoKB ale aj v ZoITVS je administratívnoprávna zodpovednosť vyvodzovaná výlučne na základe zásady oficiality a realizuje sa ako dôsledok dohľadu, alebo kontroly vykonávanej príslušným správnom orgánom.
3. **Zásada verejnosti a neverejnosti konania** – správne konanie **nie je všeobecne verejným procesom v súdnom zmysle**. V správnom konaní neexituje inštitút vylúčenia verejnosti tak ako ho napr. upravuje Správny súdny poriadok, keďže súdne konanie je zo zásady verejné. Správny poriadok výslovne ustanovuje, že **ústne pojednávanie je neverejné**, ak osobitný zákon alebo správny orgán neurčí inak. V správnom trestaní sa verejnosť pripúšťa skôr **výnimočne**. Na to, aby mohlo byť správne konanie verejné musí jeho verejnosť pripustiť zákon.
4. **Zásada písomnosti a zásada ústnosti** – vyjadrujú dve základné formy procesného postupu. Pre správne konanie je typická najmä písomnosť, keďže rozhodnutie sa spravidla oznamuje doručením jeho písomného vyhotovenia. Zároveň však Správny poriadok pozná aj ústnosť, najmä prostredníctvom ústneho pojednávania, ktoré správny orgán nariadi, ak to vyžaduje povaha veci alebo osobitný zákon. V správnom trestaní má ústnosť význam najmä pri objasnení skutku a zabezpečení práva na obhajobu a bližšie sa jej budeme venovať v rámci princípov správneho trestania.

9.4.2 Princípy (zásady) správneho trestania

Princípy správneho trestania predstavujú základné interpretačné a aplikačné východiská pre vyvodzovanie administratívnoprávnej zodpovednosti. Určujú limity postupu správneho orgánu pri rozhodovaní o vine a sankcii a zároveň chránia subjekt, voči ktorému sa správne trestanie vedie. Ich význam spočíva v tom, že usmerňujú výklad právnych noriem správneho práva a správneho práva trestného a zabezpečujú, aby výkon sankčnej právomoci verejnej správy zostal v medziach zákonnosti, predvídateľnosti a spravodlivosti.

Obsah týchto princípov sa formuje nielen vo vnútroštátnom práve, ale aj v európskom právnom priestore. Keďže právna úprava administratívnoprávnej zodpovednosti nie je v jednotlivých štátoch jednotná, princípy správneho trestania plnia aj harmonizačnú funkciu. Vytvárajú spoločný hodnotový rámec, ktorý napomáha zbližovaniu požiadaviek na výkon sankčnej právomoci. Ich základným východiskom je najmä **právo na spravodlivý proces vyplývajúce z Dohovoru**, z ktorého sa odvodzujú požiadavky na zákonnosť postupu, ochranu procesných práv, preskúmateľnosť rozhodnutia a zákaz svojvôle.

Na vnútroštátnej úrovni vyplývajú princípy správneho trestania najmä z **Ústavy SR**, **Priestupkového zákona**, **Správneho poriadku**, **Trestného zákona**, **Trestného poriadku**, **zákona o trestnej zodpovednosti právnických osôb** a z osobitných právnych predpisov upravujúcich jednotlivé správne delikty.[614] Tieto právne pramene vytvárajú normatívny základ, z ktorého možno odvodiť jednotlivé princípy správneho trestania a ich obsah pri aplikácii práva. Podľa Hamuľákovej[615] možno k princípom a zásadám správneho trestania zaradiť najmä:

1. Princíp zákonnosti (*Nullum crimen sine lege*),
2. princíp subsidiarity sankčného postihu,
3. princíp proporcionality,
4. princíp legality postihu (zásada oportunity),
5. princíp *ne bis in idem,*
6. princíp riadneho zákonného procesu,
7. princíp prezumpcie neviny,
8. princíp, že dôkazné bremeno v konaní spočíva na správnom orgáne,

[614] *Prášková, H.* Základy odpovědnosti za správní delikty. 1. vydání. Praha : C. H. Beck, 2013, s. 21 – 23.
[615] *Hamuľáková, Z.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 55.

9. princíp zákazu donucovania k sebaobviňovnaiu,
10. princíp *in dubio pro reo,*
11. princíp konania o správnom delikte v primeranej lehote,
12. princíp prihliadnutia na už uloženú sankciu,
13. absorpčná zásada,
14. princíp ukončenia správneho konania o delikte rozhodnutím,
15. princíp zákazu zneužitia správnej úvahy a právo na odôvodnenie rozhodnutia o uloženej sankcii,
16. zásada legitímneho očakávania,
17. princíp zákazu *reformatio in peius,*
18. princíp preskúmateľnosti rozhodnutia ktorým sa ukladá sankcia.

Na prvý pohľad sa môže zdať, že niektoré z princípov sa opakujú no nie je tomu tak. Každý z nich má svoje osobitné miesto a vyjadrenie v systéme správneho trestania. Už len z ich označenia je zrejmé, že ich nemožno vnímať izolovanie ako samostatný súbor pravidiel. Princípy správneho trestania tvoria vnútorne prepojený systém, ktorý nadväzuje na základné zásady správneho konania. Sú však konkrétnejšie v kontexte podmienok správneho trestania. Ich konkretizácia súvisí najmä s fenoménom rozhodovania o vine a treste za administratívny delikt – majú trestnoprávny charakter. Kým základné zásady správneho konania vytvárajú základný rámec rozhodovania verejnej správy, princípy správneho trestania tento rámec dopĺňajú o osobitné požiadavky vyplývajúce z represívneho charakteru trestania a z potreby ochrany základných práv subjektu, voči ktorému sa vedie konanie. Súčasne pri ich aplikácii v správnom konaní musia byť princípy správneho trestania rešpektované aj v legislatívnom procese a zákonodarca ich musí rešpektovať už pri tvorbe práva.[616]

Na všeobecný rámec zásad správneho konania nadväzujú jednotlivé princípy správneho trestania, ktoré sa v aplikačnej praxi navzájom dopĺňajú a často sa aj obsahovo prelínajú. Ich význam však nespočíva len v abstraktnom vymedzení, ale najmä v tom, že vytvárajú konkrétne limity postupu správneho orgánu pri zisťovaní okolností týkajúcich sa skutku, rozhodovaní o vine a pri ukladaní sankcie. Z tohto dôvodu je potrebné každý z nich vykladať osobitne, no vždy vo vzájomných súvislostiach a v prepojení na všeobecné zásady

[616] *Prášková, H.* Základy odpovědnosti za správní delikty. 1. vydání. Praha : C. H. Beck, 2013, s. 26.

správneho konania. Práve takýto prístup umožňuje pochopiť ich skutočný význam pre zákonné, spravodlivé a predvídateľné vyvodzovanie administratívnoprávnej zodpovednosti.

1. **Princíp zákonnosti *(Nullum crimen sine lege)*** – ako pri tejto zásade vyplýva z latinského prekladu *„Žiadny zločin bez zákona*" môžeme v kontexte administratívnoprávnej zodpovednosti upresniť, že ak má byť nejaké neželené **správanie osoby postihované** prostriedkami správneho trestania musí byť toto správanie ako neželané **vyslovene označené v zákone**. Z toho vyplýva, že zákon musí určiť nielen skutkové podstaty správnych deliktov, ale aj podmienky zodpovednosti a druhy sankcií *(nullum crimen sine lege scripta)*. Zároveň musí byť zákonná úprava dostatočne určitá, jasná a predvídateľná, aby bolo zrejmé, aké konanie je postihnuteľné a aký postih zaň prichádza do úvahy *(nullum crimen sine lege certa).* Súčasťou tohto princípu je aj zákaz retroaktivity prísnejšej úpravy a zákaz analógie v neprospech delikventa.[617] V ZoKB a ZoITVS je označenie neželaného správania realizované prevažne cez blanketové normy, ktoré odkazujú na konkrétne povinnosti naprieč príslušným právnym predpisom. ZoKB okrem iného odkazuje aj na Akt o kybernetickej bezpečnosti.
2. **Princíp subsidiarity sankčného postihu** – vyjadruje, že správna sankcia má byť použitá až vtedy, keď miernejšie právne alebo administratívne prostriedky nepostačujú na dosiahnutie účelu verejnoprávnej ochrany. Ide o prejav chápania sankcie ako **ultima ratio**, teda krajného prostriedku zásahu do práv jednotlivca.[618] Tento princíp úzko súvisí s proporcionalitou, pretože vyžaduje, aby správny orgán reagoval len tak intenzívne, ako to odôvodňuje závažnosť a spoločenská škodlivosť konkrétneho konania. Ak je delikt bagateľný alebo ak k náprave postačuje miernejší postup, správny orgán môže uprednostniť riešenie bez represívneho postihu, napríklad upustiť od uloženia sankcie[619] alebo vec vybaviť miernejšou formou. Možnosť upustiť od sankcie pripúšťa aj ZoKB aj ZoITVS. Tento princíp sa veľmi často využíva najmä v implementačnej fáze nového predpisu. Práve v čase implementácie novej sektorovej úpravy môže dochádzať k porušeniam zákona a povinností, ktoré sú postavené na výkladovej nejednotnosti alebo nedostatočnej praktickej skúsenosti

[617] *Prášková, H.* Základy odpovědnosti za správní delikty. 1. vydání. Praha : C. H. Beck, 2013, s. 31 – 40.
[618] *Košičiarová, S.* Zákon o priestupkoch. Podrobný komentár s judikatúrou. Praha : Leges, 2020, s. 34.
[619] *Hamuľáková, Z.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 58.

s aplikáciou právneho predpisu. Vtedy má správny orgán prirodzenú povinnosť ale aj záujem vplývať na spravovaný subjekt edukatívne aby po implementačnej fáze mohol uplatňovať reálne postihy s vedomým, že regulované subjekty si právnu úpravu osvojili a vedia ju aplikovať na úrovni požadovanej správnym orgánom.

3. **Princíp proporcionality** – patrí k základným limitom správneho trestania a bráni tomu, aby správny orgán ukladal sankciu v rozsahu, ktorý nezodpovedá povahe a závažnosti deliktu. Jeho podstata spočíva v požiadavke, aby zásah do práv delikventa neprekročil mieru nevyhnutnú na dosiahnutie represívneho a preventívneho účelu sankcie. V praxi sa tento princíp prejavuje najmä pri individualizácii sankcie, pri zákaze likvidačných sankcií a pri zohľadnení okolností konkrétneho prípadu vrátane pomerov delikventa. Mimoriadne výrazne sa uplatňuje aj pri ZoKB, kde široké sankčné rozpätia kladú na správny orgán vysoké nároky na primerané, racionálne a preskúmateľné určenie výšky sankcie.
4. **Princíp legality postihu** – vyjadruje, že správny orgán je spravidla povinný zaoberať sa každým správnym deliktom, o ktorom sa dozvie, ak zákon neustanovuje inak. Jeho korektívom je **zásada oportunity**, pri ktorej zákon pripúšťa, aby správny orgán zohľadnil okolnosti prípadu a posúdil, či je potrebné delikt prejednať a sankcionovať. Tento priestor sa uplatňuje najmä pri návrhových deliktoch, pri použití správnej úvahy alebo tam, kde je spoločenská škodlivosť činu nepatrná.[620] Ani vtedy však správny orgán nekoná voľne; jeho postup je limitovaný zákonným účelom správneho trestania, najmä ochranou zákonnosti, verejného poriadku a riadneho občianskeho spolužitia. V kontexte všeobecnej zásady procesnej rovnosti je správny orgán zaviazaný aj dovtedajšou praxou. Ak už v skutkovo podobnom prípade raz udelil sankciu je legitímne očakávať (pozri zásada legitímneho očakávania), že tak bude konať aj v ďalšom obdobnom prípade.
5. **Princíp *ne bis in idem* –** z latinského „**Nie dva – krát v tej istej veci**", je princíp, ktorý vyjadruje limit pre ukladanie sankcii. V jeho zmysle, ak bola sankcia za jeden skutok uložená, uloženie ďalšej sankcie za ten istý skutok nie je prípustné.[621] V **hmotnoprávnej rovine** znamená zákaz opätovného uloženia sankcie za skutok, o

[620] *Hamuľáková, Z.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 54.
[621] *Vrabko, M. a kol.* Správne právo procesné. Všeobecná časť. 1. vydanie. Bratislava : C. H. Beck, 2013, s. 44.

ktorom už bolo právoplatne rozhodnuté; **v procesnoprávnej rovine** bráni tomu, aby sa pre ten istý skutok znovu viedlo ďalšie sankčné konanie. Jeho význam spočíva nielen v ochrane pred duplicitným trestaním, ale aj v ochrane pred opakovaným zásahom do právnej sféry osoby, ktorá už bola postihnutá alebo ktorej vec už bola právoplatne uzavretá.[622] Ak si raz páchateľ odpykal trest za svoj delikt nie je možné ho prostredníctvom štátnej autority za ten istý skutok postihovať opätovne. V správnom trestaní tak tento princíp posilňuje právnu istotu, hospodárnosť konania a stabilitu právoplatného rozhodnutia. **Výnimka** z tohto princípu je prítomná napríklad v Priestupkovom zákone, v kontexte určovania druhu sankcie a výmery za priestupok, kedy musí správny orgán prihliadať na to či a akým spôsobom bol páchateľ za ten istý skutok postihnutý v kárnom alebo disciplinárnom konaní. Ak správny orgán príjme záver, že potrestanie v predchádzajúcom konaní bolo postačujúce môže rozhodnúť, že vec odloží alebo konanie zastaví. Urobí tak v závislosti od toho či bolo v kárnom alebo disciplinárnom konaní rozhodnuté pred alebo počas konania o priestupku. [623] Dikcia Priestupkového zákona však nevylučuje možnosť uložiť sankciu aj v priestupkovom konaní. Zákonný imperatív ukladá povinnosť *prihliadnuť* tzn., že správny orgán môže uložiť sankciu aj napriek tomu, že páchateľovi bola uložená sankcia v disciplinárnom alebo kárnom konaní. V rámci svojej diskrečnej právomoci v konexte *ne bis in idem* sa však touto skutočnosťou musí zaoberať.

6. **Princíp riadneho zákonného procesu** - konanie o administratívnom delikte možno viesť len zo zákonných dôvodov, zákonom ustanoveným spôsobom a pred zákonom určeným orgánom. Je procesnoprávnym vyjadrením zásady zákonnosti a *nullum crimen sine lege*.[624] Jeho zmyslom je vylúčiť svojvôľu pri správnom trestaní a zaručiť, že do práv osoby nebude zasahované viac, než je nevyhnutné. Táto zásada preto na jednej strane presne určuje kompetencie a postup správneho orgánu, na druhej strane zaručuje procesné postavenie obvineného.[625] V rámci princípu riadneho zákonného procesu patrí obvinenému najmä právo byť **oboznámený so svojím obvinením**, právo na **prípravu obhajoby**, právo na **obhajobu**, právo, aby **orgán dokázal vinu**

[622] *Prášková, H.* Základy odpovědnosti za správní delikty. 1. vydání. Praha : C. H. Beck, 2013, s. 56.
[623] Bližšie pozri: § 12 ods. 1 v spojení s § 66 ods. 2 písm. d) a § 76 ods. 1 písm. ch) PriesZ
[624] *Hamuľáková, Z.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 64.
[625] *Prášková, H.* Základy odpovědnosti za správní delikty. 1. vydání. Praha : C. H. Beck, 2013, s. 53.

obvinenému, právo, aby bol obvinený **vypočutý**, právo, aby sa konanie o delikte ukončilo **rozhodnutím**, právo, aby rozhodnutie bolo **zverejnené a zdôvodnené**, právo, aby bol obvinený **poučený** o opravnom prostriedku a právo na **preskúmanie rozhodnutia** nezávislým orgánom, a to tak v rámci dvojinštančnosti správneho konania, ako aj v následnom súdnom preskúmaní.[626]

7. **Princíp prezumpcie neviny** – vyjadruje, že osoba je až do právoplatného rozhodnutia vo veci správneho deliktu považovaná za nevinnú. Z tohto hľadiska sa v konaní postupne mení aj jej procesné postavenie. Zatiaľ čo vo fáze oboznamovania sa so skutkom a ustaľovaním skutkových okolností, vrátane osoby prestupcu administratívnej normy, môže byť v pozícii **podozrivého** neskôr, keď si správny orgán ustáli skutok a osobu, ktorá skutok spáchala sa podozrivý dostáva do procesného postavenia **obvineného** zo spáchania priestupku a po právoplatnom rozhodnutí sa stáva **páchateľom** správneho deliktu. Procesné postavenie má veľký význam na rozsah práv, ktorými disponuje v konaní.
8. **Princíp, že dôkazné bremeno v konaní spočíva na správnom orgáne** – ide o bezprostredný **dôsledok prezumpcie neviny**. Znamená, že obvinený nie je povinný preukazovať svoju nevinu ani aktívne vyvracať tvrdenia správneho orgánu; povinnosť preukázať skutok, jeho páchateľa aj splnenie zákonných znakov správneho deliktu nesie správny orgán. Tento **princíp úzko súvisí aj so všeobecnou zásadou materiálnej pravdy**, pretože správny orgán musí rozhodovať na základe úplne, presne a spoľahlivo zisteného skutkového stavu.[627] V správnom trestaní teda nestačí len podozrenie alebo oznámenie o delikte; správny orgán musí zákonnými dôkaznými prostriedkami preukázať vinu konkrétnej osoby.
9. **Princíp zákazu donucovania k sebaobviňovnaiu** – je vyjadrený oprávneným obvineného ale aj svedka odoprieť výpoveď ak by výpoveďou mohol spôsobiť negatívne následky sebe alebo svojím blízkym osobám. Vo vzťahu k obvinenému znamená, že správny orgán musí rešpektovať, že sa ku skutkom ktoré sú mu kladené za vinu nevyjadrí. Tento princíp podčiarkuje povinnosť správneho orgánu uniesť dôkazné bremeno. V širšom zmysle predstavuje tento princíp aj významnú **procesnú**

[626] *Košičiarová, S.* Zákon o priestupkoch. Podrobný komentár s judikatúrou. Praha : Leges, 2020, s. 38.
[627] *Hamuľáková, Z.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 69.

brzdu vo vzťahu k postupu správneho orgánu pri vedení samotného konania. Keďže správny orgán disponuje právomocami založenými na verejnej moci, nachádza sa voči obvinenej osobe v prirodzene nadradenom postavení. Práve preto musí byť výkon týchto oprávnení limitovaný zákonnými požiadavkami na férový proces. To sa prejavuje aj pri vedení výsluchu, pri ktorom správny orgán nesmie klásť **kapciózne otázky**, teda otázky vychádzajúce zo skutočnosti, ktorá ešte nebola vypočúvanou osobou potvrdená, ani **sugestívne otázky**, ktoré už v sebe obsahujú naznačenú alebo priamo vnucovanú odpoveď. Zákaz takýchto otázok chráni vypočúvanú osobu pred manipulatívnym vedením výsluchu a zároveň posilňuje vierohodnosť a použiteľnosť získaných podkladov pre rozhodnutie.

10. **Princíp *in dubio pro reo*** – z latinského ***„V pochybnostiach v prospech obvineného***" posilňuje princíp **prezumpcie neviny** a vytvára priestor pre efektívnu **procesnú obranu** realizovanú obvineným. Je taktiež naviazaný aj na povinnosť správneho orgánu uniesť **dôkazné bremeno** a proti obvinenému vykonať také dôkazy, ktoré budú jednoznačne smerovať k tomu, že administratívny delikt spáchal konkrétny subjekt pri naplnení všetkých znakov skutkovej podstaty deliktu.[628] Tento princíp sa uplatňuje najmä na fázu dokazovania ale jeho prvky je možné identifikovať už v procese rozhodovania správneho orgánu o skutočnostiach vedúcich k obvineniu subjektu. Ak správny orgán nedisponuje dostatkom priamych a procesne spôsobilých dôkazov nemôže konanie skončiť právoplatným rozhodnutím o vine a sankcii za správny delikt. Napr. priestupkové konanie sa v takom prípade zastaví z dôvodu, že spáchanie skutku, o ktorom sa koná, nebolo obvinenému z priestupku preukázané.[629]
11. **Princíp konania o správnom delikte v primeranej lehote** – z hľadiska všeobecných zásad správneho konania ide o princíp, ktorý je previazaný so **zásadou rýchlosti a hospodárnosti**. Je potrebné mať na zreteli, že samotný fakt, že voči osobe je vedené **správne konanie** vo veci správneho trestania **môže mať na osobu negatívny vplyv**. Tento princíp vytvára tlak na správny orgán, ktorý konanie vedie, aby o ňom rozhodol v primeranej lehote. Praktické vyjadrenie tohto princípu spočíva v stanovení poriadkových lehôt.

[628] *Vrabko, M. a kol.* Správne právo procesné. Všeobecná časť. 1. vydanie. Bratislava : C. H. Beck, 2013, s. 45.
[629] Bližšie pozri: § 76 ods. 1 písm. c) PriesZ.

12. **Princíp prihliadania na už uloženú sankciu –** vychádza z princípu *ne bis in idem* a taktiež aj z princípov dobrej verejnej správy. vyjadruje požiadavku, aby správny orgán pri rozhodovaní zohľadnil, že za ten istý skutok už bola páchateľovi uložená sankcia iným orgánom podľa iného právneho predpisu. **Uplatní sa najmä vtedy, ak ten istý čin zakladá zodpovednosť vo viacerých právnych režimoch, ktoré chránia odlišné spoločenské záujmy.** Jeho význam spočíva v tom, že obmedzuje neprimeranú kumuláciu represie a prispieva k spravodlivému a primeranému sankcionovaniu.[630]
13. **Absorbčná zásada –** ovplyvňuje najmä sankciu, ktorá je za správny delikt uložená. V správnom trestaní uplatňuje najmä pri súbehu viacerých správnych deliktov toho istého páchateľa. Jej podstata spočíva v tom, že **pri viacnásobnom deliktuálnom konaní nemá dôjsť k mechanickému sčítaniu sankcií, ale k uloženiu jednej sankcie podľa deliktu, ktorý je najprísnejšie postihnuteľný.** V slovenskej právnej úprave je výslovne vyjadrená najmä v priestupkovom práve[631], pri iných správnych deliktoch sa dlhodobo uplatňuje najmä na základe rozhodovacej činnosti súdov.[632] Jej význam spočíva v tom, že bráni neprimeranej kumulácii represie a posilňuje primeranosť a spravodlivosť sankčného postihu.[633]
14. **Princíp ukončenia konania o delikte rozhodnutím** – aj pri tomto princípe ide o vyjadrenie princípu dobrej verejnej správy. Vyjadruje sa ním požiadavka, aby každé konanie o správnom delikte, ktoré bolo riadne začaté, bolo ukončené rozhodnutím ako finálnou formou činnosti správneho orgánu. Neznamená to pritom len uloženie sankcie; výsledkom môže byť aj rozhodnutie o zastavení konania, prípadne rozhodnutie, ktorým sa od uloženia sankcie upustí. Význam tohto princípu spočíva v tom, že **vytvára právnu istotu, uzatvára procesné postavenie účastníka a viaže sa naň aj účinok *res iudicata*** (lat. *„vec rozsúdená"*) čo má podstatný vplyv na aplikovanie

[630] *Hamuľáková, Z.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 71.
[631] Bližšie pozri: § 12 ods. 2 PriesZ.
[632] Bližšie pozri: rozsudok NS SR sp. zn. 8Sžo/28/2007 z 1. septembra 2008; uznesenie NS SR sp. zn. 2 Sžf/9/2010 z 16. februára 2011; rozsudok NS SR sp. zn. Sžf/44/2011 z 19. októbra 2011; rozsudok NS SR sp. zn. 5Sžf/53/2014 zo 16. decembra 2014.
[633] *Srebalová, M.* Absorbčná zásada vo vnútroštátnej právnej úprave správneho trestania. In. *Lenhart, M., Hapčová, I., Hamuľák, J. (ed).* 2016. Vplyv európskeho práva na kreovanie princípov a zásad správneho trestania: Zborník príspevkov z medzinárodnej vedeckej konferencie Bratislavské právnické fórum 2016 organizovanej Univerzitou Komenského v Bratislave, Právnickou fakultou v dňoch 21. – 22. októbra 2016. Bratislava : Univerzita komenského v Bratislave, právnická fakulta, vydavateľské oddelenie, s. 182 – 189.

princípu *ne bis in idem*. V správnom trestaní preto nestačí, aby správny orgán vec len preveroval alebo procesne viedol; ak vo veci koná, musí ju zákonným spôsobom aj autoritatívne ukončiť.[634]

15. **Princíp zákazu zneužitia správnej úvahy a právo na odôvodnenie rozhodnutia o uloženej sankcii** – tam, **kde zákon ponecháva správnemu orgánu priestor na správnu úvahu, nejde o voľnosť neobmedzenú, ale o úvahu viazanú zákonom**, účelom sankcie a okolnosťami konkrétneho prípadu. Tento princíp sa v správnom trestaní prejavuje už vo fáze **dokazovania ale taktiež aj výbere druhu sankcie a pri určení jej výmery v rámci zákonného rozpätia**, kde musí správny orgán zvoliť taký postih, ktorý zodpovedá závažnosti skutku.[635] Zároveň musí svoju úvahu presvedčivo vysvetliť v odôvodnení. Osobitný význam má tento princíp napr. aj pri **sankciách podľa ZoKB**, kde vysoké sankčné rozpätia, o. i. naviazané aj na percentá celosvetového ročného obratu[636] zvyšujú nároky na racionálne a preskúmateľné odôvodnenie.
16. **Zásada legitímneho očakávania** – predstavuje v správnom trestaní osobitný **prejav princípu právnej istoty** a chráni adresáta verejnej moci pred **nepredvídateľným zásahom** do jeho právneho postavenia.[637] Jej podstata spočíva v tom, že jednotlivec sa môže pri dôvere v zákon, ustálenú aplikačnú prax a doterajší postup správnych orgánov oprávnene spoliehať na **predvídateľné rozhodovanie**. V oblasti administratívnoprávnej zodpovednosti sa táto zásada prejavuje najmä v požiadavke, aby správny orgán **v skutkovo zhodných alebo porovnateľných prípadoch rozhodoval obdobne** a aby prípadné odchýlky od doterajšej rozhodovacej línie boli vecne odôvodnené, preskúmateľné a nevykazovali znaky svojvôle.
17. **Princíp zákazu *reformatio in peius*** – z latinského *„zmena k horšiemu*" vyjadruje princíp, v ktorého zmysle **nemôže správny orgán v odvolacom konaní uložiť**

[634] *Hamuľáková, Z.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 72.
[635] *Hamuľáková, Z.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 73.
[636] Bližšie pozri: § 31 ods. 2. a 3. zákona ZoKB.
[637] *Masárová, Ľ., Maslen, M.* Princíp legitímnych očakávaní – integrálny prvok princípu právnej istoty v oblasti verejného práva. In. *Maslen, M. – Masárová, Ľ. (ed.).* 2018. Legitímne očakávania, transparentnosť verejnej správy a zneužívanie práv v aplikačnej praxi v právnom štáte: Zborník z medzinárodnej vedeckej konferencie „Právny štát – medzi vedou a umením", ako súčasti medzinárodného vedeckého kongresu Trnavské právnické dni, 20. – 21. septembra 2018. Trnava : Právnická fakulta TU v Trnave, 2018. Bratislava : Wolters Kluwer, 2018, s. 85.

prísnejšiu sankciu než uložil v rámci konania na prvom stupni. Princíp teda patrí medzi základné zásady konania o opravných prostriedkoch. Jeho význam spočíva v tom, že odstraňuje obavu účastníka z toho, že podaním opravného prostriedku by si mohol zhoršiť svoje postavenie.[638] Práve týmto spôsobom podporuje reálne využívanie opravných prostriedkov, ktoré právny poriadok účastníkovi priznáva. Táto zásada tak napomáha tomu, aby systém opravných prostriedkov nebol len formálny, ale aj prakticky funkčný.[639]

18. **Princíp preskúmateľnosti rozhodnutia, ktorým sa ukladá sankcia** – nastupuje v okamihu platnosti rozhodnutia a **umožňuje adresátom využiť prostriedky na iniciovanie prieskumu rozhodnutia**. Ide o priame vyjadrenie všeobecných zásad správneho konania. Primárne o vyjadrenie **zásady zákonnosti a zásady materiálnej pravdy**. Je úzko spätá aj princípom ukončenia konania o delikte rozhodnutím, so zásadou legitímneho očakávania ako aj s princípom zákazu zneužitia správnej úvahy a práva na odôvodnenie rozhodnutia o uložení sankcie ale aj s princípom *reformatio in peius*. Adresát rozhodnutia môže v rámci správneho konania iniciovať prieskum druhostupňovým orgánom a to vo forme podania odvolania alebo rozkladu ale aj vo forme správnej žaloby. S podnetom sa môže obrátiť okrem iného obrátiť aj na prokuratúru. Výsledkom aplikácie tohto princípu má byť **nezávisle a nestranné posúdenie viny a uloženia trestu** v nadväznosti na spáchaný správneho delikt. ZoKB a ZoITVS realizujú preskúmavanie rozhodnutia o vine a sankcii za administratívny delikt prostredníctvom konania o rozklade.

Z uvedeného prehľadu vyplýva, že **princípy správneho trestania nie sú od všeobecných zásad správneho konania oddelené**, ale predstavujú ich osobitné, sankčne orientované rozvinutie. Ich spoločným základom je predovšetkým **zásada zákonnosti**, z ktorej sa odvodzuje nielen princíp *nullum crimen sine lege*, ale aj legalita postihu, zákaz zneužitia správnej úvahy, požiadavka ukončenia veci rozhodnutím a preskúmateľnosť sankčného rozhodnutia. Na **zásadu materiálnej pravdy** priamo nadväzuje dôkazné bremeno správneho orgánu, princíp *in dubio pro reo* aj zákaz donucovania k sebaobviňovaniu, keďže len úplne a spoľahlivo zistený skutkový stav môže byť podkladom zákonného výroku o vine a

[638] *Vrabko, M. a kol.* Správne právo procesné. Všeobecná časť. 1. vydanie. Bratislava : C. H. Beck, 2013, s. 45.
[639] *Hamuľáková, Z.* Zákaz reformatio in peius v správnom konaní. 1. vydanie. Bratislava : Wolters Kluwer SR s. r. o., 2020, s. 18.

sankcii. Rovnako **zásada aktívnej súčinnosti, zásada spolupráce** a **zásada procesnej rovnosti** vytvárajú procesný priestor pre riadny zákonný proces, prezumpciu neviny, obhajobu a reálne uplatnenie opravných prostriedkov.

Osobitné princípy správneho trestania zároveň konkretizujú aj tie základné zásady, ktoré smerujú k primeranosti a spravodlivosti výkonu verejnej moci. **Zásada rýchlosti a hospodárnosti** sa v správnom trestaní premieta do požiadavky primeranej lehoty na vydanie rozhodnutia a do ochrany pred neprimeraným procesným zaťažovaním účastníka konania. **Zásada materiálnej rovnosti** sa prejavuje najmä v princípe legitímneho očakávania, v proporcionalite sankcie a v rovnakom prístupe k sankcionovaniu skutkovo porovnateľných prípadov. S ňou úzko súvisí aj zákaz *reformatio in peius*. Na ochranu právnej istoty potom nadväzujú princípy ***ne bis in idem***, prihliadnutia na už uloženú sankciu a absorbčná zásada, ktoré bránia neprimeranej kumulácii represie. V konečnom dôsledku tak všeobecné zásady správneho konania vytvárajú základný procesný rámec, zatiaľ čo princípy správneho trestania tento rámec **spresňujú pre situácie, v ktorých správny orgán autoritatívne rozhoduje o delikte a sankcii**.

9.5 Pramene správneho práva trestného a europeizácia správneho trestania

Správne právo trestné je vytvárané **viacvrstvovým systémom prameňov**, v ktorom sa **vnútroštátna právna úprava prelína s európskymi a medzinárodnými štandardmi ochrany základných práv**. Na vnútroštátnej úrovni jeho základ tvoria najmä Ústava SR, Správny poriadok, Priestupkový zákon a osobitné zákony upravujúce jednotlivé správne delikty. **Správne právo trestné však nemožno vykladať izolovane od európskeho právneho priestoru**. Europeizácia správneho trestania sa prejavuje predovšetkým tým, že výkon sankčnej právomoci verejnej správy je čoraz výraznejšie limitovaný požiadavkami vyplývajúcimi z Dohovoru, z judikatúry Európskeho súdu pre ľudské práva, z práva Európskej únie a z odporúčacích aktov Rady Európy, ktoré postupne formujú spoločný minimálny štandard zákonnosti, proporcionality, procesnej spravodlivosti, súdnej preskúmateľnosti a ochrany pred svojvôľou. Hoci správne trestanie zostáva prevažne v rukách vnútroštátneho zákonodarcu a správnych orgánov, jeho súčasná podoba je už výsledkom zjavného harmonizačného tlaku, ktorý smeruje k zbližovaniu základných princípov sankcionovania

naprieč európskym právnym priestorom. Oblasť európskej regulácie ochrany osobných údajov a kybernetickej bezpečnosti je v posledných rokoch najlepším dôkazom výrazného vplyvu europeizácie na vnútroštátnu úpravu.

Kľúčovým medzinárodným dokumentom pre oblasť správneho trestania je Dohovor o ochrane ľudských práv a základných slobôd, ktorý vznikol na pôde Rady Európy. Hoc dohovor používa pojem *trestný čin* z hľadiska správneho práva trestného je nutné ho na základe rozhodovacej činnosti ESĽP aplikovať aj na správne delikty.[640] V európskom kontexte treba osobitne zdôrazniť význam Odporúčania Výboru ministrov Rady Európy (91) 1 o správnych sankciách a Rezolúcie Výboru ministrov Rady Európy (77) 31 o ochrane jednotlivca vo vzťahu k rozhodnutiam správnych orgánov. Tieto akty, spolu s nadväzujúcou judikatúrou ESĽP, vytvárajú základný európsky štandard správneho trestania, ktorý správne sankcionovanie približuje požiadavkám spravodlivého procesu známym zo súdneho trestania. Ich význam spočíva najmä v posilnení zákonnosti, procesných záruk, ochrany jednotlivca pred svojvôľou a v požiadavke dodatočných garancií pri ukladaní správnych sankcií.[641] Správne právo trestne v súčasnosti ovplyvňujú aj novšie únijné akty, najmä nariadenie DORA, smernica NIS2 či nariadenie GDPR, ktoré už v osobitných regulovaných oblastiach výslovne formujú sankčnú politiku, dohľadové mechanizmy a osobitné režimy administratívnoprávnej zodpovednosti.

Na všeobecnú národnú úpravu správneho práva trestného zmienenú vyššie nadväzuje v našom prípade osobitná, sektorová úprava týkajúca sa kybernetickej bezpečnosti. Ide najmä o

1. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov,
2. zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov,
3. zákon č. 367/2024 Z. z. o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov,
4. zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov,

[640] *Horvat, M.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 35.
[641] *Vrabko, M. a kol.* Správne právo procesné. Všeobecná časť. 1. vydanie. Bratislava : C. H. Beck, 2013, s. 41.

5. 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),
6. zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

Uvedené predpisy predstavujú vo vzťahu k všeobecnému režimu správneho práva trestného **osobitnú právnu úpravu**, teda režim **lex specialis**, prostredníctvom ktorého sa všeobecné princípy správneho trestania premietajú do konkrétnej sektorovej regulácie. Ich význam spočíva najmä v tom, že spravidla upravujú **hmotnoprávnu stránku** správneho práva trestného: vymedzujú osobitné povinnosti adresátov právnej regulácie, určujú okruh chránených záujmov a opisujú tie formy nežiaduceho konania alebo opomenutia, ktorých porušenie zakladá vznik administratívnoprávnej zodpovednosti. Práve v týchto predpisoch sa preto najvýraznejšie konkretizuje objekt správneho deliktu, jeho objektívna stránka, ako aj osobitosti sankčného mechanizmu viazaného na konkrétny regulovaný úsek.

Zároveň platí, že jednotlivé sektorové zákony neupravujú administratívno-právnu zodpovednosť jednotným spôsobom. Niektoré z nich pracujú súbežne s režimom **priestupkov** aj **iných správnych deliktov**, zatiaľ čo iné sú vystavané predovšetkým alebo výlučne na režime správnych deliktov, najmä vo vzťahu k právnickým osobám a podnikajúcim fyzickým osobám, či subjektom verejnej správy v pozícii spravovaného subjektu. Aj preto je potrebné ich popisovať osobitne, s dôrazom na ich vnútornú systematiku, chránený objekt a zákonom zvolený model sankcionovania. V osobitnej časti tejto kapitoly sa preto budeme venovať práve týmto sektorovým predpisom, pričom ťažisko výkladu bude spočívať najmä na **ZoKB** a **ZoITVS**. Práve tieto dva predpisy tvoria jadro administratívnoprávnej zodpovednosti kybernetickej bezpečnosti a vytvárajú priestor na didaktickú analýzu jednotlivých druhov správnych deliktov až do úrovne znakov skutkovej podstaty a ich následnej kategorizácie.

9.6 Delenie správnych deliktov

V slovenskej teórii možno nájsť **viacero delení správnych deliktov**.[642] Niektoré vychádzajú z povahy subjektu, iné zo spôsobu zodpovednosti alebo z funkcie konkrétneho režimu. V ďalšom výklade budeme používať toto základné pracovné členenie:

1. **priestupky,**
2. **iné správne delikty fyzických osôb,**
3. **správne delikty právnických osôb a fyzických osôb – podnikateľov,**
4. **správne disciplinárne delikty,**
5. **správne poriadkové delikty**.

Takéto členenie zodpovedá aj slovenskej odbornej diskusii o správnom trestaní. V nej sa ako základné kategórie uvádzajú priestupky, delikty fyzických a právnických osôb postihované bez ohľadu na zavinenie, disciplinárne delikty a poriadkové delikty.[643]

Z hľadiska systematiky tejto učebnice je osobitná pozornosť sústredená najmä na **priestupky, iné správne delikty fyzických osôb a správne delikty právnických osôb a fyzických osôb – podnikateľov**, keďže práve tieto tri kategórie tvoria jadro prakticky najvýznamnejších foriem správnych deliktov v kybernetickej bezpečnosti. Prostredníctvom priestupkov približujeme procesný a hmotnoprávny rámec správneho trestania, vrátane tých inštitútov, ktoré majú význam aj pre všeobecnú teóriu deliktuálnej administratívnoprávnej zodpovednosti. Z toho dôvodu im je venovaná osobitná pozornosť. Výklad iných správnych deliktov fyzických osôb a správnych deliktov podnikateľských subjektov následne umožní zachytiť osobitosti zodpovednosti subjektov, ktoré vystupujú v regulovaných sektoroch, najmä v oblastiach upravených osobitnými zákonmi popísanými v tejto učebnici. Správne disciplinárne delikty a správne poriadkové delikty sú spracované stručnejšie, predovšetkým z hľadiska ich zaradenia do systematiky správnych deliktov, a záver tejto časti dopĺňa stručný výklad zodpovednosti za výkon verejnej správy.

---

[642] Bližšie pozri: *Vrabko, M. a kol.* Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava : Ch. H. Beck, 2025, s. 212. alebo *Horvat, M* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 20 - 21.

[643] Primerane porovnaj: *Machajová, J.* In *Škultéty, P. a kol.* Správne právo hmotné. Všeobecná časť. Bratislava : VO PraF UK, 2005, s. 151; *Cepek, B.* In *Vrabko, M*. a kol. Správne právo hmotné. Všeobecná časť. Bratislava : C. H. Beck, 2012, s. 282; *Košičiarová, S.* Správne právo hmotné. Všeobecná časť. Plzeň : Aleš Čeněk, 2015, s. 217; *Hamuľáková, Z.* In *Vrabko, M. a kol.* Správne právo hmotné. Všeobecná časť. Bratislava : C. H. Beck, 2018, s. 208. poznámka pod čiarou prebratá z: *Horvat, M.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 21.

9.6.1 Priestupok

Priestupky predstavujú tradičný a historicky najviac rozpracovaný druh správneho deliktu. V zmysle legálnej definície je priestupok ***zavinené konanie, ktoré porušuje alebo ohrozuje záujem spoločnosti a je za priestupok výslovne označené v tomto alebo v inom zákone, ak nejde o iný správny delikt postihnuteľný podľa osobitných právnych predpisov, alebo o trestný čin.***[644] Zákon pri definícii neurčuje konkrétnu skutkovú podstatu, ale pre účel zachovania univerzálnosti definície vymedzuje všeobecné znaky priestupku.[645] **Od roku 2024 sa za priestupok považuje aj priestupok spáchaný prostredníctvom elektronickej komunikačnej služby ak to povaha priestupku umožňuje.**[646] Tento princíp sa uplatňoval už pred legislatívnou zmenou z roku 2024 čo pripúšťa aj zákonodarca v dôvodovej správe a svoj motív priamo uviesť túto skutočnosť v Priestupkovom zákone opiera o explicitnosť právnej úpravy.[647]

9.6.1.1 Znaky priestupku

Priestupok je typicky viazaný na **fyzickú osobu** a na princíp **subjektívnej zodpovednosti**, keďže zákon vyžaduje zavinenie, spravidla aspoň vo forme nedbanlivosti. Znaky priestupku rozdeľujeme na materiálne a formálne.

Materiálnymi znakmi priestupku sú:

1. **zavinenie** (zavinené konanie) – nedbanlivosť alebo úmysel,
2. **škodlivosť** (konanie, ktoré porušuje alebo ohrozuje záujem spoločnosti) – záujem spoločnosti je právne neurčitý (vágny) pojem. Spolu s pojmami verejný záujem a spoločenský záujem predstavujú objekt priestupku.[648] Právna neurčitosť pojmu je zámerná, pretože v tomto prípade má rôznorodé vyjadrenie v závislosti od okruhu spoločenských vzťahov regulovaných normami správneho práva a tak posúdenie tohto znaku spadá do rámca *ad hoc* posúdenia za použitia správnej úvahy správnym orgánom v rámci konkrétnej sektorovej úpravy a jej potrieb.

[644] Bližšie pozri: § 2 PriesZ.
[645] *Košičiarová, S.* Zákon o priestupkoch. Podrobný komentár s judikatúrou. Praha : Leges, 2020, s. 84.
[646] Bližšie pozri: § 2 ods. 3 PriesZ.
[647] Bližšie pozri: Národná rada Slovenskej republiky (2023 – doposiaľ), parlamentná tlač 364 – Vládny návrh zákona o niektorých opatreniach na zlepšenie bezpečnostnej situácie v Slovenskej republike.
[648] *Srebalová, M.* § 2 Pojem priestupku. In: *Srebalová, M a kol.* Zákon o priestupkoch. 2. vydanie. Bratislava: C. H. Beck, 2020, s. 7–8.

Formálnymi znakmi priestupku sú:

1. **všeobecné znaky priestupku**, ktoré sú spoločné pre všetky priestupky, napríklad zavinenie, vek alebo príčetnosť páchateľa, a
2. **znaky skutkovej podstaty priestupku**, ktoré umožňujú jednotlivé priestupky bližšie identifikovať. Skutková podstata priestupku musí zahŕňať štyri základné znaky, a to:
   a. **subjekt –** deliktuálne spôsobilý páchateľ, ktorý svojím konaním naplnil všetky znaky skutkovej podstaty priestupku;
   b. **subjektívnu stránku –** vnútorný psychický stav páchateľa k svojmu konaniu a jeho následku založený na vôľovej a intelektuálnej zložke;
   c. **objekt –** zákonom chránené spoločenské vzťahy, pričom zásahy do nich zákon označuje ako priestupky a
   d. **objektívnu stránku –** konanie → následok = príčinná súvislosť.

PriesZ vymedzuje, kedy konanie nie je možné považovať za priestupok v súvislosti s naplnením **okolností vylučujúcich protiprávnosť konania**. Pôsobia *ex tunc*, takže konanie od samého začiatku nie je správnym deliktom.[649] Ide o:

1. **nutnú obranu** – niekto odvracia primeraným spôsobom hroziaci útok na zákonom chránený záujem, alebo
2. **krajnú núdzu** – niekto odvracia nebezpečenstvo priamo hroziace zákonom chránenému záujmu s podmienkou, že takýmto konaním nebol spôsobený zrejme rovnako závažný následok, ako ten ktorý hrozil a nebezpečenstvo nebolo možné v danej situácii odvrátiť inak.

Naplnenie okolnosti vylučujúcej protiprávnosť konania si vyžaduje **naplnenie niekoľkých podmienok**. V prípade **nutnej obrany** to je útok na zákonom chránený záujem, priamo trvajúci alebo hroziaci útok a primeranosť obrany. V prípade **krajnej núdze** ide o existenciu nebezpečenstva, bezprostrednú resp. priamu hrozbu, subsidiarita krajnej núdze a proporcionalita krajnej núdze.[650]

Od okolností vylučujúcich protiprávnosť konania je potrebné odlíšiť **dôvody zániku trestnosti** (zodpovednosti) a **okolnosti vylučujúce zodpovednosť**. K zániku trestnosti

[649] *Prášková, H.* Základy odpovědnosti za správní delikty. 1. vydání. Praha : C. H. Beck, 2013, s. 336.
[650] Bližšie pozri: *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 87 – 88.

dochádza, keď subjekt spácha priestupok no dodatočne stratí svoju spoločenskú škodlivosť a nemožno ho dodatočne prejednať. Dochádza k nemu *ex nunc* čo je ďalší zo znakov odlišujúcich dôvody zániku trestnosti od okolnosti vylučujúcej protiprávnosť konania.[651] Ide o prípady spojené s:

1. **uplynutím času** – zákon stanovuje lehotu v ktorej je možné priestupok od jeho spáchania prejednať;
2. **udelením amnestie** – amnestiu za spáchané priestupky udeľuje vláda SR; [652]
3. **smrťou páchateľa** – zánik subjektu ako jedného zo znakov skutkovej podstaty;
4. **legislatívnou zmenou** – zmenou zákona konanie prestane byť deliktuálne. [653,654]

Okolnosti vylučujúce zodpovednosť sa viažu na subjekt priestupku a týkajú sa jeho veku a príčetnosti. Za priestupok môže byť zodpovedná iba fyzická osoba, ktorá dovŕšila 14 rokov veku a v čase spáchania skutku je príčetná. Nepríčetnosť si však nesmie privodiť sama užívaním alkoholických alebo omamných a psychotropných látok.[655]

9.6.1.2 Sankcie a ochranné opatrenia

Za spáchanie priestupku môže správny orgán uložiť **sankciu** alebo **ochranné opatrenie**. PriesZ upravuje tieto sankcie:

1. **pokarhanie,**
2. **pokuta,**
3. **zákaz činnosti,**
4. **prepadnutie veci.**

Pri ukladaní sankcie[656] musí brať správny orgán do úvahy:

1. **závažnosť priestupku** – spôsob spáchania priestupku, jeho následky a okolnosti, za ktorých bol priestupok spáchaný;
2. **mieru zavinenia** – za vážnejšie sa považuje úmyselné zavinenie;
3. **pohnútky** – aká bola vnútorná motivácia páchateľa;

[651] *Prášková, H.* Základy odpovědnosti za správní delikty. 1. vydání. Praha : C. H. Beck, 2013, s. 336.
[652] K bodu 1 a bodu 2 bližšie pozri: § 20 ods. 1 PriesZ.
[653] Bližšie pozri: § 7 ods. 1 PriesZ.
[654] Pozn.: V danom prípade ide o tzv. **pravú retroaktivitu** to znamená, že na posúdenie skutku sa nepoužije úprava platná v čase spáchania skutku ale novšia za predpokladu, že je pre páchateľa priaznivejšia.
[655] Bližšie pozri: § 5 PriesZ.
[656] Bližšie pozri: § 12 ods. 1 PriesZ.

4. **osobu páchateľa** – špeciálny subjekt, všeobecne určený subjekt, či ide o prvopáchateľa alebo recidivistu;
5. **či a akým spôsobom bol subjekt za ten istý skutok postihnutý v disciplinárnom alebo kárnom konaní** – neuplatňuje sa princíp *ne bis in idem* a správny orgán môže rozhodnúť o uložení sankcie ale aj o upustení od sankcie v závislosti od posúdenia konkrétneho prípadu.[657]

Od uloženia sankcie možno v rozhodnutí o priestupku upustiť, ak k náprave páchateľa postačí samotné prejednanie priestupku.[658] V takomto prípade sa rozhodnutím výlučne vysloví vina páchateľa bez uloženia sankcie.[659] Tento režim v prípade iných správnych deliktov preberá ZoKB ale aj ZoITVS.

V prípade, že sa páchateľ dopustí viacerých priestupkov správny orgán uloží sankciu podľa ustanovenia viažuceho sa na najprísnejšie postihnuteľný priestupok. PriesZ týmto **vylučuje** tzv. **sčítaciu metódu**[660], na ktorej základe sa postih za minimálne dva spáchané priestupky sčíta. **Využíva sa** tu tzv. **kumulatívna a absorbčná metóda**[661,662], v ktorej zmysle prísnejšia sankcia absorbuje menej prísnu sankciu.[663] V prípade pokuty môže správny orgán jej výšku napočítať iba do výšky hornej sadzby za najzávažnejší skutok. Jej výšku však musí stanoviť na základe okolností, posúdenia škodlivosti a pod. Zákaz činnosti môže správny orgán uložiť, len ak ho možno uložiť za niektorý zo spáchaných priestupkov.[664]

Najmiernejšou možnou sankciou, ktorej uloženie pripúšťa Priestupkový zákon v riadnom konaní je **pokarhanie**. Ukladá sa pri priestupkoch nižšej závažnosti. Jeho význam spočíva predovšetkým v **morálnom pôsobení na páchateľa**, nie v majetkovom postihu. Aj preto ho **nemožno uložiť spolu s pokutou**, hoci môže byť kombinované s inými sankciami, napríklad so zákazom činnosti alebo s prepadnutím veci. Pokarhanie sa **ukladá rozhodnutím**. Ústne vyhlásenie má význam vtedy, ak je účastník prítomný, pretože umožňuje

[657] *Hamuľáková, Z.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 102 - 103.
[658] Bližšie pozri: *Srebalová, M.* § 11 [Druhy sankcií a ukladanie sankcií]. In: *Srebalová, M. a kol.* Zákon o priestupkoch. 2. vydanie. Bratislava: C. H. Beck, 2020, s. 58–59.
[659] *Vrabko, M. a kol.* Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava : Ch. H. Beck, 2025, s. 220.
[660] Napr.: Páchateľ spácha dva priestupky pričom za každý skutok je možné udeliť pokutu do tisíc eur a správny orgán rozhodne o udelení pokuty vo výške dvetisíc eur.
[661] Napr.: Páchateľ spácha dva priestupky, za jeden mu hrozí pokuta päťsto eur a za druhý pokuta tisíc eur. Správny orgán v závislosti od závažnosti môže rozhodnúť o udelení pokuty do tisíc eur.
[662] Bližšie pozri absorbčná zásada v časti Princípy (zásady) správneho trestania.
[663] *Košičiarová, S.* Zákon o priestupkoch. Podrobný komentár s judikatúrou. Praha : Leges, 2020, s. 163.
[664] Bližšie pozri: § 12 ods. 2 PriesZ.

bezprostredné výchovné pôsobenie. Za deň oznámenia sa však považuje len vtedy, ak sa účastník výslovne vzdá práva na doručenie písomného rozhodnutia, pričom o tomto vyhlásení treba spísať zápisnicu. Pokarhanie nemožno uložiť v blokovom konaní.[665] V blokovom konaní je možné vybaviť priestupok napomenutím.[666]

Najbežnejšiu a najčastejšie udeľovanou sankciou za priestupky je bezpochyby **pokuta.** Pokuta sa veľmi bežne ako sankcia využíva aj pri iných správnych deliktoch v jednotlivých sektorových predpisoch. Výťažok z nej spravidla tvorí **príjem štátneho rozpočtu**[667] ale môže tvoriť aj príjem obce či subjektu určeného osobitným predpisom. V prípade jej nezaplatenia môže byť predmetom núteného výkonu vo forme peňažnej exekúcie. **Výška pokuty sa líši** v závislosti od spáchaného priestupku. Spravidla určuje zákon rozpätie určením iba hornej hranice (napr. do 33 eur) alebo určením dolnej aj hornej hranice (napr. od 33 do 330 eur). Špeciálna úprava hornej hranice pokuty sa týka mladistvých znížením na polovicu a stanovením maximálnej výšky.[668] Pokutu možno uložiť aj v **skrátených formách** priestupkového konania v **blokovom konaní** a v **rozkaznom konaní**[669].

Zákaz činnosti musí byť ako sankcia výslovne ustanovený právnym predpisom. Vzťahuje sa na **konanie, ktoré sa už uskutočnilo a nie na budúce správanie – *ex tunc***. V prípade *ex nunc* pôsobenia by išlo o opatrenie orgánu verejnej správy s tzv. kvázisankčnym charakterom.[670] Takéto opatrenie s kvázisankčným charakterom je typické pre **ZoKB**, kedy môže NBÚ ukladať tzv. **opatrenia na nápravu**.[671] Zákaz činnosti možno uložiť len vo vzťahu k činnosti, ktorá podlieha osobitnému právnemu režimu. Ide najmä o činnosť vykonávanú v rámci povolania alebo zamestnania v pracovnom pomere, v inom obdobnom pomere, alebo o činnosť, na ktorej výkon sa vyžaduje povolenie alebo súhlas štátneho orgánu. Podstatné je, že **musí ísť o činnosť, ktorú možno právne identifikovať a obmedziť**. Sankciu zákazu činnosti preto **nemožno uložiť pri činnostiach vykonávaných vo voľnom čase** alebo pri činnostiach, na ktoré vzniká oprávnenie priamo zo zákona bez osobitného povolenia.[672]

---

[665] *Srebalová, M.* § 11 [Druhy sankcií a ukladanie sankcií]. In: *Srebalová, M. a kol.* Zákon o priestupkoch. 2. vydanie. Bratislava: C. H. Beck, 2020, s. 56–57.
[666] *Košičiarová, S.* Zákon o priestupkoch. Podrobný komentár s judikatúrou. Praha : Leges, 2020, s. 147.
[667] Bližšie pozri: § 30 ods. 5 a 31 ods. 20 ZoKB ale aj § 29 ods. 5 ZoITVS.
[668] *Srebalová, M.* § 13 [Pokuta]. In: *Srebalová, M. a kol.* Zákon o priestupkoch. 2. vydanie. Bratislava: C. H. Beck, 2020, s. 68.
[669] Bližšie pozri § 29l ods. 2 ZoKB.
[670] *Košičiarová, S.* Zákon o priestupkoch. Podrobný komentár s judikatúrou. Praha : Leges, 2020, s. 175.
[671] Bližšie pozri: § 29j ZoKB.
[672] *Srebalová, M.* § 14 [Zákaz činnosti]. In: *Srebalová, M. a kol.* Zákon o priestupkoch. 2. vydanie. Bratislava: C. H. Beck, 2020, s. 71–72.

Sankciu **prepadnutia veci** možno uložiť len za splnenia osobitných zákonných podmienok a popri všeobecných pravidlách ukladania sankcií. Jej účelom je:

1. zabrániť opakovaniu priestupku;
2. odňať páchateľovi vec použitú alebo určenú na spáchanie priestupku; prípadne
3. odňať prospech získaný priestupkom.

Uložiť ju možno len vtedy, ak **vec patrí výlučne páchateľovi**[673] a zároveň bola na priestupok **použitá, určená, získaná** priestupkom alebo **nadobudnutá za takú vec**. Ak vlastníctvo nie je jasné, správny orgán musí túto otázku najprv vyriešiť; ak prepadnutie uložiť nemožno, môže za splnenia zákonných podmienok prichádzať do úvahy **zhabanie veci**. Predmetom prepadnutia môže byť len konkrétna, individuálne určená a existujúca **hnuteľná vec**, ktorú treba v rozhodnutí presne označiť. Pri ukladaní tejto sankcie musí správny orgán rešpektovať **zásadu proporcionality**, najmä vzhľadom na hodnotu veci a jej účel. Prepadnutie preto spravidla **neprichádza do úvahy pri veciach vysokej hodnoty** alebo pri veciach, ktoré síce boli použité, ale svojou povahou nie sú určené na páchanie priestupkov. Vlastnícke právo k prepadnutej veci nadobúda SR dňom právoplatnosti rozhodnutia.[674]

Prehľad druhov sankcií ukladaných podľa Priestupkového zákona podľa Košičiarovej[675]:

<table>
<tr><td rowspan="2">Sankcie
(§ 11)</td><td colspan="2">Neskrátené konanie o priestupku</td><td colspan="2">Skrátené konanie o priestupku</td></tr>
<tr><td>konanie o priestupku
(§ 51)</td><td>spoločné konanie v prípade súbehu priestupkov
(§ 57 ods. 1)</td><td>blokové konanie
(§ 84)</td><td>rozkazné konanie
(§ 87)</td></tr>
<tr><td rowspan="2">pokarhanie
(§ 11 ods. 1)</td><td colspan="2">Pokarhanie nemožno uložiť spolu s pokutou
(§ 11 ods. 2)</td><td rowspan="2">nie</td><td rowspan="2">nie</td></tr>
<tr><td>áno

(možno uložiť aj v konaní</td><td>áno</td></tr>
</table>

[673] *Hamuľáková, Z.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 106.
[674] *Srebalová, M.* § 15 [Prepadnutie veci]. In: *Srebalová, M. a kol.* Zákon o priestupkoch. 2. vydanie. Bratislava: C. H. Beck, 2020, s. 75–77.
[675] *Košičiarová, S.* Zákon o priestupkoch. Podrobný komentár s judikatúrou. Praha : Leges, 2020, s. 149.

	podľa § 87 ods. 4 posledá veta)			
pokuta (§ 13)	áno	áno	áno	áno
zákaz činnosti (§ 14)	Možno uložiť len ak tak ustanovuje zákon.	Možno uložiť, len keď ho možno *uložiť* za niektorý z priestupkov spáchaných v súbehu. Ak zákaz činnosti za niektorý z priestupkov *nemožno* uložiť, nemožno ho uložiť ani pri postihu všetkých priestupkov spáchaných v súbehu.	nie	nie
prepadnutie veci (§ 15)	áno	Nemožno uložiť, len keď ho *nemožno* uložiť za priestupok najprísnejšie postihnuteľný. Predmetné pravidlo sa neuplatní, ak by zákon ukladal *povinnosť* prepadnutie veci uložiť za niektorý z priestupkov spáchaných v súbehu.	nie	nie

Tabuľka č. 5: Prehľad druhov sankcií ukladaných podľa Priestupkového zákona.

Ochranné opatrenia predstavujú popri sankciách osobitnú skupinu inštitútov priestupkového práva. Na rozdiel od sankcií, ktorých hlavný účel spočíva v represii, sú ochranné opatrenia zamerané predovšetkým na **preventívne a ochranné pôsobenie do budúcnosti**. Ich cieľom nie je v prvom rade potrestať páchateľa, ale zabrániť ďalšiemu porušovaniu alebo ohrozovaniu záujmov chránených zákonom. Sú to opatrenia štátneho donútenia spôsobujúce istú formu ujmy ich adresátom. So sankciami majú spoločné črty.[676]

Priestupkový zákon upravuje dva druhy ochranných opatrení:

1. **obmedzujúce opatrenie** a
2. **zhabanie veci**.

[676] *Hamuľáková, Z.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 106.

Spoločnou črtou oboch ochranných opatrení je, že smerujú k znemožneniu ďalšej protiprávnej činnosti a k ochrane spoločnosti pred jej opakovaním.[677] Pôsobia výlučne do budúcnosti a majú profylaktickú povahu.[678]

Obmedzujúce opatrenie sa viaže priamo na osobu páchateľa priestupku a sleduje najmä zníženie rizika opätovného páchania – recidívy. Jeho podstatou je obmedziť páchateľovi možnosť zdržiavať sa na miestach alebo v prostredí, s ktorými sa opakované páchanie priestupkov spravidla spája. Možno ho uložiť za podmienok, že:

1. je obmedzujúce opatrenie **primerané povahe a závažnosti priestupku** – zásada proporcionality;
2. je uložené **spolu so sankciou** – nedá sa uložiť samostatne a
3. je uložené **najdlhšie na obdobie jedného roka**.[679]

Zhabanie veci má odlišný charakter, keďže smeruje proti veci, ktorá bola použitá na spáchanie priestupku, bola na to určená, bola priestupkom získaná alebo bola nadobudnutá za vec získanú priestupkom. Na rozdiel od obmedzujúceho opatrenia môže zhabanie veci za splnenia zákonných podmienok zasiahnuť osobu odlišnú od páchateľa.[680] Za dodržania zásady proporcionality možno vec zhabať ak:

1. **patrí páchateľovi**, ktorého nemožno za priestupok stíhať, alebo
2. **nepatrí páchateľovi** priestupku a ak to vyžaduje bezpečnosť osôb majetku alebo iný všeobecný záujem.[681]

Ochranné opatrenia sú prostriedkom štátneho donútenia, a preto ich možno uložiť len pri rešpektovaní **zásady zákonnosti**. Správny orgán môže uložiť len také ochranné opatrenie, ktoré zákon výslovne pripúšťa, a len za podmienok, ktoré zákon ustanovuje. Zároveň sa na ich ukladanie vzťahuje aj **zásada proporcionality**. Správny orgán musí vždy posudzovať primeranosť opatrenia vzhľadom na povahu priestupku, osobu páchateľa a v prípade zhabania veci aj vzhľadom na hodnotu a povahu dotknutej veci. Ochranné opatrenia sa ukladajú vo výroku rozhodnutia o priestupku, musia byť riadne odôvodnené a možno ich uložiť len v riadnom priestupkovom konaní. Nemožno ho uložiť v skrátenej forme konania

[677] *Horvat, M.* § 16 [Druhy ochranných opatrení]. In: *Srebalová, M. a kol.* Zákon o priestupkoch. 2. vydanie. Bratislava: C. H. Beck, 2020, s. 78–79.
[678] *Košičiarová, S.* Zákon o priestupkoch. Podrobný komentár s judikatúrou. Praha : Leges, 2020, s. 194.
[679] *Vrabko, M. a kol.* Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava : Ch. H. Beck, 2025, s. 220.
[680] *Horvat, M.* § 16 [Druhy ochranných opatrení]. In: *Srebalová, M. a kol.* Zákon o priestupkoch. 2. vydanie. Bratislava: C. H. Beck, 2020, s. 79.
[681] *Vrabko, M. a kol.* Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava : Ch. H. Beck, 2025, s. 220.

o priestupku (blokové konanie, rozkazné konanie).[682] Ich význam spočíva v tom, že dopĺňajú sankčný systém tam, kde samotná sankcia nemusí byť dostatočná alebo nie je najvhodnejším prostriedkom ochrany spoločnosti. Na ochranné opatrenia sa **nevzťahuje amnestia.**[683]

9.6.1.3 Subsidiarita a analogia legis Priestupkového zákona

V systéme vyvodzovania administratívnoprávnej zodpovednosti za priestupky má osobitný význam **subsidiarita PriesZ**. V kontexte iných správnych deliktov ako priestupkov je to zase otázka ***analógie legis*** PriesZ. Pri priestupkoch sa v slovenskom právnom poriadku uplatňuje aj tzv. **dvojitá subsidiarita**.[684] Tá vzniká vtedy, keď osobitný zákon ako *lex specialis* najprv odkáže na PriesZ a ten následne odkáže na Správny poriadok. V takom prípade sa vytvára reťazec právnej úpravy: najprv sa použije osobitný sektorový predpis, potom PriesZ a napokon Správny poriadok. Takýto model je výslovne prítomný napríklad pri zákone o kybernetickej bezpečnosti,[685] zákone o kritickej infraštruktúre[686] či pri zákone o ochrane utajovaných skutočností,[687] ktoré vo veci prejednávania priestupkov odkazujú na *všeobecný predpis o priestupkoch*; samotný PriesZ potom ustanovuje, že ak on alebo iný zákon neustanovuje inak, na konanie o priestupku sa použijú *všeobecné predpisy o správnom konaní.*[688]

Z dogmatického hľadiska to znamená, že PriesZ plní vo vzťahu k viacerým osobitným resp. sektorovým úpravám, funkciu **osobitného všeobecného predpisu** pre priestupky, zatiaľ čo Správny poriadok vystupuje ako všeobecný procesný predpis, ktorý dopĺňa medzery tam, kde ich nevyplnil ani osobitný resp. sektorový zákon, ani PriesZ. Subsidiarita je teda zákonom predpokladaný mechanizmus doplnenia úpravy, nie voľná voľba správneho orgánu. Správny orgán preto nemôže medzi týmito predpismi ľubovoľne prechádzať, ale musí rešpektovať ich systematické poradie a pravidlo ***lex specialis derogat legi generali***. Z hľadiska subsidiarity rozlišujeme štyri procesné režimy:

---

[682] *Košičiarová, S.* Zákon o priestupkoch. Podrobný komentár s judikatúrou. Praha : Leges, 2020, s. 197.
[683] *Horvat, M.* § 16 [Druhy ochranných opatrení]. In: *Srebalová, M. a kol.* Zákon o priestupkoch. 2. vydanie. Bratislava: C. H. Beck, 2020, s. 82.
[684] *Hamuľáková, Z.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 113.
[685] § 30 ods. 3 ZoKB.
[686] § 17 ods. 4 zákona č. 367/2024 Z. z. o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov
[687] § 78 ods. 5 zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov.
[688] § 51 PriesZ.

1. výlučné použitie všeobecného predpisu;
2. použitie osobitného predpisu so subsidiárnym použitím všeobecného predpisu;
3. subsidiárne použitie len niektorých ustanovení všeobecného predpisu a použitie zvyšných ustanovení osobitného predpisu a
4. vylúčenie použitia všeobecného predpisu s výlučným použitím osobitného predpisu.[689]

Od subsidiarity treba odlíšiť ***analógiu legis*** **Zákona o priestupkoch** vo vzťahu k iným správnym deliktom. *Vo vzťahu k iným správnym deliktom sa zákon o priestupkoch nepoužije* a subsidiárne sa aplikuje iba Správny poriadok.[690] V prípade *analógie legis* už nejde o výslovný zákonný odkaz, ale o úvahu, či možno pri právnej medzere primerane použiť ustanovenie PriesZ na podobný režim. Takáto otázka vzniká najmä pri **iných správnych deliktoch fyzických osôb, správnych deliktoch právnických osôb a fyzických osôb – podnikateľov, správnych disciplinárnych deliktoch** a **správnych poriadkových deliktoch**. Ide teda o kategórie deliktov, ktoré stoja vedľa priestupkov, ale neriadia sa automaticky priestupkovým režimom. Úvahy o *analógii legis* sú na mieste a to najmä z dôvodu, že v *slovenský právny poriadok neobsahuje predpis, ktorý by unifikoval procesné pravidlá a postupy pri ukladaní sankcií za iné správne delikty. Čiastočne kodifikované sú iba priestupky.*[691]

Rozhodujúce pritom je, že ***analógia legis*** nesmie v hmotnoprávnej rovine rozširovať represiu v neprospech delikventa. Nemožno teda analogicky vytvárať nové skutkové podstaty, rozširovať okruh zodpovedných subjektov ani ukladať sankcie bez výslovného zákonného podkladu. **V procesnej rovine je primerané použitie zákona o priestupkoch možné len opatrne, ak osobitná úprava obsahuje medzeru a ak tým nedôjde k oslabeniu procesných garancií.** Stručne povedané, pri priestupkoch sa uplatňuje predovšetkým výslovná právna úprava a zákonom založená subsidiarita, kým pri ostatných správnych deliktoch môže PriesZ pôsobiť len ako obmedzený interpretačný vzor a to vždy s prihliadnutím na povahu konkrétneho režimu a na hranice princípu zákonnosti. V praxi sa

[689] Bližšie pozri: *Vrabko, M. a kol.* Správne právo procesné. Všeobecná časť. 1. vydanie. Bratislava : C. H. Beck, 2013, s. 57 – 58.
[690] *Čentéš, J., Beleš, A.* Vzťah kódexu správneho trestania a trestného práva. In. *Havelková, M., Grešová, L. a Bleho, Š. (zost.).* Nová právna úprava správneho trestania, Zborník z vedeckej konferencie konanej v dňoch 14. a 15. októbra 2021 v Bratislave. Bratislava : Univerzita Komenského v Bratislave, Právnická fakulta, 2021, s. 53.
[691] *Havelková, M.* Plná jurisdikcia správnych súdov a jej vplyv na administratívne konanie vo veciach správneho trestania. In Acta Facultatis Iuridicae Universitatis Comenianae, Tomus XXXIX, č. 1/2020. Bratislava : Právnická fakulta Univerzity Komenského v Bratislave, 2020, s. 117.

analógia legis PriesZ bežne využíva a preto jej v rámci učebnice venujeme osobitnú pozornosť. PriesZ v teoretickej rovine pomerne podrobne demonštruje štandardy vyvodzovania administratívnoprávnej zodpovednosti v súvislosti so všetkymi druhmi správnych deliktov.

9.6.1.4 Konanie o priestupkoch

Konanie o priestupkoch je osobitným druhom správneho konania, v ktorom príslušný správny orgán rozhoduje o vine a sankcii za priestupok. Ide o rozhodovací proces vo verejnej správe, ktorého výsledkom je individuálny správny akt – **rozhodnutie**. Toto štádium nadväzuje na predchádzajúce **objasňovanie priestupku,**[692] ktorého účelom je obstaranie podkladov potrebných na rozhodnutie. Priestupkové konanie tak predstavuje procesnú formu, prostredníctvom ktorej sa realizuje hmotnoprávna úprava priestupkov. Jeho cieľom je, aby správny orgán správne, objektívne a bez zbytočných prieťahov zistil, či bol priestupok spáchaný, kto ho spáchal, za akých okolností k nemu došlo a či je potrebné uložiť sankciu alebo iné opatrenie.[693] Osobitosťou priestupkového konania je, že ide o **správne trestné konanie**, teda o konanie s represívnym následkom, v ktorom sa rozhoduje o administratívnoprávnej zodpovednosti. V tomto kontexte je preto potrebné brať do úvahy aj spôsob a rozsah, akým môže správne trestanie zasiahnuť do základných ľudských práv a slobôd. Z toho dôvodu sa aj podľa Ústavného súdu SR kladú na správne trestné konanie nároky vyplývajúce z Čl. 6 ods. 1 Dohovoru upravujúce právo na spravodlivé súdne konanie, keďže povaha správneho trestného konania je obdobná s trestným konaním.[694]

9.6.1.5 Subjekty priestupkového konania

Priestupkové konanie diferencuje dva základné subjekty. Ide o **správny orgán** – orgán, ktorý vedie priestupkové konanie **a účastníkov konania**. Účastníci konania sú v rôznom procesnom postavení. Okrem správneho orgánu a účastníkov sa vo všeobecnosti na konaní môžu podieľať aj zúčastnené osoby[695] ale napr. aj zákonný zástupca, opatrovník,

[692] § 58 – 61 PriesZ.
[693] *Srebalová, M.* § 51 Všeobecné ustanovenie. In: *Srebalová, M. a kol.* Zákon o priestupkoch. 2. vydanie. Bratislava: C. H. Beck, 2020, s. 248–249.
[694] Nález ÚS SR z 15. októbra 1998 sp. zn. PL. ÚS 12/97 prebratý z *Košičiarová, S.* Zákon o priestupkoch. Podrobný komentár s judikatúrou. Praha : Leges, 2020, s. 428.
[695] Bližšie pozri: § 15a Správny poriadok

zástupca (splnomocnenec), svedkovia, znalci, tlmočníci, verejnosť a iné osoby, ktorých účasť je nevyhnutná pre potreby spoľahlivo zisteného stavu veci.

Subjekty priestupkového konania:

1. **Správny orgán –** subjekt konania, ktorý je dotovaný verejnou mocou dbajúci najmä o to aby občania nesťažovali plnenie úloh verejnej správy a nenarúšali verejný poriadok a občianske spolunažívanie.
2. **Účastníci konania** - medzi fakultatívnych účastníkov konania radíme spravidla obvineného z priestupku. Obligatórnymi účastníkmi sú v závislosti od priestupku a skutkových okolností poškodený; vlastník veci, ktorá podlieha režimu zhabania; navrhovateľ ak konanie začalo na návrh (často totožný s poškodeným).
3. **Iné subjekty** – subjekty, ktorých účasť je nevyhnutná pre spoľahlivo zistený stav veci a zákonný priebeh priestupkového konania.

Fakultatívnym subjektom na strane účastníkov **je obvinený** z priestupku. Toto procesné postavenie vychádza z **prezumpcie neviny** – a teda, že až do právoplatného rozhodnutia sa na obvineného hľadí, ako by skutok nespáchal. V spojení s aplikáciou Čl. 6 ods. 1 Dohovoru mu prislúcha aj špecifický katalóg jeho procesných oprávnení. Môže sa vyjadriť ku všetkým skutočnostiam kladeným za vinu, k vykonaným dôkazom, môže uplatňovať skutočnosti a dôkazy za účelom vedenia svojej obhajoby, podávať návrhy v konaní, odvolať sa voči rozhodnutiu na prvom stupni a nemôže byť donucovaný k výpovedi ani k priznaniu. Osobitný režim sa na obvineného využije aj v prípade ak ide o mladistvého.[696] V procesnom postavení obvineného môže byť v priestupkovom konaní výlučne fyzická osoba.

Poškodený vystupuje v konaní ako **obligatórny subjekt** a do konania vstupuje ak si uplatní nárok na náhradu škody spôsobenej priestupkom. **Náhradou škody sa správny orgán nebude zaoberať automaticky**. Konanie o náhrade škody sa nazýva aj ako **adhézne konanie.** Procesné oprávnenia poškodeného sú limitované fázou prejednania náhrady majetkovej škody spôsobenej priestupkom a rozhodnutím o náhrade škody. Oprávnenie podať opravný prostriedok je limitované na tú časť výroku rozhodnutia, ktorá sa týka otázky náhrady škody. **Cieľ, ktorý poškodený sleduje je cieľ nahradenia škody** osobou uznanou vinnou zo spáchania priestupku. To, ktorá osoba bude vinná zo spáchania priestupku je pre poškodeného v zásade irelevantné. Na to aby, bola škoda kvalifikovaná ako majetková musí

[696] *Hamuľáková, Z.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 132.

byť vyčísliteľná v peniazoch. Pôjde napr. o prípady ušlého zisku alebo škody na majetku.[697] Účastník na strane poškodeného môže byť fyzická osoba a rovnako tak aj právnická osoba.

Konanie o priestupku spravidla začína z úradnej povinnosti správneho orgánu. Môžu však nastať situácie, kedy konanie začína na návrh ďalšieho z radu **obligatórnych** subjektov na strane účastníka – **navrhovateľa.** Ide o osobu, ktorá je **postihnutá priestupkom** alebo jej **zákonného zástupcu** alebo **opatrovníka**. Spravidla ide o prípady, kedy vznikla postihnutej osobe **nemajetková ujma**. Nie je vylúčené, že jeden subjekt bude vystupovať v dvojjedinej procesnoprávnej pozícii ako navrhovateľ a zároveň aj ako poškodený.[698] Procesní práva navrhovateľa sa v prvom rade týkajú oprávnenia disponovať návrhom, nahliadať do spisu , navrhovať dôkazy, vyjadrovať sa k podkladom pre rozhodnutie, navrhovanie svedkov a pod.[699] V procesnom postavení navrhovateľa môže byť výlučne fyzická osoba.

Posledný z radu **obligatórnych** subjektov priestupkového konania je **vlastník veci, ktorá môže byť zhabaná alebo bola zhabaná** má rovnako ako všetky obligatórne subjekty limitované svoje procesnoprávne postavenie. **Odvolať** sa môže len proti tej časti rozhodnutia, ktorá sa týka zhabania veci. **Zhabanie veci je ochranné opatrenie**, ktoré prichádza do úvahy aj v situácii, keď vec patrí osobe, ktorú nemožno za priestupok stíhať, napríklad pre nedostatok veku, alebo keď vec nepatrí páchateľovi priestupku.[700]Účastníkom konania je výlučne v časti týkajúcej sa zhabania veci. Pripomíname, že v tomto prípade musíme dôsledne odlíšiť zhabanie veci od prepadnutia veci a zaistenia veci.[701]

9.6.1.6 Fázy priestupkového konania

Priestupkové konanie je správne konanie, ktoré sa skladá z niekoľkých fáz. Tie vedú k spoľahlivo zistenému stavu veci, prípadne aj vo forme vykonania nápravy v odvolacom konaní a následne k výkonu rozhodnutia, resp. inej finálnej formy činnosti, ktorá je výsledkom priestupkového konania.

---

[697] *Hamuľáková, Z.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 133 – 134.
[698] *Košičiarová, S.* Zákon o priestupkoch. Podrobný komentár s judikatúrou. Praha : Leges, 2020, s. 197.
[699] *Máčaj, Ľ.* Rozšírenie dispozičnej zásady v priestupkovom konaní? In. *Potešil, L., Hejč, D., Valdhans, J. (eds.).* Dny práva 2018 – Days of law 2018 Část III. – Řízení o přestupcích (nejen) z pohledu správních orgánů a správnich soudů. Sborník z konference. Brno : Masarykova univerzita. 2019, s. 173.
[700] *Hamuľáková, Z.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 134.
[701] Bližšie pozri: *Košičiarová, S.* Zákon o priestupkoch. Podrobný komentár s judikatúrou. Praha : Leges, 2020, s. 616.

Fázy priestupkového konania sú:

1. **Objasňovanie priestupkov** – predprocesná fáza.
2. **Konanie na prvom stupni** – realizuje sa vždy, je základným prvkom výkonu verejnej správy v rámci vyvodzovania administratívnoprávnej zodpovednosti za spáchané priestupky.
3. **Konanie o opravnom prostriedku** – realizuje sa v prípade, že niektorý z účastníkov konania namieta nezákonný postup alebo nezákonné rozhodnutie v prvostupňovom konaní.
4. **Vykonávacie konanie** – vyplýva z povahy finálnej formy činnosti, ktorou bežne končí priestupkové konanie – rozhodnutie, ktoré je možné vykonať dobrovoľne alebo prostredníctvom núteného výkonu rozhodnutia. Nastupuje v prípade právoplatnosti rozhodnutia o priestupku a dobrovoľného nesplnenia uloženej povinnosti.

Vo **fáze objasňovania** priestupkov, správny orgán obstaráva podklady, potrebné na rozhodnutie a zisťuje najmä **či došlo k spáchaniu skutku,** ktorý je priestupkom a **či tento skutok spáchala konkrétna osoba** podozrivá z jeho spáchania. Po zodpovedaní týchto dvoch otázok môže správny orgán pristúpiť k správnej úvahe o právnych následkoch priestupku. V ďalšom kroku objasňovania teda správny orgán hodnotí **či sa páchateľovi uloží sankcia,** alebo sa od jej uloženia **upustí,** ak na jeho nápravu postačuje samotné prejednanie priestupku. Súčasťou ustáľovania právneho názoru, v rámci objasňovania je aj rozhodovanie o tom či správny orgán má resp. či môže za daných skutkových okolností **uložiť ochranné opatrenie.** V tejto fáze sa ustáľuje aj procesná stratégia správneho orgánu. **Správny orgán vo fáze objasňovania kvalifikuje deliktuálne konanie, ustaľuje okruh účastníkov, pripravuje sa na dokazovanie a rozhodnutie vo veci.**

V zmysle PriesZ správny orgán začína konanie spravidla *ex officio* – z úradnej povinnosti. Vtedy sa uplatňuje **zásada oficiality**. Iba veľmi malé množstvo konaní začína na základe **dispozičnej zásady –** ide o priestupky na úseku práva na prístup k informáciám a priestupok ublíženia na cti.[702] Sú to prípady, kedy správny orgán nevie zo svojho postavenia určiť intenzitu spáchanej ujmy napr. miera, do akej sa poškodený cíti byť dotknutý na svojej cti.[703] Rozdeľ medzi zásadou oficiality a dispozičnou zásadou spočíva v tom, kto disponuje

[702] *Hamuľáková, Z.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 124.

[703] Príklad: Inak môže vnímať urážku na cti rozhodca šiestej futbalovej ligy a inak môže vníma urážku na cti člena cirkevného spevokolu.

aktívnou legitimáciou začať priestupkové konanie. **Dispozičná zásada** priznáva toto oprávnenie účastníkovi konania – ten so svojím návrhom na začatie disponuje v každej fáze procesu až do vydania právoplatného rozhodnutia. To však neznamená, že je správny orgán zbavený svojej procesnoprávnej povinnosti uskutočňovať úkony v začatom správnom konaní, keďže aj pri návrhových konaniach sleduje ochranu a presadzovanie verejného záujmu.[704, 705]

Zásada oficiality priznáva toto oprávnenie správnemu orgánu, ktorý je vecne príslušný na vedenie priestupkového konania – konanie prebieha z jeho podnetu a nie je závislé na účastníkovi konania.[706] Zároveň **zásada oficiality** predpokladá, že pred priestupkovým konaním sa bude realizovať predprocesná fáza – **objasňovanie priestupkov**. Konanie, ktoré sa začína v intenciách **dispozičnej zásady** je správny orgán povinný realizovať aj **bez objasňovania**.[707]

Na prvom stupni konanie realizuje správny orgán vecne príslušný v zmysle PriesZ alebo osobitného právneho predpisu.[708] V prípade ZoKB je to NBÚ. Úlohou správneho orgánu je posúdiť, či došlo k porušeniu právnej povinnosti a právne správne vyhodnotiť všetky znaky priestupku a podmienky zodpovednosti. Priestupkové konanie je neoddeliteľne späté s posudzovaním skutkového aj právneho stavu. V tomto konaní sa rozhoduje o tom:

1. či konanie napĺňa znaky priestupku,
2. či je preukázané zavinenie,
3. či sú splnené podmienky na uloženie sankcie a
4. aký druh sankcie alebo opatrenia zodpovedá povahe prípadu.[709]

Pri rozhodovaní o priestupku musí správny orgán rešpektovať osobitné zásady priestupkového konania, všeobecné zásady správneho konania, ako aj základné požiadavky spravodlivého procesu.

---

[704] *Košičiarová, S.* Zákon o priestupkoch. Podrobný komentár s judikatúrou. Praha : Leges, 2020, s. 551 – 552.
[705] *Máčaj, Ľ.* Rozšírenie dispozičnej zásady v priestupkovom konaní? In. *Potešil, L., Hejč, D., Valdhans, J. (eds.).* Dny práva 2018 – Days of law 2018 Část III. – Řízení o přestupcích (nejen) z pohledu správních orgánů a správních soudů. Sborník z konference. Brno : Masarykova univerzita. 2019, s. 175 – 176.
[706] *Vrabko, M. a kol.* Správne právo procesné. Všeobecná časť. 1. vydanie. Bratislava : C. H. Beck, 2013, s. 68.
[707] *Hamuľáková, Z.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 117.
[708] Pre priblíženie vecnej príslušnosti pozri: *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 126 – 127.
[709] *Machajová, J.* Základy priestupkového práva. Komentár. Šamorín : Heuréka, 1998, s. 132 – 133. Prebraté z *Srebalová, M.* § 51 Všeobecné ustanovenie. In: *Srebalová, M. a kol.* Zákon o priestupkoch. 2. vydanie. Bratislava: C. H. Beck, 2020, s. 249.

Osobitne dôležitá je povinnosť správneho orgánu zistiť **presne a úplne skutkový stav veci**, obstarať potrebné dôkazy a tieto dôkazy riadne vyhodnotiť. Priestupkové konanie tak nie je len technickým postupom smerujúcim k uloženiu sankcie, ale predstavuje právne viazaný proces, ktorého účelom je zabezpečiť zákonné, spravodlivé a preskúmateľné rozhodnutie vo veci priestupku.[710]

Po skončení konania na prvom stupni, pred právoplatnosťou rozhodnutia má účastník konania možnosť podať voči rozhodnutiu odvolanie, prípadne ak na prvom stupni koná ústredný orgán štátnej správy **rozklad.** Rozsah oprávnenia podať odvolanie sa posudzuje v závislosti od procesného postavenia na strane účastníka konania. Obvinený sa môže odvolať v celom rozsahu a obligatórny účastníci iba v rozsahu, v akom sa výrok týka ich práv a povinností. S odvolacím konaním sa nevyhnutne spája zásada *reformatio on peius* – zákaz zmeny rozhodnutia v odvolacom konaní k horšiemu.[711] Pretože obvinený sa nemá obávať využiť riadne opravné prostriedky ako prostriedky svojej procesnej obrany.

9.6.1.7 Skrátené formy konania o priestupkoch

PriesZ pripúšťa realizovane konania aj tzv. skrátenou formou. Za týmto účelom využíva dva inštitúty – **blokové konanie** a **rozkazné konanie**. Skrátená forma priestupkového konania je predovšetkým naplnením **zásady hospodárnosti a efektívnosti správneho konania** všeobecne vyplývajúcej zo Správneho poriadku. V jej zmysle má správny orgán povinnosť dbať na to, aby konanie prebiehalo hospodárne a bez zbytočného zaťažovania účastníkov konania a iných osôb.[712] V oboch prípadoch je potrebné mať na zreteli, že ide o inštitúty využívané v rámci správneho trestania a tak musí obvinený zo spáchania priestupku disponovať kvalifikovanými inštitútmi procesnej obrany ako to predpokladá právo na spravodlivý proces. Rovnako ako v prípade blokového konania tak aj v prípade rozkazného konania musí byť splnený predpoklad, že správny orgán **objektívne posúdil** všetky okolnosti a podarilo sa mu **spoľahlivo zistiť** stav veci. V oboch typoch konaní disponuje obvinený zo spáchania priestupku **užšími procesnými oprávneniami**. V jeho procesnej dispozícii však zostáva kompetencia **iniciovať riadne konanie**. Obvinený zo

[710] *Srebalová, M.* § 51 Všeobecné ustanovenie. In: *Srebalová, M. a kol.* Zákon o priestupkoch. 2. vydanie. Bratislava: C. H. Beck, 2020, s. 256.
[711] *Hamuľáková, Z.* Zákaz reformatio in peius v správnom konaní. 1. vydanie. Bratislava : Wolters Kluwer SR s. r. o., 2020, s. 16.
[712] Bližšie pozri: § 3 ods. 4. posledná veta Správny poriadok.

spáchania priestupku je motivovaný využiť inštitút skráteného priestupkového konania najmä vo forme hrozby nižšou sankciou, ktorá mu hrozí. Deje sa tak najmä v súvislosti so skutočnosťou, že skrátená forma konania organizačne a ekonomicky nezaťažuje správny orgán natoľko ako riadne konanie. V riadnom konaní potom spravidla hrozia obvinenému vyššie sankcie. V tomto prípade sa neuplatňuje aplikácia zásaday *reformatio in peius* a to najmä pre skutočnosť, že sa nerealizuje odvolacie konanie ale konanie na prvom stupni.[713]

Blokové konanie je skrátenou formou priestupkového konania, ktorá umožňuje rýchle a menej formalizované vybavenie priestupku. Uplatní sa vtedy, ak je priestupok **spoľahlivo zistený** a obvinený je **ochotný pokutu zaplatiť**. Jeho podstatou je bezprostredné vybavenie veci bez plného dokazovania, bez osobitného predvolania na konanie a bez vydania klasického písomného rozhodnutia v štandardnej podobe. Výsledkom je individuálny správny akt vo forme **bloku**. Ak obvinený s blokovým konaním nesúhlasí, priestupok sa musí prejednať v riadnom konaní. Ak sa správny orgán rozhodne v riadnom konaní uložiť blokovú pokutu jeho postup je nezákonný, pretože túto skrátenú formu konania nie je možné kombinovať s riadnym konaním.[714]

V blokovom konaní možno uložiť najmä **pokutu**, prípadne priestupok vybaviť **napomenutím**, ak zákon nevylučuje takýto postup. Pre túto formu konania je typické, že po prijatí a zaplatení pokuty sa vec stáva právoplatne skončenou a nemožno proti nej podať odvolanie ani využiť mimoriadne opravné prostriedky. Blokové konanie sa neuplatní pri všetkých priestupkoch; vylúčené je najmä pri **návrhových priestupkoch** a tam, kde by bolo potrebné ukladať zákaz činnosti, prepadnutie veci alebo ochranné opatrenia. Ide teda o procesný nástroj určený najmä na vybavenie menej zložitých a spoľahlivo objasnených priestupkov. ZoKB nepripúšťa možnosť vybaviť vec v blokovom konaní.

Rozkazné konanie je druhou skrátenou formou priestupkového konania. Uplatňuje sa vtedy, ak je **nepochybné**, že sa obvinený priestupku dopustil, a vec nebola vybavená v blokovom konaní. Jeho zmyslom je rýchle a hospodárne rozhodnutie bez nariadenia ústneho pojednávania a bez vykonania plného dokazovania. Na rozdiel od blokového konania sa na jeho použitie **nevyžaduje súhlas obvineného**. Výsledkom je **rozkaz**, teda písomné rozhodnutie, ktoré má rovnaké náležitosti ako rozhodnutie o priestupku.

[713] Bližšie pozri: *Hamuľáková, Z.* Zákaz reformatio in peius v správnom konaní. 1. vydanie. Bratislava : Wolters Kluwer SR s. r. o., 2020, s. 16 a § 82 Správny poriadok.
[714] *Košičiarová, S.* Zákon o priestupkoch. Podrobný komentár s judikatúrou. Praha : Leges, 2020, s. 551 – 736.

Proti rozkazu môže obvinený podať do **15 dní odpor**. Včasným podaním odporu sa rozkaz ruší a správny orgán pokračuje v riadnom konaní. Následne v ďalšom konaní je správny orgán viazaný obsahom vydaného rozkazu.[715] Ak odpor podaný nie je, rozkaz nadobúda účinky **právoplatného rozhodnutia**. Rozkazné konanie nemožno použiť pri **návrhových priestupkoch** a ani voči osobe, ktorá je zbavená spôsobilosti na právne úkony alebo má túto spôsobilosť obmedzenú. V zmysle ZoKB je možné vybaviť vec rozkazom, ak bolo pri výkone dohľadu spoľahlivo zistené, že PZS porušil zákonom stanovenú povinnosť. Vo veci podania odporu a jeho účinkov sa úprava v ZoKB neodlišuje od všeobecnej úpravy.[716]

9.6.1.8 Výkon rozhodnutia o priestupku a sankcii za priestupok

Výkon rozhodnutia predstavuje štádium **po právoplatnom rozhodnutí**, v ktorom sa zabezpečuje splnenie povinnosti uloženej správnym orgánom. V ideálnom právnom štáte je dôvodné predpokladať **dobrovoľné plnenie** povinnosti a bezproblémová vymožiteľnosť práv. Avšak v skutočnosti dochádza aj k situáciám, kedy k dobrovoľnému plneniu nedochádza.[717] Ak teda **povinný subjekt nesplní uloženú povinnosť** dobrovoľne **nasleduje nútený výkon**. V správnom trestaní ide spravidla o vymoženie uloženej pokuty alebo o uskutočnenie iného zákonom predpokladaného spôsobu výkonu rozhodnutia. Jeho zmyslom nie je znova rozhodovať o vine, ale zabezpečiť praktickú realizáciu už uloženej povinnosti. Aj v tejto fáze musí správny orgán postupovať zákonne, primerane a len v medziach právom zverených spôsobov výkonu. PriesZ pritom dnes obsahuje len **osobitné formy výkonu rozhodnutia**, zatiaľ čo všeobecný procesný rámec výkonu zostáva viazaný na všeobecné správnoprocesné pravidlá. Ide o štandardné hmotnoprávne a procesnoprávne vymedzenie núteného výkonu vo verejnej správe či vymedzenie vymáhania peňažných a nepeňažných plnení.[718]

PriesZ výslovne pripúšťa najmä dve osobitné formy výkonu rozhodnutia. Prvou je **výkon rozhodnutia verejnoprospešnými prácami**, ktorý môže prísť do úvahy na návrh páchateľa, ak ide o pokutu prevyšujúcu 60 eur a nebola uložená v blokovom konaní; za každé 3 eurá pokuty sa vykoná jedna hodina verejnoprospešných prác a ich výkon musí byť ukončený najneskôr do jedného roka. Druhou je **výkon rozhodnutia zrážkami z dávky**

[715] *Vrabko, M.* § 87 Rozkazné konanie. In: *Srebalová, M. a kol.* Zákon o priestupkoch. 2. vydanie. Bratislava: C. H. Beck, 2020, s. 436.
[716] Bližšie pozri: § 29l ZoKB.
[717] *Vrabko, M. a kol.* Správne právo procesné. Všeobecná časť. 1. vydanie. Bratislava : C. H. Beck, 2013, s. 228.
[718] Bližšie pozri: § 71 – 80 Správny poriadok.

sociálneho poistenia, pomoci v hmotnej núdzi alebo z rodičovského príspevku, ktorý zákon viaže len na taxatívne určené priestupky a uplatní sa subsidiárne, ak rozhodnutie nemožno vykonať zrážkami zo mzdy.

9.6.2 Iné správne delikty

Iné správne delikty predstavujú v systéme správneho práva trestného tú časť administratívnoprávnej zodpovednosti, ktorá sa neuplatňuje v režime priestupkov, no napriek tomu ide o konanie postihované prostriedkami správneho práva trestného. Ide o širšiu a menej kodifikovanú kategóriu, ktorej spoločným znakom je, že jednotlivé skutkové podstaty nebývajú sústredené v jednom všeobecnom predpise, ale sú rozptýlené v osobitných zákonoch upravujúcich konkrétne úseky verejnej správy. Práve preto je pri ich výklade potrebné vychádzať nielen zo všeobecných princípov správneho trestania, ale aj zo systematiky osobitnej právnej úpravy, ktorá určuje okruh povinností, chránený objekt, model zodpovednosti aj osobitosti sankčného postihu.

Na účely tejto učebnice je táto problematika rozdelená do troch základných podkapitol. Prvú budú tvoriť **iné správne delikty fyzických osôb**, teda tie prípady, v ktorých zákon postihuje fyzickú osobu mimo priestupkového režimu. Druhú budú tvoriť **správne delikty právnických osôb a fyzických osôb – podnikateľov, ako aj fyzických osôb vykonávajúcich kvalifikované činnosti**. Tretia podkapitola je tvorená výkladom k **správnym disciplinárnym deliktom a správnym poriadkovým deliktom**. Takéto členenie zodpovedá nielen ich rozdielnemu subjektovému základu, ale aj odlišnej konštrukcii zodpovednosti. Kým pri fyzických osobách možno vo viacerých prípadoch stále uvažovať o blízkosti k priestupkovej zodpovednosti, pri právnických osobách a podnikajúcich fyzických osobách spravidla vystupuje do popredia objektívna zodpovednosť, viazaná najmä na porušenie zákonných povinností pri výkone podnikania, regulovanej alebo inej odborne kvalifikovanej činnosti. V prípade správnych poriadkových deliktov a správnych disciplinárnych deliktov ide o osobitné režimy sledujúce osobitné účely – najmä účel zabezpečenia priebehu správneho konania na strane správnych poriadkových deliktov a účel dodržiavania pracovnej a služobnej disciplíny vo forme dodržiavania interných predpisov v rámci konkrétnych subjektov s disciplinárnou právomocou na strane správnych disciplinárnych deliktov.

Z hľadiska regulácie **kybernetickej bezpečnosti** má toto delenie osobitný význam. Veľká časť právnych vzťahov v tejto oblasti totiž nesmeruje k všeobecnému okruhu subjektov,

ale k **špeciálne určeným adresátom právnych povinností**, akými sú najmä PZS povinné osoby, osoby vykonávajúce osobitne regulované alebo kvalifikované činnosti, členovia štatutárnych orgánov, ako aj podnikateľské subjekty pôsobiace v rámci regulovaného digitálneho prostredia. Práve z tohto dôvodu tvorí podstatnú časť administratívnoprávnej zodpovednosti v oblasti kybernetickej bezpečnosti nie priestupkový režim, ale režim **iných správnych deliktov**, ktorý zákonodarcovi umožňuje presnejšie reagovať na osobitosti regulovaného sektora, na vyššiu mieru profesionalizácie adresátov a na potrebu intenzívnejšej ochrany verejného záujmu. S vyššou mierou profesionalizácie sa priamo úmerne zvyšuje nárok na štandard dodržiavania regulácie a tým pádom sa sprísňuje aj forma postihu za správne delikty.

Cieľom tejto kapitoly preto nie je len pomenovať jednotlivé druhy týchto deliktov, ale predovšetkým ukázať ich miesto v systéme správneho práva trestného, ich vzťah k priestupkom a ich význam v tých oblastiach verejnej správy, v ktorých zákonodarca uprednostňuje osobitný režim pred všeobecným priestupkovým modelom.

9.6.2.1 Iné správne delikty fyzických osôb

Iné správne delikty fyzických osôb predstavujú osobitnú kategóriu správnych deliktov, ktorá stojí popri priestupkoch, správnych disciplinárnych deliktoch a správnych poriadkových deliktoch. Nejde o homogénny súbor, ale o rôznorodú skupinu deliktov upravených v osobitných zákonoch mimo priestupkového režimu. V odbornej literatúre sa spravidla vymedzujú ako **protiprávne konanie alebo opomenutie fyzickej osoby, ktorého znaky ustanovuje osobitný zákon a za ktoré správny orgán ukladá zákonom ustanovenú sankciu, ak nejde o trestný čin**.[719] Ich spoločným znakom teda je, že ide o verejnoprávny postih fyzickej osoby, ktorý zákonodarca z rôznych dôvodov nezaradil medzi priestupky.
Typickým znakom tejto kategórie je **roztrieštenosť a nejednotnosť právnej úpravy**. Osobitné zákony spravidla upravujú len skutkovú podstatu deliktu, sankciu, príslušnosť správneho orgánu a niekedy aj lehotu na vyvodenie zodpovednosti. Chýba však jednotná všeobecná hmotnoprávna aj procesnoprávna úprava, čo je dlhodobo predmetom odbornej kritiky. Z procesného hľadiska sa preto pri ich prejednávaní spravidla vychádza zo **Správneho poriadku**, nie z PriesZ. Zároveň sa vylučuje súbeh s priestupkom alebo trestným činom; ak je

[719] *Horvat, M.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 162.

určitý skutok kvalifikovaný ako iný správny delikt fyzickej osoby, nemožno ho za ten istý skutok súčasne postihnúť iným sankčným režimom.

Z hľadiska systematiky možno tieto delikty členiť najmä na **správne delikty zamestnancov, pracovníkov a funkcionárov** a na **zvyškové správne delikty fyzických osôb**.[720] V rozšírenom členení sa osobitne uvádzajú aj **správne delikty fyzických osôb – vlastníkov a držiteľov určitej veci**.[721] Pri deliktoch zamestnancov ide o delikty so **špeciálnym subjektom**, keďže ich nemôže spáchať akákoľvek fyzická osoba, ale len osoba v osobitnom postavení. Ich **objektom** býva najmä riadny chod verejnej správy a plnenie verejnoprávnych povinností. Zvyškové správne delikty fyzických osôb sú naopak širšou skupinou, pri ktorej zákonodarca vedome vyňal deliktný postih fyzickej osoby z priestupkového režimu, hoci nejde ani o disciplinárny, ani o poriadkový delikt. Práve preto ide o kategóriu, ktorá je z teoretického aj aplikačného vnímaná kontroverzne a to najmä preto, že je najmenej jednotná.

Kategórií iných správnych deliktov fyzických osôb sa najčastejšie vyčíta, že oproti priestupkom vytvárajú neodôvodnenú disparitu v právnom postavení fyzických osôb, a to tak v hmotnoprávnej, ako aj v procesnoprávnej rovine. Kým priestupkový režim poskytuje obvinenému výslovne formulované záruky, ako sú prezumpcia neviny, ústne konanie či osobitne upravené práva obvineného, pri iných správnych deliktoch fyzických osôb sa spravidla vychádza len zo všeobecného správneho konania, ktoré takúto úroveň ochrany výslovne a systematicky neobsahuje.[722] Pri vyvodzovaní administratívnoprávnej zodpovednosti v režime iných správnych deliktov fyzických osôb preto do procesu výrazne vstupuje aplikácia princípov správneho trestania, ktoré majú jednotiaci charakter a vo veľkej väčšine sú odvodené práve z konania o priestupkoch.

9.6.2.2 Iné správne delikty právnických osôb a podnikajúcich fyzických osôb, ako aj fyzických osôb vykonávajúcich kvalifikované činnosti

Správne delikty právnických osôb a podnikajúcich fyzických osôb, ako aj fyzických osôb vykonávajúcich kvalifikované činnosti, možno charakterizovať ako **protiprávne konanie právnickej osoby alebo fyzickej osoby oprávnenej na výkon určitej činnosti,**

[720] *Vrabko, M. a kol.* Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava : Ch. H. Beck, 2025, s. 241.
[721] *Horvat, M.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 163.
[722] *Prášková, H.* Základy odpovědnosti za správní delikty. 1. vydání. Praha : C. H. Beck, 2013, s. 157.

ktorého znaky sú ustanovené zákonom a za ktoré správny orgán ukladá zákonom ustanovenú sankciu ak nejde o trestný čin.[723] Už z tejto definície vyplýva, že ide o osobitnú skupinu iných správnych deliktov, ktorá sa v systéme administratívnoprávnej zodpovednosti odlišuje predovšetkým **subjektom deliktu**. Nejde o všeobecný subjekt, akým je pri priestupkoch fyzická osoba ako taká, ale o **špeciálny subjekt**, viazaný na podnikanie, výkon regulovanej činnosti alebo inú odborne kvalifikovanú činnosť. Sú veľmi typické pre ZoKB a čiastočne z hľadiska znaku výkonu kvalifikovanej činnosti aj pre ZoITVS, ktorý zaväzuje prevažne orgány verejnej správy pri špecifických činnostiach.

Práve špeciálny subjekt je ich určujúcim znakom. Zákonodarca spravidla upravuje zodpovednosť **právnických osôb** a **podnikajúcich fyzických osôb** spoločne, preto sa v teórii označujú aj ako **zmiešané správne delikty**.[724] V právnych predpisoch sa to prejavuje používaním pojmov ako podnikateľ, prevádzkovateľ, povinná osoba, orgán riadenia či iný obdobný subjekt, pod ktorý môžu patriť tak právnické osoby, ako aj fyzické osoby oprávnené na podnikanie alebo na výkon kvalifikovaných činností. V prípade právnickej osoby sa deliktuálna spôsobilosť viaže na jej vznik, teda spravidla na deň zápisu do príslušného registra. Pri podnikajúcej fyzickej osobe sa viaže na okamih nadobudnutia oprávnenia na podnikanie alebo výkon inej kvalifikovanej činnosti, typicky na zápis do živnostenského registra alebo vznik iného osobitného oprávnenia.

Od priestupkov sa tieto delikty zásadne odlišujú aj v **subjektívnej stránke**. Kým priestupok je vystavaný na zavinení, pri správnych deliktoch právnických osôb a podnikajúcich fyzických osôb sa spravidla uplatňuje **objektívna zodpovednosť**, teda zodpovednosť bez skúmania zavinenia, pričom pre absenciu liberačných dôvodov v právnych predpisoch hovoríme o **absolútnej objektívnej zodpovednosti.**[725] Rozhodujúce je, či bol porušený zákonom ustanovený režim a či vznikol protiprávny stav. Takto koncipovaný model zodpovedá tomu, že ide o subjekty pôsobiace v regulovanom priestore, od ktorých sa očakáva vyššia miera odbornosti, organizačnej pripravenosti a právnej disciplíny.

Tomuto predpokladu a nárokom zodpovedá aj **sankčný režim**, ktorý je spravidla prísnejší než pri priestupkoch. Pri týchto deliktoch sa ukladajú pokuty vo výrazne vyšších

[723] *Hamuľáková, Z.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 180.
[724] *Vrabko, M. a kol.* Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava : Ch. H. Beck, 2025, s. 243.
[725] *Hamuľáková, Z.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 184 – 185.

reláciách, a to práve preto, že ide o kvalifikované subjekty pôsobiace na regulovaných úsekoch, ktorých činnosť môže mať podstatný dopad na verejný záujem. V **kybernetickej bezpečnosti**, to platí dvojnásobne. Subjekty ako PZS, poskytovatelia digitálnych služieb alebo napríklad správca TLD či orgán riadenia môžu svojím zlyhaním zasiahnuť nielen jednotlivcov, ale aj fungovanie širších spoločenských a hospodárskych vzťahov. Aj preto zákonodarca pracuje s vyššími sankčnými pásmami, so stanovením hornej aj dolnej hranice pokuty a v ZoKB aj s mechanizmom viazania sankcie na **percento z celosvetového ročného obratu tzv. obratovú pokutu**. Práve tento prístup, posilnený aj európskou reguláciou vrátane smernice **NIS2**, ukazuje, že pokuty sa pri týchto deliktoch môžu pohybovať až v miliónových sumách, bez hornej hranice, aby subjekty pôsobiace v tomto priestore pristupovali k plneniu svojich povinností maximálne obozretne a s vedomím vysokej spoločenskej zodpovednosti.

Význam správneho v rámci tejto kategórie správnych deliktov spočíva predovšetkým v potrebe zabezpečiť **riadne plnenie zákonných povinností**, ktoré sa viažu na výkon podnikania či výkon kvalifikovaných činností a na pôsobenie v regulovaných odvetviach. Práve porušovanie týchto povinností, jeho frekvencia a často aj **závažné následky pre verejný záujem** odôvodňujú, aby zákonodarca vytváral osobitný režim administratívnoprávnej zodpovednosti právnických osôb a podnikajúcich fyzických osôb.[726]

Nejde teda len o represívnu reakciu na protiprávny stav, ale aj o nástroj preventívneho usmerňovania resp. riadenia správania subjektov, ktorých činnosť môže mať výrazný hospodársky a spoločenský dopad. Práve v tomto smere právna teória dlhodobo zdôrazňuje, že správne trestanie v rámci týchto správnych deliktov je nevyhnutnou súčasťou ochrany verejného záujmu v podmienkach modernej regulovanej spoločnosti.

9.6.2.3 Správne disciplinárne delikty a správne poriadkové delikty

V rámci systematiky teórie správnych deliktov nemožno zostať len pri priestupkoch a iných správnych deliktoch fyzických a právnických osôb. Úplnosť výkladu si vyžaduje aj stručné zachytenie tých deliktných režimov, ktoré sú síce užšie a funkčne špecifickejšie, no vnútorne dotvárajú štruktúru administratívnoprávnej zodpovednosti. Práve do tejto skupiny patria správne disciplinárne delikty a správne poriadkové delikty. Ich význam nespočíva v

[726] *Prášková, H.* Základy odpovědnosti za správní delikty. 1. vydání. Praha : C. H. Beck, 2013, s. 157 – 158.

šírke aplikačného záberu, ale v tom, že každý z nich chráni osobitný typ právneho poriadku: jeden vnútornú disciplínu a druhý riadny priebeh konania či výkon verejnej moci. Preto si obe kategórie vyžadujú aspoň základné samostatné vymedzenie.

I. **Správne disciplinárne delikty** predstavujú osobitný druh správnych deliktov, ktorý sa viaže na porušenie povinností vyplývajúcich z osobitného služobného, pracovného, členského alebo iného obdobného statusového vzťahu. Ich podstata spočíva v tom, že nejde o porušenie všeobecnej povinnosti voči štátu alebo spoločnosti, ale o porušenie povinnosti spojenej s príslušnosťou fyzickej osoby k určitej organizácii, inštitúcii alebo profesijnej štruktúre. Subjektom disciplinárneho deliktu je preto vždy **špeciálna fyzická osoba**, teda osoba, ktorá sa nachádza v osobitnom právnom postavení a ktorej povinnosti vyplývajú práve z tohto postavenia. Môže ísť napríklad o príslušníka ozbrojeného zboru, štátneho zamestnanca, člena profesijnej komory, študenta verejnej vysokej školy alebo osobu vo výkone trestu.[727]

   Z hľadiska **objektívnej stránky** môže byť disciplinárny delikt spáchaný **konaním, nekonaním aj opomenutím**, pričom spravidla ide o porušenie vnútorných pravidiel služby, výkonu funkcie, profesie alebo organizačného poriadku. Typickým znakom je, že o takomto delikte nerozhoduje všeobecný správny orgán v štandardnom režime správneho trestania, ale subjekt, ktorému právo priznáva **disciplinárnu právomoc**. Tá je založená na osobitnom splnomocnení a viaže sa na konkrétny organizačný alebo profesijný systém. Disciplinárna zodpovednosť je pritom spravidla vystavaná na **zavinení**, keďže jej zmyslom je reagovať na osobné zlyhanie člena určitej štruktúry pri plnení povinností, ktoré sa od neho vzhľadom na jeho status očakávajú.

   Na týchto znakoch je vystavaná aj definícia, v ktorej zmysle je správnym disciplinárnym deliktom **spravidla zavinené protiprávne konanie, prípadne opomenutie konania, fyzickej osoby, ktorá má kvalifikovaný vzťah k vykonávateľovi verejnej správy, pričom znaky takéhoto deliktu sú vymedzené v zákone alebo vo vnútornom predpise vydanom na základe zákona a za jeho spáchanie orgán vykonávateľa verejnej správy, ktorému bola zverená disciplinárna právomoc, ukladá disciplinárne sankcie, teda disciplinárne tresty alebo iné disciplinárne opatrenia.**[728] Sankcie môžu mať peňažnú aj

[727] *Vrabko, M. a kol.* Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava : Ch. H. Beck, 2025, s. 222.
[728] *Horvat, M.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 215.

nepeňažnú povahu, napríklad vo forme pokuty, zníženia osobného ohodnotenia, obmedzenia výkonu určitej činnosti, preradenia na inú pozíciu v rámci organizačnej štruktúry alebo iného disciplinárneho opatrenia.[729]

Účelom disciplinárnych deliktov je chrániť **riadny výkon služby, funkcie alebo povolania** a udržiavať vnútornú disciplínu v rámci relatívne uzavretých a stabilizovaných organizačných sústav. Práve preto majú disciplinárne sankcie osobitný charakter a bývajú prispôsobené vnútornému režimu danej inštitúcie. Správne disciplinárne delikty tak nepredstavujú len ďalšiu formu správneho trestania, ale aj osobitný nástroj vnútornej regulácie, ktorým sa zabezpečuje stabilita, funkčnosť a dôveryhodnosť organizovaných verejných a profesijných štruktúr. Vo vzťahu k priestupkom majú správne disciplinárne delikty špecifický význam pretože predstavujú jednu z výnimiek z prísneho chápania zásady *ne bis in idem.*[730] Z hľadiska kybernetickej bezpečnosti je potrebné venovať im osobitnú pozornosť a to nielen do vnútra verejnej správy, kde hovoríme o tomto štandardnom vyššie popísanom režime ale aj o inšpirácii týkajúcej sa mechanizmov vyvodzovania disciplinárnej zodpovednosti, v rámci súkromnoprávnych vzťahov, pri nastavovaní compliance režimu pre PZS.

II. **Správne poriadkové delikty** predstavujú kategóriu správnych deliktov s výrazne **procesnoprávnou povahou**. Ich právna úprava nie je sústredená v jednom všeobecnom predpise, ale je rozptýlená v množstve osobitných právnych predpisov na jednotlivých úsekoch verejnej správy. Z teoretického hľadiska ich možno vymedziť ako **protiprávne konanie alebo opomenutie konania osoby, ktoré ruší, sťažuje alebo marí postup orgánu verejnej správy, najmä počas správneho konania alebo pri výkone kontroly, a za ktoré správny orgán ukladá poriadkové sankcie, najmä poriadkové pokuty podľa osobitného právneho predpisu**. Ich zmyslom nie je primárne postihovať porušenie hmotnoprávnej povinnosti, ale chrániť **riadny, nerušený, účinný a účelný priebeh procesného postupu**.[731]

Objektom správnych poriadkových deliktov je ochrana priebehu a účelu správneho konania, dohľadu, kontroly alebo iného zákonom upraveného postupu. **Objektívna**

[729] Bližšie pozri: *Prášková, H.* Základy odpovědnosti za správní delikty. 1. vydání. Praha : C. H. Beck, 2013, s. 150.
[730] Bližšie pozri časť Princípy (zásady) správneho trestania a *Vrabko, M. a kol.* Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava : Ch. H. Beck, 2025. s. 225.
[731] *Horvat, M.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 246 - 247.

stránka spočíva v tom, že zodpovedný resp. povinný subjekt svojím konaním alebo nečinnosťou marí, sťažuje alebo narúša zákonný postup správneho orgánu. **Subjektom** môže byť spravidla **fyzická osoba**, no nie je vylúčené, aby sa takého deliktu dopustila aj **právnická osoba**, prípadne iný subjekt, ktorému zákon ukladá procesnú povinnosť. Z hľadiska **subjektívnej stránky** sa nevyžaduje zavinenie.[732] Aj pri správnych poriadkových deliktoch sa uplatňuje princíp ***nullum crimen sine lege***, a preto deliktuálne môže byť len také konanie, ktoré zákon výslovne predpokladá ako postihnuteľné.

Pri tejto kategórii treba odlišovať **poriadkovú pokutu** od **poriadkovej sankcie**.[733] Poriadková sankcia je pojem širší a okrem poriadkovej pokuty zahŕňa aj nepeňažnú podobu napr. vo forme vykázania z miesta konania úkonu.[734] Poriadková pokuta je pojem užší a predstavuje peňažnú sankciu. Poriadkovú pokutu môžeme identifikovať napr. aj v ZoKB, ktorý umožňuje uložiť poriadkovú pokutu subjektu, ktorý neposkytuje súčinnosť pri výkone dohľadu alebo marí výkon kontroly.[735] Aj v tejto oblasti teda správne poriadkové delikty plnia dôležitú funkciu: zabezpečujú, aby kontrolné a dohľadové mechanizmy verejnej správy neostali len formálne, ale aby boli aj reálne vykonateľné.

Obe uvedené kategórie ukazujú, že systém správnych deliktov nie je tvorený len všeobecnými deliktnými režimami, ale aj osobitnými formami zodpovednosti, ktoré reagujú na špecifické potreby verejnej správy. Kým správne disciplinárne delikty chránia vnútornú disciplínu a riadne fungovanie statusovo organizovaných štruktúr, správne poriadkové delikty chránia samotný proces výkonu verejnej moci a zabezpečujú jeho nerušený priebeh. Ich spoločným menovateľom je užšia funkčná viazanosť na konkrétny organizačný alebo procesný rámec. Ich význam nespočíva v rozsahu aplikácie, ale v tom, že dopĺňajú všeobecný systém administratívnoprávnej zodpovednosti tam, kde je potrebné chrániť osobitný režim služby, disciplíny alebo procesného poriadku.

[732] *Vrabko, M. a kol.* Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava : Ch. H. Beck, 2025. s. 240.
[733] *Horvat, M.* In. *Hamuľáková, Z., Horvat, M.* Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, s. 247.
[734] *Prášková, H.* Základy odpovědnosti za správní delikty. 1. vydání. Praha : C. H. Beck, 2013, s. 152.
[735] Bližšie pozri: § 29n ZoKB.

9.7 Administratívnoprávna zodpovednosť vykonávateľov verejnej správy

Zodpovednosť vykonávateľov verejnej správy predstavuje osobitný okruh právnej zodpovednosti, ktorý sa uplatňuje pri výkone verejnej správy, no nemožno ho stotožňovať s deliktuálnou administratívnoprávnou zodpovednosťou v užšom zmysle. V tejto oblasti vystupujú do popredia najmä dva základné druhy zodpovednosti, a to **disciplinárna zodpovednosť** a **zodpovednosť za škodu pri výkone verejnej moci**. Obe sú upravené osobitnými právnymi predpismi a ich spoločným menovateľom je, že sa viažu na vznik škody, resp. na porušenie povinností pri výkone verejnej správy, ktoré môže viesť k majetkovej alebo inej ujme. Všeobecne pritom platí, že vznik zodpovednosti za škodu predpokladá súčasné splnenie viacerých podmienok:

1. existenciu protiprávneho úkonu alebo škodovej udalosti,
2. vznik škody,
3. príčinnú súvislosť medzi konaním a škodou a
4. zavinenie.[736]

Vo vnútri verejnej správy sa tieto vzťahy prejavujú najmä ako zodpovednosť vo vzťahu k podriadeným subjektom, navonok ide spravidla o zodpovednosť voči spravovaným subjektom, teda napríklad účastníkom konania. Ak orgán verejnej správy alebo jeho zamestnanec poruší právnu povinnosť, vydá nezákonné rozhodnutie, nekoná včas alebo inak spôsobí ujmu, právny poriadok vytvára mechanizmy, prostredníctvom ktorých možno túto škodu nahradiť.

9.7.1 Zodpovednosť za škodu spôsobenú pri výkone verejnej moci

V kontexte náhrady škody spôsobenej spravovanému subjektu spravujúcim subjektom, je základným predpisom **zákon č. 514/2003 Z. z. o zodpovednosti za škodu spôsobenú pri výkone verejnej moci**. Zákon vychádza z princípu, že **štát nesie objektívnu zodpovednosť za škodu spôsobenú pri výkone verejnej moci**, ak táto škoda vznikla v dôsledku zákonom vymedzeného zásahu orgánu verejnej moci. Ide o prípady, keď bola škoda spôsobená:

1. **nezákonným rozhodnutím,**

[736] *Lazar, J. A kol.* Základy občianského hmotného práva. 2. zväzok. Bratislava : Iura Edition, 2000, s. 206. prevzané z: *Vrabko, M. a kol.* Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava : Ch. H. Beck, 2025, s. 253 - 254.

2. **nezákonným zatknutím, zadržaním alebo iným pozbavením osobnej slobody,**
3. **rozhodnutím o treste, ochrannom opatrení alebo väzbe, ako aj**
4. **nesprávnym úradným postupom.**

Podstatné pritom je, že tejto zodpovednosti sa štát nemôže zbaviť, pretože ide o zákonom ustanovený, vylúčením liberačných dôvodov posilnený režim, ktorého účelom je zabezpečiť ochranu osôb pred nezákonným alebo nesprávnym výkonom verejnej moci. Z uvedenej úpravy možno vyvodiť všeobecné pravidlo, že **vo veciach náhrady škody spôsobenej pri výkone verejnej moci koná v mene štátu ten orgán, do ktorého vecnej pôsobnosti patrí oblasť, v rámci ktorej škoda vznikla, alebo ten orgán, ktorého rozhodnutím či nesprávnym úradným postupom bola škoda spôsobená.** Ak osobitné pravidlá neumožňujú určiť príslušný orgán jednoznačne, zákon ustanovuje subsidiárne riešenie, podľa ktorého koná v mene štátu Ministerstvo spravodlivosti SR. Platí tu aj všeobecné pravidlo, že ak je nárok uplatnený na nepríslušnom orgáne, tento orgán je povinný žiadosť bezodkladne postúpiť príslušnému orgánu, pričom účinky uplatnenia nároku zostávajú zachované.

Tento mechanizmus je možné uplatniť aj na prípady, kedy vo veciach kybernetickej bezpečnosti rozhodujú príslušné spravujúce orgány.[737] Môže ísť napr. o prípad, kedy príslušný správny orgán rozhodne o blokovaní škodlivého obsahu[738] vo forme blokovania webu čím prevádzkovateľovi vznikne škoda vo forme výpadku príjmov za reklamu spojených s navštevovaním webu. Ak sa neskôr preukáže, že rozhodnutie bolo z nejakého dôvodu nezákonné môže sa osoba, ktorá prevádzkuje infraštruktúru domáhať náhrady škody, za ktorú je zodpovedný príslušný ústredný orgán štátnej správy.

9.7.2 Disciplinárna zodpovednosť

Druhá z foriem administratívnoprávnej zodpovednosti vykonávateľov verejnej správy je **disciplinárna zodpovednosť**, ktorá sa uplatňuje vo vzťahu k zamestnancom vykonávateľov verejnej správy. Ide o osobitný druh hmotnoprávnej zodpovednosti založený na porušení povinností vyplývajúcich zo služobného alebo pracovného vzťahu vo verejnej správe. V podmienkach štátnej správy je jej základ upravený najmä v **zákone č. 55/2017 Z. z. o štátnej**

[737] *Vrabko, M. a kol.* Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava : Ch. H. Beck, 2025, s. 253 - 254.
[738] Bližšie pozri: § 27b ZoKB.

službe a v **zákone č. 552/2003 Z. z. o výkone práce vo verejnom záujme**. Jej podstatou je, že zamestnanec verejnej správy zodpovedá za porušenie povinností pri výkone služby alebo práce vo verejnom záujme voči subjektu, ktorý je oprávnený túto zodpovednosť vyvodzovať, typicky voči **služobnému úradu**. Táto forma zodpovednosti tak plní nielen sankčnú, ale aj vnútornú organizačnú a stabilizačnú funkciu, keďže smeruje k zachovaniu riadneho, zákonného a profesionálneho výkonu verejnej správy. **Objektom** je v tomto prípade zabezpečenie riadneho výkonu verejnej správy spojeného s hospodárnosť jej činnosti v kontexte predchádzania vzniku škody. **Subjektom** administratívnoprávnej zodpovednosti vo verejnej správe je fyzická osoba v služobnom alebo štátnozamestnaneckom pomere. Ide teda o špeciálny subjekt. Vyvodzovanie disciplinárnej zodpovednosti môže byť realizované voči subjektom, ktoré porušia príslušné predpisy (napr. povinnosti vyplývajúce zo sektorových predpisov, disciplinárny poriadok alebo pracovný poriadok) alebo vedome nesplnia alebo porušia uloženú povinnosť.

V kontexte tejto učebnice ide napr. o situácie, kedy sú príslušné fyzické osoby **preškolené v súvislosti s nástrahami spojenými phishingom**, alebo s používaním osobných dátových nosičov, súkromných elektronických zariadení či súkromných e-mailov na vybavovanie pracovnej agendy a **služobný úrad im dá pokyn, aby sa takejto činnosti vyhli, prípadne ju hlásili** – jeho nesplnenie môže mať za následok iniciovanie disciplinárneho konania voči fyzickej osobe, ktorá stanovenú povinnosť nesplní. Ako je z príkladu zrejmé na prvý pohľad nemusí ísť o závažné disciplinárne previnenie. No v prípade, že by jeho následkom napr. skolabovali elektronické služby katastra nehnuteľností mohla by byť s týmto konaním zamestnanca spájaná obrovská škoda s celospoločenským dosahom, ktorá by zvyšovala mieru závažnosti skutku. V súvislosti s disciplinárnou zodpovednosťou zamestnancov verejnej správy preto rozlišujeme prípady, kedy dochádza k menej závažnému porušeniu disciplíny a k závažnému porušeniu disciplíny. V závislosti od závažnosti je potom posudzované aj vyvodzovanie osobnej zodpovednosti. Závažné porušenie disciplíny môže viesť aj k okamžitému skončeniu štátnozamestnaneckého alebo pracovného pomeru.

10. ADMINISTRATÍVNOPRÁVNA ZODPOVEDNOSŤ V KYBERNETICKEJ BEZPEČNOSTI - OSOBITNÁ ČASŤ

Osobitná časť nadväzuje na všeobecné teoretické východiská zo všeobecnej časti a premieňa ich na konkrétnu aplikačnú analýzu jednotlivých právnych predpisov tvoriacich právne jadro kybernetickej bezpečnosti. Jej metodologickým základom je postup, pri ktorom sa pri vybraných osobitných predpisoch skúma, aké formy administratívnoprávnej zodpovednosti upravuje, aké skutkové podstaty správnych deliktov obsahuje, aké sankčné mechanizmy pripúšťa, aké procesné osobitosti zavádza a či vytvára aj priestor pre zodpovednosť za škodu alebo iné osobitné následky porušenia právnych povinností. Výklad je vystavaný od konkrétneho právneho predpisu k jeho systematickému zaradeniu do všeobecného rámca správneho práva trestného. Cieľom tejto časti nie je len opis jednotlivých ustanovení, ale aj zvýraznenie toho, ako sa všeobecné princípy administratívnoprávnej zodpovednosti reálne uplatňujú v sektore kybernetickej bezpečnosti.[739]

10.1 Zákon o kybernetickej bezpečnosti

ZoKB v kontexte administratívnoprávnej zodpovednosti prešiel významnou revíziou spojenou s implementáciou Smernice NIS2. ZoKB obsahuje komplexný rámec vyvodzovania administratívnoprávnej zodpovednosti. Subjektom sú fyzické a právnické osoby, ktorým ZoKB priznáva špecifický rozsah povinností. Vo všeobecnosti preto môžeme konštatovať, že ide o špeciálne subjekty – právna úprava sa týka osôb, ktorých činnosť je týmto zákonom regulovaná. Okrem spravovaných subjektov upravuje ZoKB aj práva a povinnosti správnych orgánov, ktoré splnomocňuje na výkon verejnej moci. V celej šírke administratívnoprávnej zodpovednosti je preto možné vyvodzovať aj zodpovednosť za škodu spôsobenú výkonom verejnej moci.

Zodpovednostný rámec zákona je pritom vystavaný ako regulačný cyklus:

1. identifikácia regulovaného subjektu a jeho postavenia (najmä cez registračný režim),

[739] Informácia o využívaní nástrojov umelej inteligencie: Pri spracovaní tejto kapitoly bol použitý nástroj umelej inteligencie ChatGPT (GPT-5.4 Thinking) ako pomocný nástroj v rámci autorom riadeného pracovného postupu. Jeho použitie malo podporný charakter a uskutočňovalo sa na základe pokynov autora, jeho priebežnej spätnej väzby, kontroly a následnej autorskej úpravy. Za koncepciu kapitoly, jej štruktúru, metodologické východiská, výber zdrojov, odbornú argumentáciu, právne závery a výslednú podobu textu zodpovedá výlučne autor.

2. stanovenie a implementácia bezpečnostných opatrení (vrátane bezpečnostnej dokumentácie),
3. overovanie a kontrola účinnosti (audit alebo samohodnotenie),
4. incidentný režim (hlásenia a reakcie),
5. dohľadové nástroje (kontrola, vybavovanie sťažností) a
6. následne presadzovanie práva v dvoch rovinách:
   a. nápravnej (odstránenie nezákonného stavu) a
   b. represívnej (pokuty za delikty).

Táto postupnosť je metodicky dôležitá, pretože jednotlivé skutkové podstaty deliktov nadväzujú na konkrétne fázy tohto cyklu.

10.1.1 Postavenie zákona o kybernetickej bezpečnosti v systéme správneho práva trestného

V systéme správneho práva trestného ide o osobitnú právnu úpravu – *lex specialis*, na ktorú sa subsidiárne vzťahujú všeobecné predpisy. V kontexte priestupkovej časti ide o PriesZ, na ktorý sa zase vzťahuje Správny poriadok. Hovoríme preto o dvojitej subsidiarite. V spoločných ustanoveniach ZoKB vylučuje pôsobnosť Správneho poriadku v špecifických konaniach. Ten nevylučuje pri prejedávaní správnych deliktov a ukladaní poriadkových pokút. Na iné správne delikty sa preto bude vzťahovať Správny poriadok. Ako zo všeobecnej teórie vyplýva priama aplikácia PriesZ v prípade iných správnych deliktov neprichádza do úvahy. V mnohých princípoch správneho trestania však vyvodzovanie administratívnoprávnej zodpovednosti pri iných správnych deliktoch vychádza z princípov kodifikovaných PriesZ.
ZoKB nereguluje jeden homogénny okruh adresátov, ale viacero skupín s odlišnou intenzitou povinností. V jadre **stoja PZS**, pri ktorých ZoKB rozlišuje aj režim **kritickej základnej služby**. Na tento okruh nadväzuje **dodávateľská vrstva** (tretie strany s významným vplyvom), osobitná skupina poskytovateľov vybraných digitálnych služieb a infraštruktúr, osobitne upravená **doménová správa** (správca TLD a registrátori) a napokon **certifikačný ekosystém kybernetickej bezpečnosti** viazaný na právo EÚ.

Okrem hmotnoprávnych povinností obsahuje ZoKB aj osobitné dohľadové a sankčné mechanizmy. **Vylučuje pôsobnosť správneho poriadku v rozkazom konaní, pri kontrole a vybavovaní sťažností či pri schvaľovaní dohody o náprave.** Ale taktiež aj v špecifických konaniach spojených napr. so zápisom a výmazom z registra PZS čo má podstatný vplyv na

činnosť regulovaného subjektu. Zákon upravuje osobitné skutkové podstaty, osobitné subjekty zodpovednosti, osobitné sankčné rozpätia a zároveň osobitný dohľadový mechanizmus. Za dôležité považujeme zdôrazniť, že zodpovednostný režim je naviazaný na výkon dohľadu príslušným správnym orgánom.

Z didaktického hľadiska je potrebné odlíšiť **dve roviny presadzovania práva**. Prvou je **rovina dohľadovo-nápravná**, ktorá smeruje k zastaveniu porušovania a k odstráneniu nezákonného stavu (typicky prostredníctvom uloženia povinností, prípadne predbežných opatrení). Druhou je **rovina represívna**, v ktorej sa prejednávajú delikty a ukladá pokuta ako sankcia. Obe roviny sa v zákone prelínajú, no majú odlišnú funkciu: náprava obnovuje súlad *pro futuro*, sankcia reaguje na minulé porušenie povinnosti.

Výkon dohľadu zákon zveruje NBÚ a **spočíva**:

1. vo vybavovaní sťažností,
2. v kontrole,
3. v ukladaní opatrení na zastavenie porušovania povinností a nápravu nezákonného stavu (opatrenia na nápravu),
4. v schvaľovaní dohôd o náprave,
5. v prejednávaní správnych deliktov a
6. ukladaní poriadkových pokút a pokút.

Všeobecný objekt ochrany, na ktorý nadväzujú dohľadové aj sankčné mechanizmy ZoKB, možno učebnicovo zovšeobecniť najmä na:

1. dostupnosť, dôvernosť a integritu sietí a informačných systémov a súvisiacich služieb,
2. kontinuitu a odolnosť základných a kritických služieb,
3. schopnosť včasnej detekcie, hlásenia a riešenia incidentov,
4. riadenie rizík (vrátane rizík dodávateľského reťazca a technologických závislostí),
5. účinnosť dohľadu a kontrolnej činnosti orgánu verejnej moci (procesná disciplína, súčinnosť),
6. dôveryhodnosť a transparentnosť identifikačných a evidenčných mechanizmov (registre, doménové údaje, certifikácia).

ZoKB nereguluje jeden univerzálnym **subjekt** a tým pádom upravuje aj viac režimov vyvodzovania administratívnoprávnej zodpovednosti.

10.1.2 Sankcie a iné negatívne následky spojené s nedodržiavaním zákona o kybernetickej bezpečnosti

Za správne delikty (priestupky, iné správne delikty a správne poriadkové delikty) je možné uložiť v zmysle § 29n, § 30 a § 31 ZoKB **výlučne pokuty**. Ide o štandardne stanovené rozpätie sankcií so stanovením dolnej a hornej hranice:

- pri poriadkových pokutách je stanovená iba horná hranica na úrovni 1 500 eur a je možné ju ukladať opakovane do úhrnnej výšky 15 000 eur;
- pri priestupkoch je dolná hranica na úrovni 100 eur a horná hranica na úrovni 5 000 eur;
- pri správnych deliktoch je dolná hranica na úrovni 300 eur a horná hranica až 10 000 000 eur prípadne je horná hranica individualizovaná a určená percentom z výšky celosvetového obratu páchateľa, v závislosti od konkrétnej skutkovej podstaty.

ZoKB popri pokutách pracuje aj s donucovacími a nápravnými nástrojmi. **Pokuta** je sankcia ukladaná za správny delikt alebo priestupok. **Penále** má donucovací charakter viazaný na omeškanie so splnením uloženej povinnosti. **Opatrenia na nápravu** predstavujú zásah smerujúci k odstráneniu nezákonného stavu a k bezprostrednému zníženiu rizika; môžu byť ukladané samostatne, ale zákon zároveň pripúšťa ich kumuláciu s pokutou (ak je naplnená skutková podstata deliktu) a pri omeškaní aj s penále. Toto rozlíšenie je dôležité pre metodicky čisté posúdenie, či sa v konkrétnej veci sleduje primárne obnovenie súladu alebo represia. Pri penále a opatrení na nápravu z hľadiska účinkov na adresáta hovoríme o ich kvázisankčnom charaktere.

Ako uvádzame vyššie okrem dolnej a hornej hranice umožňuje zákon v prípade správnych deliktov ukladať aj pokuty do výšky 1,4 % resp. 2 % z celkového celosvetového obratu. Stanovenie **obratovej pokuty**, teda pokuty stanovenej v závislosti na výške celosvetového obratu ZoKB upravoval už vo svojej vyhlásenej podobe, ktorou zákonodarca reagoval na potrebu implementácie Smernice NIS. Pôvodná smernica však takýto imperatív neobsahovala. Ten sa objavuje až v Smernici NIS2. Trend ukladania obratových pokút sa v prevažnej miere spája s transpozíciou regulácie EÚ a je prítomný napr. v zákone o ochrane osobných údajov[740] alebo zákone o ochrane hospodárskej súťaže,[741] ktoré sú úzko naviazané

[740] § 104 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.
[741] § 42 – 45 zákona č. 187/2021 Z. z. o ochrane hospodárskej súťaže a o zmene a doplnení niektorých zákonov.

na európske právo. Rozdiel vo vyhlásenom znení zákona a súčasnom znení po transpozícii Smernice NIS2 spočíva v skutočnosti, že pôvodné znenie rámcovalo obratovú pokutu hornou hranicou do výšky 300 000 eur. Súčasné znenie ZoKB hornú hranicu neupravuje. Záverom tejto časti môžeme konštatovať, že slovenská legislatívna tvorba už v čase implementácie Smernice NIS zachytávala trendy obratovej pokuty, ktoré sa naplno prejavili až v Smernici NIS2.

Zvýšenie sankčných rozpätí a zavedenie obratovej logiky zároveň posilňuje požiadavku procesnej efektívnosti dohľadu. ZoKB preto popri ukladaní pokút v riadnom režime pracuje aj so skráteným mechanizmom **rozkazného konania** (§ 29l), ktorý umožňuje uložiť sankciu bez ďalšieho konania, ak bolo pri výkone dohľadu spoľahlivo zistené porušenie povinnosti v jednotlivom prípade. Rozkazom možno podľa povahy zisteného nedostatku uložiť pokutu (do 10 000 eur) a opatrenie na nápravu, a to samostatne alebo súbežne; pri trvajúcom nedostatku aj opakovane. PZS môže proti rozkazu podať **do 15 dní odôvodnený odpor**; jeho včasným podaním sa rozkaz zrušuje a NBÚ pokračuje v konaní o uložení opatrenia na nápravu bez viazanosti skutkovými zisteniami, právnou kvalifikáciou ani druhom a výškou sankcie z rozkazu. Ak odpor podaný nie je, rozkaz má účinky právoplatného rozhodnutia bez možnosti opravného prostriedku.[742]

Ustanovenie § 29n ZoKB predstavuje **konkrétnu sektorovú materializáciu všeobecnej teórie správnych poriadkových deliktov**. Jeho účelom nie je sankcionovať porušenie hmotnoprávnych povinností PZS, ale **chrániť riadny a účinný priebeh dohľadu ako procesného postupu verejnej správy.** Poriadková pokuta tu preto vystupuje ako osobitná poriadková sankcia s donucovacím a preventívnym účinkom, ktorá popri iných opatreniach zabezpečuje, **aby dohľad neostal formálny, ale bol v praxi aj reálne vykonateľný.** Skutková podstata má typickú procesnoprávnu štruktúru:

- **objektom** je nerušený výkon kontroly a autorita dohľadového mechanizmu;
- **objektívna stránka** spočíva v konaní alebo opomenutí kontrolovaného subjektu, ktorým sa znemožní alebo sťaží kontrola, prípadne sa marí jej výsledok alebo náprava zistených nedostatkov;
- **subjektom** je kontrolovaný subjekt v postavení adresáta procesných povinností pri dohľade (v prevažnej miere ide o PZS);

[742] Bližšie pozri všeobecnú časť podkapitolu Skrátené formy priestupkového konania.

- **subjektívna stránka** nie je konštruovaná ako rozhodujúci prvok, keďže ide o nástroj vynútenia procesnej disciplíny a zabezpečenia spolupráce pri výkone verejnej moci.

V kontexte širších zodpovednostných vzťahov vyplývajúcich zo ZoKB môže byť povinný subjekt postihnutý aj formou **výmazu z príslušného registra**[743] **V tomto prípade však nehovoríme o sankcii ako následku naplnenia znakov skutkovej podstaty správneho deliktu.** V zmysle zásady *nullum crimen sine lege* sú správne delikty opísané vo vyššie spomenutých ustanoveniach ZoKB. Výmaz z registra je preto možné vnímať ako administratívny postih odlišný od sankcie, keďže nejde o zákaz činnosti v pravom slova zmysle sankčného postihu ale jeho uskutočnením PZS stráca oprávnenie na prevádzkovanie. Takýto výmaz preto môže mať kvázisankčný charakter, keďže sa s ním môžu pre PZS spájať negatívne dôsledky. Ak sa teda správny orgán dozvie o nespĺňaní kritérií spojených zo zápisom do registra môže rozhodnúť, že daný PZS nebude ďalej v registri figurovať. **Z metodického hľadiska je vhodné tento následok zaradiť medzi administratívnoprávne následky viazané na status subjektu (strata postavenia v registri), nie medzi sankcie správneho trestania.** V aplikačnej praxi preto treba striktne odlišovať, či orgán rozhoduje o splnení podmienok statusu (registračný režim), alebo o vine a sankcii za delikt (deliktuálny režim).

Odklon od štandardného poňatia sankcií ako negatívneho dôsledku deliktuálneho konania možno identifikovať aj v možnosti **zákazu poskytovania služby**.[744] V tejto rovine však ide prednostne o **opatrenie na nápravu nezákonného stavu**, ktorého účelom nie je potrestať subjekt za delikt, ale bezprostredne znížiť úroveň rizika a zabrániť pokračovaniu stavu, ktorý je nezlučiteľný so zákonnými požiadavkami kybernetickej bezpečnosti. Zákaz poskytovania služby sa spája s negatívnym následkom pre poskytovateľa za neplnenie zákonnej povinnosti a mohlo by sa zdať, že ide de facto o sankciu. Opatrenie na nápravu však nemôžeme vnímať ako sankciu v pravom slova zmysle. Ide skôr o hybridný inštitút na pomedzí sankcie a opatrenia slúžiaceho na bezprostredné zvrátenie neželaného stavu. Hybridná povaha tohto nástroja spočíva v tom, že síce vyvoláva citeľný negatívny následok pre regulovaný subjekt, no pôsobí **pro futuro** a je viazaný na **možnosť obnovy súladu**: odstránením zistených nedostatkov sa subjekt môže vrátiť do režimu riadneho poskytovania služby. V právnej teórii hovoríme aj v tomto prípade o tzv. kvázisankčnom charaktere. Zákaz

[743] Bližšie pozri: § 17 ods. 7 ZoKB.
[744] Bližšie pozri: § 29j ods. 1 písm. d) ZoKB.

tak vo svojej podstate vytvára donucovací rámec na dosiahnutie nápravy, nie definitívny trest za minulé porušenie. Je nevyhnutné režim opatrenia na nápravu striktne oddeliť od režimu vyvodzovania zodpovednosti za správny delikt.

Zákonodarca tento konštrukt potvrdzuje tým, že konanie o uložení opatrenia na nápravu stavia na dohľadovej logike: správny orgán ukladá PZS taxatívne vymenované povinnosti podľa závažnosti, rozsahu, dĺžky trvania, následkov a povahy zistených nedostatkov; môže uložiť aj povinnosť vykonať audit a realizovať odporúčania, prijať opatrenia na nápravu, informovať dotknuté osoby alebo verejnosť o rizikách či následkoch porušenia povinnosti, a v krajnom prípade **zakázať poskytovanie základnej služby** do času odstránenia nezákonného stavu, pričom tento **zákaz nie je prípustný pri určitých kategóriách PZS – orgánoch verejnej moci.**[745] V uvažovaní o opatrení na nápravu ako o sankcii v pravom slova zmysle potom táto skutočnosť **oslabuje princíp materiálnej rovnosti**, keďže sa za také isté konanie v rozpore so zákonom pripúšťajú dva režimy s negatívnym dôsledkom pre adresáta. Priaznivejším pre orgán verejnej moci a menej priaznivým pre subjekt, ktorý nie je orgánom verejnej moci. Správny orgán má okrem možnosti uložiť zákaz prevádzkovania služby aj možnosť uložiť opatrenie **zákazu výkonu funkcie štatutárnemu orgánu.**[746]

Zároveň ZoKB výslovne pripúšťa, aby správny orgán popri nápravnom opatrení uložil aj **pokutu za správny delikt** a v prípade omeškania aj **penále**.[747] V čase uloženia zákazu poskytovania služby sa teda právna situácia typicky viaže na existenciu protiprávneho stavu a potrebu jeho odstránenia; **subjekt ešte nie je páchateľom** deliktu v zmysle právoplatného rozhodnutia o vine a uložení sankcie. Deliktuálna rovina sa uzatvára až rozhodnutím o vine a sankcii za správny delikt, ktoré má represívny charakter a nadväzuje na preukázanie naplnenia skutkovej podstaty opísanej v príslušných ustanoveniach ZoKB.

[745] Bližšie pozri: Národná rada Slovenskej republiky (2023 – doposiaľ), parlamentná tlač 508 – Vládny návrh zákona, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony, Dôvodová správa B. Osobitná časť Čl. I. k bodu 75.
[746] § 29j ods. 4 ZoKB.
[747] Bližšie pozri: § 29j ods. 2 a 3 ZoKB.

10.1.3 Priestupky [§ 30]

Ustanovenie § 30 ZoKB vytvára osobitnú, sektorovú úpravu priestupkov ako jednej z foriem administratívnoprávnej zodpovednosti fyzických osôb. V prvom odseku taxatívne vymedzuje šesť skutkových podstát, ktoré sú viazané na porušenie kľúčových povinností v režime kybernetickej bezpečnosti (mlčanlivosť, oznamovanie, plnenie povinností PZS, dodržiavanie interných bezpečnostných opatrení, kvalifikovaný výkon auditu a zákonný režim samohodnotenia).

Metodologicky je táto časť vystavaná od skutku k znakom skutkovej podstaty. Pri každom konaní, ktoré ZoKB označuje za priestupok, najprv stručne priblížime podstatu porušenej povinnosti (t. j. čo zákon chráni a prečo je dané konanie deliktuálne významné v kontexte kybernetickej bezpečnosti). Následne, v prehľadovej štruktúre, uvedieme základné znaky skutkovej podstaty (objekt – subjekt – objektívna stránka – subjektívna stránka), aby čitateľ získal mapu toho, čo je potrebné v aplikačnej praxi posudzovať. Výklad má čiastočne komentárový charakter: čitateľa prevádza jednotlivými priestupkami tak, že na konkrétnom ustanovení demonštruje praktický význam znakov skutkovej podstaty, ich vzájomnú nadväznosť a typické výkladové akcenty (najmä pri blanketových alebo technicky determinovaných povinnostiach). Cieľom nie je nahradiť komentár k ZoKB, ale učebnicovo zviditeľniť deliktuálnu dimenziu jednotlivých povinností: ako sa preklápajú do režimu priestupkovej zodpovednosti, ktoré prvky sú rozhodujúce pre naplnenie skutkovej podstaty a ktoré sa premietajú najmä do úvahy o závažnosti a sankcii.

10.1.3.1 Porušenie povinnosti mlčanlivosti [§ 30 ods. 1 písm. a)]

V prípade tohto priestupku ide o porušenie zákonnej povinnosti mlčanlivosti pri plnení úloh podľa ZoKB alebo v súvislosti s ním. Ustanovením tejto skutkovej podstaty priestupku sa chráni dôvernosť režimových informácií a bezpečnostné záujmy, ktoré by mohli byť ich sprístupnením ohrozené. Na účely ZoKB sú chránené také skutočnosti, ktoré sa osoba dozvedela pri plnení úloh podľa ZoKB alebo v súvislosti s ním a nie sú verejne známe. Povinnosť mlčanlivosti trvá aj po skončení dohody o spolupráci, pracovnoprávneho (alebo obdobného) vzťahu a služobného pomeru.

Subjektom je špeciálna fyzická osoba, ktorá *plní alebo plnila úlohy* podľa ZoKB alebo v súvislosti s ním. Nejde o všeobecný subjekt typu *ktokoľvek*. **Objekt** predstavuje ochranu dôverných informácií a dôveryhodného výkonu úloh v sektore kybernetickej bezpečnosti.

Sekundárne aj ochrana bezpečnej prevádzky služieb a zníženie rizík spojených s únikom informácií. **Objektívna stránka**: konanie spočíva v porušení mlčanlivosti typicky tým, že subjekt vyzradí alebo oznámi neverejnú skutočnosť neoprávnenej osobe sprístupní ju mimo oprávneného okruhu (napr. publikovaním, zaslaním nesprávnemu adresátovi); umožní únik nedodržaním primeraných organizačných alebo technických opatrení. Z hľadiska následku je skutková podstata vystavaná primárne na porušení povinnosti. Skutočné ohrozenie či škoda budú spravidla významné pri posudzovaní závažnosti a pri úvahe o výmere sankcie. Keďže skutková podstata nevyžaduje výslovne úmysel z hľadiska **subjektívnej stránky** je priestupok možné spáchať aj z nedbanlivosti. V praxi pôjde často o nedbanlivostné nakladanie s informáciami.

Povinnosť mlčanlivosti podľa ZoKB sa uplatní popri mlčanlivostiach a tajomstvách podľa iných právnych predpisov; porušenie môže preto vyvolať aj ďalšie právne následky mimo priestupkového režimu ZoKB. V kontexte s týmto priestupkom môže byť voči páchateľovi priestupku vyvodzovaná aj disciplinárna zodpovednosť.[748]

10.1.3.2 Poskytnutie nepravdivých údajov v oznamovacej povinnosti [§ 30 ods. 1 písm. b)]

Podstata tohto priestupku spočíva v tom, že osoba, ktorej vznikla oznamovacia povinnosť podľa § 17 ods. 2 ZoKB, uvedie v oznámení **nepravdivé údaje**. Zmyslom oznamovania je umožniť NBÚ identifikovať a evidovať subjekty, ktoré vykonávajú činnosti alebo poskytujú služby s významom pre kybernetickú bezpečnosť. Najmä z dôvodu aby bolo možné voči nim uplatňovať zákonom predpokladané povinnosti dohľadu, koordinácie a riadenia rizík. Ustanovenie preto chráni predovšetkým **pravdivosť, úplnosť a spoľahlivosť údajov**, ktoré sú podkladom pre vedenie registra PZS a pre následné výkonové kompetencie NBÚ.

Subjektom je **špeciálna fyzická osoba**, ktorá *vykonáva činnosť* podľa § 17 ods. 1 ZoKB a tým jej vzniká povinnosť oznámiť túto skutočnosť NBÚ. Špeciálnosť subjektu sa prejavuje tým, že nejde o *kohokoľvek*, ale o osobu, ktorá fakticky vstúpila do regulovaného režimu (napr. vykonávaním činnosti v relevantnom sektore alebo poskytovaním určitej služby).

[748] Bližšie pozri kapitolu vo všeobecnej časti Správne disciplinárne delikty a správne poriadkové delikty v časti správne disciplinárne delikty a kapitolu Administratívnoprávna zodpovednosť vykonávateľov verejnej správy v časti disciplinárnej zodpovednosti.

Objektom je ochrana **riadneho výkonu verejnej správy v kybernetickej bezpečnosti,** najmä vedenia vecne správnej evidencie a schopnosti orgánu verejnej moci adresne komunikovať so subjektmi, ukladať im povinnosti a vykonávať dohľad. Sekundárne sa chráni aj **bezpečná kontinuita služieb**, keďže nesprávne identifikovaný subjekt môže zostať mimo potrebných opatrení. **Objektívna stránka** spočíva v **poskytnutí nepravdivých údajov** v oznámení (napr. nepravdivý názov alebo sídlo, fiktívne či neaktuálne kontakty, nesprávne údaje o zástupcovi, prípadne nepravdivý údaj o rozsahu pôsobenia v členských štátoch). Následok je typicky viazaný na **narušenie správnosti evidencie** a na sťaženie alebo znemožnenie dohľadu a komunikácie NBÚ; konkrétne ohrozenie kybernetickej bezpečnosti sa bude spravidla posudzovať na základe kritéria **závažnosti** a čo bude predstavovať aj významné kritérium pri úvahe o sankcii. Keďže skutková podstata nevyžaduje úmysel, z hľadiska **subjektívnej stránky** je priestupok možné spáchať aj **z nedbanlivosti,** napríklad uvedením nepresných údajov bez primeraného overenia alebo neaktualizovaním údajov, ktoré oznamovateľ považoval za formálne. Z hľadiska preventívneho pôsobenia sankcie sa na subjekt vytvára tlak, aby pri uvádzaní údajov postupoval s najvyššou mierou obozretnosti a precíznosti.

10.1.3.3 Porušenie povinností PZS [§ 30 ods. 1 písm. c)]

Táto skutková podstata je typickým **blanketovým priestupkom**: neformuluje vlastné zakázané konanie, ale odkazuje na porušenie konkrétnych povinností PZS podľa § 19 ods. 1 až 4, 6 a 7 ZoKB. Objekt je preto definovaný spojením týchto dvoch ustanovení. Ide o praktickú formu, ktorá umožňuje v legislatívnom procese odkázať na konkrétnu povinnosť bez potreby formulovania skutkovej podstaty. Zmyslom týchto ustanovení je donútiť PZS plniť jadrové povinnosti kybernetickej bezpečnosti – od nastavenia bezpečnostných opatrení, cez riadenie rizík a dodávateľských vzťahov, až po incident management a notifikačné povinnosti. V praxi preto vždy treba presne pomenovať, **ktorá povinnosť z § 19 bola porušená,** v akom rozsahu a v akom čase.

Subjektom je **špeciálna fyzická osoba** v postavení PZS. **Objektom** je ochrana **kybernetickej bezpečnosti a odolnosti** základných služieb a zároveň ochrana verejného záujmu na tom, aby PZS v regulovanom režime dodržiavali štandardy minimalizácie rizík. **Objektívna stránka** sa napĺňa už samotným **porušením povinnosti**. Pôjde najmä o situácie, keď PZS neprijme alebo nevykonáva všeobecné (a prípadne sektorové) bezpečnostné opatrenia v požadovanom rozsahu a lehote (§ 19 ods. 1 ZoKB),

nezabezpečí zmluvný režim a kontrolovateľnosť bezpečnostných opatrení pri využití tretej strany (§ 19 ods. 2 až 4 ZoKB), nezvládne kľúčové povinnosti pri incidente a spolupráci s NBÚ (riešenie incidentu, hlásenie závažného incidentu, súčinnosť, zabezpečenie dôkazov, oznamovanie OČTK, analýza závislostí, mechanizmus včasného informovania vedenia a pod. – § 19 ods. 6), alebo nesplní oznamovacie povinnosti a hlásenie zmien údajov (§ 19 ods. 7 ZoKB). **Subjektívna stránka** pri priestupkoch spravidla vyžaduje **zavinenie**, pričom pri tejto skutkovej podstate bude v praxi typické **nedbanlivostné** porušenie povinností (najmä zlyhanie procesov, kontroly dodávateľa, oneskorené hlásenia či neadekvátne opatrenia). **Pri kvalifikácii a odôvodnení rozhodnutia má správny orgán osobitne dbať na zásady zákonnosti, proporcionality a materiálnej pravdy, lebo ide o široko formulovaný delikt viazaný na viacero heterogénnych povinností.**

10.1.3.4 Postup v rozpore s opatreniami prijatými PZS [§ 30 ods. 1 písm. d]

Skutková podstata podľa tohto ustanovenia postihuje fyzickú osobu, ktorá *nepostupovala v súlade s technickými, organizačnými alebo personálnymi opatreniami prijatými PZS*. Ide o priestupok, ktorým zákonodarca sleduje, aby sa bezpečnostné pravidlá nevyčerpali len formálnym prijatím, ale boli reálne dodržiavané v každodennej prevádzke a tým znižovali úroveň rizika pre poskytovanú službu.

Objektom je ochrana kybernetickej bezpečnosti a odolnosti základnej služby, teda ochrana záujmov spojených s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov. Tieto záujmy sa v systéme zákona konkretizujú najmä prostredníctvom *bezpečnostných oprávnení* podľa § 20 ods. 1 ZoKB, ktoré zahŕňajú úlohy, procesy, role a technológie v organizačnej, personálnej, fyzickej a technologickej oblasti. Opatrenia sa prijímajú na základe analýzy rizík a smerujú k prevencii, detekcii, reakcii a obnove po incidente (§ 20 ods. 1 písm. a) až e) ZoKB). **Subjektom** je špeciálna fyzická osoba, ktorej sa opatrenia PZS reálne týkajú (typicky zamestnanec, štatutárny orgán, člen štatutárneho orgánu alebo iná osoba poverená výkonom činností súvisiacich s prevádzkou základnej služby). Nejde o kohokoľvek, ale o osobu viazanú vnútorným režimom bezpečnostných pravidiel PZS. **Objektívna stránka** spočíva v porušení povinnosti postupovať podľa prijatých opatrení, či už konaním alebo opomenutím. V praxi pôjde najmä o nerešpektovanie:

1. technických pravidiel (napr. prístupové režimy, autentifikácia, kryptografické zásady),
2. organizačných postupov (napr. postupy pri incidentoch, hlásenie udalostí, interné eskalácie) alebo
3. personálnych opatrení (napr. povinné školenia, dodržiavanie pridelených rolí a zodpovedností).

Následok nie je vždy rozhodujúci pre samotné naplnenie skutkovej podstaty, avšak reálne ohrozenie či porušenie chráneného záujmu bude typicky významné pri úvahe o závažnosti a výmere sankcie. Pri konkrétnych prípadoch sa posudzuje aj kauzálny nexus medzi porušením opatrení a vznikom incidentu alebo zvýšením rizika. Keďže skutková podstata neviaže zodpovednosť na úmysel, priestupok možno z hľadiska **subjektívnej stránky** spáchať aj z nedbanlivosti; typické sú situácie, keď osoba podcení režim opatrení, nevykoná povinný úkon alebo nedodrží postup, hoci vzhľadom na okolnosti a svoje pomery mala a mohla predvídať riziká.[749]

10.1.3.5 Audit vykonaný necertifikovaným audítorom kybernetickej bezpečnosti [§ 30 ods. 1 písm. e)]

Priestupok je viazaný na výkon auditu kybernetickej bezpečnosti v rozpore s § 29 ods. 3 ZoKB. Zmyslom tejto skutkovej podstaty je chrániť dôveryhodnosť auditu ako kľúčového kontrolného nástroja, ktorý overuje plnenie povinností podľa ZoKB, posudzuje zhodu prijatých bezpečnostných opatrení a identifikuje nedostatky s cieľom navrhnúť nápravu a predchádzať incidentom (§ 29 ods. 1 ZoKB). Audit pritom nie je administratívna formalita, ale mechanizmus, od ktorého sa odvíja schopnosť PZS udržať požadovanú úroveň kybernetickej bezpečnosti a odolnosti.

Objektom priestupku je verejný záujem na riadne zabezpečenej kybernetickej bezpečnosti prostredníctvom kvalifikovaného a nezávislého overenia plnenia povinností. Sekundárne sa chráni aj dôvera orgánu dohľadu a dotknutých subjektov v to, že závery auditu sú odborné, verifikovateľné a porovnateľné v rámci jednotného rámca. **Subjektom** je špeciálna fyzická osoba **v postavení audítora kybernetickej bezpečnosti**. Ustanovenie § 29

[749] *Chlipala, M., Makatura, I., Pilár, Š.* Zákon o kybernetickej bezpečnosti Komentár. Prvé vydanie. Žilina : Eurokódex s. r. o. 2019, s. 286.

ods. 3 ZoKB výslovne viaže výkon auditu na *certifikovaného audítora kybernetickej bezpečnosti.* Priestupok neznie proti PZS ale proti osobe vykonávajúcej audit, ktorá má postavenie certifikovaného audítora (či už ako fyzická osoba samostatne, alebo ako spoločník/štatutár/zamestnanec právnickej osoby zabezpečujúcej audit). **Objektívna stránka** spočíva vo vykonaní auditu *v rozpore* s § 29 ods. 3 ZoKB, typicky tým, že audit vykoná osoba bez platnej certifikácie, mimo rámca certifikačných podmienok, prípadne tak, že audit fakticky vykonáva necertifikovaná osoba a certifikovaný audítor vystupuje len formálne. Následok nie je konštrukčným znakom skutkovej podstaty; podstatné je porušenie kvalifikačnej garancie auditu. Praktické dôsledky (napr. neodhalené nedostatky, falošný pocit súladu, neskorší incident) budú typicky významné pri hodnotení závažnosti konania a pri ukladaní sankcie. **Subjektívna stránka** nie je v texte skutkovej podstaty viazaná na úmysel. V priestupkovom režime preto spravidla postačí nedbanlivosť, napríklad ak audítor nekontroluje platnosť alebo rozsah certifikácie, podcení režim certifikácie, prípadne sa spolieha na formálne zastúpenie certifikovanou osobou bez reálneho výkonu auditu. Úmyselné obídenie certifikačného režimu bude zvyšovať závažnosť a môže byť relevantné aj pre iné právne následky (napr. profesijné, zmluvné alebo dokonca až trestnoprávne v rovine spáchania trestného činu neoprávneného podnikania).

Z hľadiska systematiky zákona ide o priestupok, ktorý posilňuje kvalitatívny štandard kontrolných mechanizmov: ak audit má slúžiť na nápravu existujúceho stavu a prevenciu incidentov, musí byť vykonaný osobou, ktorej odborná spôsobilosť je preukázaná predpokladanou certifikáciou upravenou v ZoKB.

10.1.3.6 Samohodnotenie v rozpore so zákonným režimom [§ 30 ods. 1 písm. f)]

Priestupok podľa § 30 ods. 1 písm. f) ZoKB postihuje situáciu, keď fyzická osoba vykoná samohodnotenie prostredníctvom jednotného informačného systému kybernetickej bezpečnosti v rozpore s § 29 ods. 8 ZoKB. Zmyslom tohto ustanovenia je umožniť **PZS, ktorý nie je prevádzkovateľom kritickej základnej služby**, nahradiť audit samohodnotením, avšak len v presne určenom režime podľa ZoKB a príslušných normatívnych správnych aktoch vydaných NBÚ. Pri posúdení tejto skutkovej podstaty je potrebné **odlíšiť inštitút samohodnotenia**, ktorý sa vykonáva prostredníctvom manažéra kybernetickej bezpečnosti **od inštitútu auditu**, ktorý sa vykonáva prostredníctvom certifikovaného audítora kybernetickej bezpečnosti.

Objektom je ochrana spoľahlivosti a zákonnosti kontrolného mechanizmu, t. j. aby preverovanie účinnosti bezpečnostných opatrení nebolo len formálne, ale realizované spôsobom, ktorý ZoKB považuje za dôveryhodný na základe stanovených štandardov (osoba hodnotiteľa, vykonanie prvého samohodnotenia, periodicita samohodnotenia). **Subjektom** je špeciálna fyzická osoba – **PZS, ktorý nie je prevádzkovateľom kritickej základnej služby**, preto skutková podstata cieli na konkrétny povinný subjekt. **Objektívna stránka** spočíva v samotnom vykonaní samohodnotenia mimo zákonných podmienok (napr. vykoná ho iná osoba než manažér kybernetickej bezpečnosti, vykoná sa mimo stanovenej periodicity, alebo sa použije v čase, keď sa má vykonať audit). Následok sa typicky nevyžaduje; rozhodujúce je porušenie zákonného postupu, pričom reálne dopady budú relevantné pri úvahe o závažnosti a sankcii. Z hľadiska **subjektívnej stránky** skutková podstata nevyžaduje úmysel, priestupok možno spáchať aj z nedbanlivosti (napr. opomenutie vykonania samohodnotenia prostredníctvom manažéra kybernetickej bezpečnosti, alebo vykonanie samohodnotenia mimo rámca stanovenej periodicity).

10.1.4 Iné správne delikty [§ 31]

Ustanovenie § 31 ZoKB obsahuje osobitnú, sektorovú úpravu iných správnych deliktov. Tie predstavujú ústrednú formu administratívnoprávnej zodpovednosti viazanej predovšetkým na právnické osoby, podnikateľské subjekty ale aj vykonávateľov verejnej správy pôsobiacich v regulovaných segmentoch kybernetickej bezpečnosti. Na rozdiel od § 30 ZoKB, ktorý cieli na fyzické osoby v režime priestupkov, § 31 ZoKB rozčleňuje administratívnoprávnu zodpovednosť podľa typu adresáta a intenzity porušenej povinnosti. Z hľadiska subjektu tak zákon pracuje s viacerými režimami:

1. PZS (§ 31 ods. 1 a 2 ZoKB),
2. prevádzkovateľ kritickej základnej služby ako kvalifikovaný prípad s prísnejšou sankciou (§ 31 ods. 3 ZoKB),
3. osoby poskytujúce vybrané digitálne služby alebo vykonávajúce činnosti podľa § 2 ods. 2 ZoKB (§ 31 ods. 4 a 5 ZoKB),
4. správca TLD a registrátor domén (§ 31 ods. 6 ZoKB),
5. širší okruh zaväzujúci orgány verejnej moci, PZS, právnické osoby podľa príloh pri vybraných dohľadových a bezpečnostných povinnostiach (§ 31 ods. 7 ZoKB) a

6. subjekty certifikačného rámca podľa Aktu o kybernetickej bezpečnosti (§ 31 ods. 8 až 11 ZoKB).

Sankčný mechanizmus je diferencovaný podľa závažnosti a systémového významu povinnosti: pri základných deliktoch prevádzkovateľov ide o pevné rozpätie pokuty (§ 31 ods. 1 ZoKB), pri deliktoch s jadrovým dopadom na bezpečnostnú odolnosť a manažment incidentov sa uplatňuje vyšší strop a alternatívne aj obratová pokuta (§ 31 ods. 2 ZoKB), pričom pri kritických základných službách zákon zvyšuje hornú hranicu aj percento obratu (§ 31 ods. 3 ZoKB). Vo vzťahu k ostatným subjektom (§ 31 ods. 4 až 11 ZoKB) zákon stanovuje samostatné rozpätia zodpovedajúce ich funkcii v ekosystéme (cezhraničné väzby, doménová infraštruktúra, súčinnosť pri dohľade, certifikačná disciplína). Spoločnou rámcovou korekciou je požiadavka individualizácie sankcie podľa závažnosti, spôsobu spáchania, trvania a následkov (§ 31 ods. 12 ZoKB), možnosť upustiť od pokuty pri nepatrnom následku, recidívne zvýšenie sankcie (§ 31 ods. 13 ZoKB), premlčacie lehoty (§ 31 ods. 17 ZoKB) a pravidlá určovania obratu (§ 31 ods. 15 až 16 ZoKB).

Všeobecný objekt ochrany pri § 31 možno didakticky zovšeobecniť najmä takto:

1. ochrana kybernetickej bezpečnosti a odolnosti základných a kritických základných služieb,
2. ochrana funkčného dohľadu a vynútiteľnosti povinností (vrátane súčinnosti a presadzovania rozhodnutí NBÚ),
3. ochrana spoľahlivosti kontrolných mechanizmov (audit, samohodnotenie, nápravné opatrenia),
4. ochrana včasnej detekcie a koordinácie reakcie na incidenty (hlásenia, automatizované poskytovanie informácií, reaktívne/ochranné opatrenia),
5. ochrana transparentnosti a dohľadateľnosti doménovej infraštruktúry,
6. ochrana dôveryhodnosti európskeho certifikačného rámca a súvisiacich informačných povinností.

Metodologicky je táto časť vystavaná rovnako ako časť týkajúca sa priestupkov – od skutku k znakom skutkovej podstaty, avšak s dôrazom na štruktúru adresátov a na sankčné vetvenie v rámci § 31. Pri každej skutkovej podstate najprv stručne definujeme, akú povinnosť zákon chráni a kde je jej miesto v dohľadovom a compliance režime (evidencia a oznamovanie, bezpečnostná dokumentácia a opatrenia, audit a náprava, incident reporting, zásahy NBÚ v čase incidentu, doménová transparentnosť, súčinnosť, certifikačná disciplína).

Následne uvedieme znaky skutkovej podstaty (objekt – subjekt – objektívna stránka – subjektívna stránka) s osobitným akcentom na to, že pri väčšine deliktov § 31 zákon neviaže zodpovednosť na úmysel, a preto sa v aplikačnej praxi presadzuje objektivizovaný prístup, pričom miera zavinenia má typicky význam najmä pri individualizácii výšky pokuty.

10.1.4.1 Nesplnenie oznamovacej povinnosti pri začatí činnosti [§ 31 ods. 1 písm. a)]

Tento správny delikt sankcionuje opomenutie základnej vstupnej povinnosti do regulačného režimu kybernetickej bezpečnosti: subjekt, ktorý začne vykonávať činnosť spadajúcu pod § 17 ods. 1 ZoKB, musí túto skutočnosť v zákonnej lehote oznámiť NBÚ.

Subjektom deliktu je PZS – špeciálny subjekt, ktorý sa stal adresátom povinností podľa ZoKB tým, že fakticky začal vykonávať relevantnú činnosť alebo poskytovať službu v sektoroch podľa príloh ZoKB. **Objektom** je ochrana riadneho výkonu dohľadu a koordinácie v kybernetickej bezpečnosti; bez včasného oznámenia NBÚ nevie subjekt identifikovať, zaradiť do evidencie a včas naň uplatniť preventívne a kontrolné mechanizmy. **Objektívna stránka** spočíva v porušení povinnosti *oznámiť začiatok vykonávania činnosti* – spravidla ide o neoznámenie vôbec alebo o oneskorené oznámenie. Súčasťou oznamovacej povinnosti je aj minimálny obsah oznámenia (identifikačné a kontaktné údaje vrátane elektronických adries, verejných IP adries a telefónnych čísel, informácia o pôsobení v členských štátoch EÚ a údaje o zástupcovi, ak je relevantný). Následok nie je konštrukčným znakom deliktu; podstatné je samotné porušenie povinnosti, pričom reálne dopady (napr. sťaženie dohľadu, oneskorené uloženie opatrení) sa typicky zohľadnia pri správnej úvahe o výške pokuty. Z hľadiska **subjektívnej stránky** zákon nevyžaduje úmysel; pri tejto kategórii správnych deliktov PZS sa v praxi uplatňuje objektivizovaný režim zodpovednosti (zodpovednosť viazaná na porušenie povinnosti), pričom miera zavinenia sa môže premietnuť najmä do individualizácie sankcie.

10.1.4.2 Nesplnenie oznamovacej povinnosti pri zmene zapísaných údajov [§ 31 ods. 1 písm. b)]

Tento správny delikt nadväzuje na úvodnú oznamovaciu povinnosť podľa § 17 ods. 2 ZoKB, no už v udržiavacom režime: cieľom je, aby register PZS obsahoval aktuálne a použiteľné údaje počas celého trvania regulácie.

Subjektom deliktu je PZS ako špeciálny subjekt, ktorému vznikli práva a povinnosti zápisom do registra. **Objektom** je ochrana riadneho výkonu verejnej správy v sektore

kybernetickej bezpečnosti – najmä funkčná evidencia, adresná komunikácia, možnosť efektívneho dohľadu a včasného presadzovania povinností. **Objektívna stránka** spočíva v porušení povinnosti oznámiť *každú zmenu zapísaných skutočností, ktorá nie je referenčným údajom* v zákonnej lehote a predpísanou formou – prostredníctvom jednotného informačného systému kybernetickej bezpečnosti. Typicky pôjde o neoznámenie zmeny vôbec alebo o oneskorené oznámenie; vecne môžu byť relevantné najmä zmeny kontaktných a doručovacích údajov, zmeny v identifikačných údajoch, zmeny v rozsahu poskytovaných služieb, či zmeny na pozíciách zodpovedných osôb (napr. manažér kybernetickej bezpečnosti). Následok nie je konštrukčným znakom deliktu; postačuje porušenie povinnosti, pričom praktický dopad (napr. znemožnenie doručenia, sťaženie kontroly, oneskorenie reakcie na incident) sa zohľadňuje pri hodnotení závažnosti a pri individualizácii sankcie. Z hľadiska **subjektívnej stránky** zákon pri tejto skutkovej podstate nepracuje s úmyslom. Pri správnych deliktoch PZS preto prevláda objektivizovaný prístup: zodpovednosť sa viaže na porušenie povinnosti, kým miera zavinenia (ak ju správny orgán v konkrétnej veci hodnotí) má význam najmä pri úvahe o výške pokuty a pri posúdení, či ide o izolované zlyhanie alebo o systémové zanedbanie compliance režimu.

10.1.4.3 Nesplnenie oznamovacej povinnosti pri prevádzkovaní kritickej základnej služby [§ 31 ods. 1 písm. c)]

Tento správny delikt nadväzuje na osobitný **kritický** režim PZS. Jeho funkciou je, aby NBÚ disponoval včasnou a spoľahlivou informáciou o tom, že PZS vykonáva aspoň jednu kritickú základnú službu v zmysle § 18 ods. 1 ZoKB, čím sa aktivujú **intenzívnejšie očakávania na dohľad a riadenie rizík.** Oznámenie podľa § 18 ods. 2 ZoKB preto nie je len formálnou evidenčnou povinnosťou, ale súčasťou systému **identifikácie subjektov s potenciálne vysokým vplyvom na verejný poriadok, bezpečnosť, verejné zdravie alebo na systémové fungovanie vybraných sektorov.**

Subjektom deliktu je PZS ako špeciálny subjekt, ktorý zároveň vykonáva **aspoň jednu kritickú základnú službu**; v praxi pôjde spravidla o právnickú osobu, pričom ZoKB výslovne ráta aj s verejnými subjektmi. **Objektom** je ochrana riadneho výkonu verejnej správy v kybernetickej bezpečnosti – najmä správnosť registra, adresnosť dohľadu a schopnosť NBÚ nastaviť primerané kontrolné a presadzovacie mechanizmy voči subjektom s kritickým významom. **Objektívna stránka** spočíva v porušení oznamovacej povinnosti, t. j. v

opomenutí oznámiť NBÚ, že PZS vykonáva kritickú základnú službu. Následok nie je konštrukčným znakom deliktu; postačuje porušenie povinnosti, pričom praktické dôsledky (napr. sťaženie dohľadu, zníženie schopnosti včasnej koordinácie pri incidente) sa zohľadňujú pri hodnotení závažnosti a pri individualizácii sankcie. Z hľadiska **subjektívnej stránky** ZoKB pri tejto skutkovej podstate neviaže zodpovednosť na úmysel; pri správnych deliktoch PZS preto typicky prevláda objektivizovaný prístup, kde je rozhodujúce samotné porušenie povinnosti a compliance nastavenie (t. j. či PZS má interné mechanizmy identifikácie, že jeho činnosť spadá pod § 18 ods. 1 ZoKB, a mechanizmus včasného oznámenia).

10.1.4.4 Zlyhanie povinností pri využití tretej strany a pri riadení dodávateľského reťazca [§ 31 ods. 1 písm. d)]

Tento správny delikt pokrýva dodávateľský reťazec (supply chain) jadro kybernetickej regulácie: zákon tu vyžaduje, aby PZS vedel bezpečnostne uchopiť externé závislosti, ktoré priamo vplývajú na dostupnosť, dôvernosť a integritu jeho sietí a informačných systémov. Delikt je konštruovaný blanketovo – odkazuje na porušenie povinností podľa § 19 ods. 2 až 4 ZoKB (zmluvný režim s treťou stranou, analýza rizík, kontrolovateľnosť), § 19 ods. 6 písm. f) ZoKB (analýza závislostí aktív, IS, produktov a služieb IKT v dodávateľskom reťazci) a § 19 ods. 7 ZoKB (hlásenie zmien vrátane informácie o zmluve s treťou stranou s významným vplyvom pri kritickej základnej službe).

Subjektom deliktu je PZS ako špeciálny subjekt. **Objektom** je ochrana kybernetickej bezpečnosti a odolnosti základnej služby, osobitne schopnosť riadiť riziká vyplývajúce z outsourcingu a z dodávateľských vzťahov. **Objektívna stránka** sa napĺňa porušením povinnosti: typicky neuzatvorením alebo nevhodným nastavením zmluvy s treťou stranou pri činnosti priamo súvisiacej s CIA triádou, nevykonaním analýzy rizík pri uzatváraní zmluvy, nevytvorením reálnej kontrolovateľnosti (vrátane povinnosti tretej strany podrobiť sa kontrole), nezohľadnením zákonných výnimiek (napr. nízke riziko alebo tretia strana ako poskytovateľ základnej služby), neplnením informačnej povinnosti voči tretej strane pri incidente, zanedbaním povinnej analýzy závislostí v dodávateľskom reťazci, alebo neohlásením zmien a relevantných zmluvných skutočností NBÚ. Následok nie je obligatórnym znakom; rozhodujúce je porušenie povinnosti, pričom reálne dopady (napr. zhoršenie detekcie incidentu, rozšírenie kompromitácie cez dodávateľa, oneskorená reakcia) sa premietajú do hodnotenia závažnosti a výmery pokuty. **Subjektívna stránka** pri tomto

type deliktov býva objektivizovaná: zákon neviaže zodpovednosť na úmysel a PZSje hodnotený podľa toho, či mal nastavený účinný compliance režim vo vzťahu k tretím stranám (zmluvné klauzuly, procesy riadenia rizík, auditovateľnosť, priebežné vyhodnocovanie závislostí a oznamovanie zmien). V praxi bude správny orgán rozlišovať medzi izolovaným pochybením a systémovým zanedbaním riadenia dodávateľského reťazca, čo je typicky rozhodujúce pre individualizáciu sankcie.

10.1.4.5 Neaktuálna alebo nereálna bezpečnostná dokumentácia [§ 31 ods. 1 písm. e)]

Tento správny delikt nadväzuje na požiadavku, aby bezpečnostné opatrenia neboli len „formálne prijaté", ale aj reálne riadené a preukázateľné. § 20 ods. 3 ZoKB viaže prijímanie a realizáciu bezpečnostných opatrení na schválenú bezpečnostnú dokumentáciu, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu. Zmyslom je, aby dokumentácia odrážala skutočné procesy, roly a technológie a aby bola použiteľná pri audite, dohľade a riešení incidentov.

Subjektom deliktu je PZS ako špeciálny subjekt regulácie. **Objektom** je ochrana kybernetickej bezpečnosti a odolnosti základnej služby, bezprostredne však aj ochrana funkčnej dokumentácie ako nástroja riadenia a kontroly súladu. **Objektívna** stránka sa napĺňa porušením povinnosti udržiavať bezpečnostnú dokumentáciu aktuálnu a zodpovedajúcu reálnemu stavu (§ 20 ods. 3). Typicky pôjde o situácie, keď PZS:

1. neaktualizuje dokumentáciu po významných zmenách v sieťach, informačných systémoch, konfiguráciách, rolách a zodpovednostiach alebo v dodávateľskom modeli;
2. má dokumentáciu odtrhnutú od praxe (opisuje opatrenia, ktoré sa nevykonávajú, alebo naopak, reálne postupy nie sú zdokumentované);
3. nevie preukázať pokrytie opatrení v rozsahu § 20 ods. 2 ZoKB spôsobom, ktorý umožní kontrolu účinnosti a súladu.

Následok nie je znakom deliktu; postačuje samotné porušenie povinnosti. Reálne dopady (napr. sťaženie auditu, dohľadu, manažmentu incidentov alebo zvýšenie rizika) sa však zohľadnia pri posúdení závažnosti a pri výmere pokuty. Z hľadiska **subjektívnej stránky** ide o objektivizovaný režim: jadrom je nesplnenie zákonnej povinnosti; prípadná miera zavinenia sa typicky premietne najmä do individualizácie sankcie.

10.1.4.6 Porušenie povinností PZS spojených s auditom [§ 31 ods. 1 písm. f)]

Tento správny delikt pokrýva „kontrolnú" vrstvu compliance režimu v kybernetickej bezpečnosti. Audit podľa § 29 ZoKB nie je len formálny prvok, ale kľúčový mechanizmus overenia, či PZS reálne plní povinnosti, či prijaté opatrenia zodpovedajú zákonným požiadavkám a či sú účinné. Delikt podľa § 31 ods. 1 písm. f) ZoKB sa viaže na porušenie povinností podľa § 29 ods. 1, 2, 5 alebo 8 ZoKB, teda na:

1. prvotnú povinnosť preveriť účinnosť opatrení v stanovenej lehote;
2. periodické audity a audity vykonané po zmene majúcej významný vplyv;
3. predkladanie záverečnej správy s návrhom nápravy a
4. zákonné podmienky samohodnotenia ako alternatívy auditu.

Subjektom deliktu je PZS ako špeciálny subjekt regulácie. **Objektom** je verejný záujem na tom, aby úroveň kybernetickej bezpečnosti a odolnosti nebola deklaratórna, ale overiteľná, porovnateľná a vynútiteľná – vrátane toho, aby NBÚ mal k dispozícii relevantné výstupy pre dohľad a následné presadzovanie práva. **Objektívna stránka** sa napĺňa porušením niektorej z auditných povinností. Typicky pôjde o:

1. nevykonanie auditu v zákonnej lehote (napr. po zaradení do registra), prípadne nevykonanie auditu po významnej zmene alebo v určených intervaloch (§ 29 ods. 1 a 2 ZoKB),
2. nepredloženie záverečnej správy NBÚ spolu s opatreniami na nápravu a lehotami (§ 29 ods. 5 ZoKB), vrátane oneskoreného predloženia alebo predloženia bez reálnej „nápravnej" časti,
3. zneužitie alebo nesplnenie podmienok samohodnotenia (§ 29 ods. 8 ZoKB), napr. vykonanie samohodnotenia mimo stanovenej periodicity, vykonanie samohodnotenia v čase, keď sa má vykonať audit, alebo nerešpektovanie povinnosti podrobiť sa auditu v zákonom stanovenej lehote.

Následok nie je konštrukčným znakom deliktu; rozhoduje porušenie povinnosti. Praktické dopady (napr. neodhalené nedostatky, oneskorená náprava, zvýšené riziko incidentu) sa však premietajú do závažnosti a individualizácie sankcie. **Subjektívna stránka** sa pri tomto type deliktov spravidla neviaže na úmysel; zodpovednosť je objektivizovaná a jadrom je porušenie zákonnej povinnosti, kým miera zavinenia (ak ju orgán hodnotí) sa typicky uplatní až pri úvahe o výške pokuty.

10.1.4.7 Nevykonanie opatrenia na nápravu v lehote podľa záverečnej správy z auditu [§ 31 ods. 1 písm. g)]

Tento správny delikt je úzko previazaný s inštitútom auditu kybernetickej bezpečnosti. Audit podľa § 29 ZoKB slúži na overenie plnenia povinností podľa ZoKB, posúdenie zhody prijatých bezpečnostných opatrení a na identifikáciu nedostatkov, ktoré je potrebné odstrániť, aby sa zabezpečila požadovaná úroveň kybernetickej bezpečnosti a predchádzalo sa incidentom. ZoKB vyžaduje, aby PZS predložil NBÚ záverečnú správu o výsledkoch auditu spolu s opatreniami na nápravu a s lehotami na ich odstránenie (§ 29 ods. 5 ZoKB). Skutková podstata podľa § 31 ods. 1 písm. g) ZoKB potom postihuje situáciu, keď PZS nevykoná opatrenie na nápravu v lehote, ktorú takáto záverečná správa predpokladá.

Subjektom deliktu je PZS ako špeciálny subjekt regulácie. **Objektom** je ochrana riadneho zabezpečovania kybernetickej bezpečnosti a odolnosti základných služieb, pričom osobitne sa chráni funkčnosť auditného mechanizmu ako nástroja odhaľovania a odstraňovania nedostatkov v bezpečnostných opatreniach. **Objektívna stránka** spočíva v porušení povinnosti vykonať identifikované opatrenia na nápravu v určenej lehote; pre naplnenie deliktu je rozhodujúce samotné nesplnenie lehoty, nie vznik kybernetického incidentu. Následné riziká alebo reálne dopady (napr. pretrvávanie nedostatkov v bezpečnostných opatreniach) majú význam najmä pri hodnotení závažnosti a pri určovaní výšky pokuty. **Subjektívna stránka** je pri tejto skutkovej podstate typicky objektivizovaná: zodpovednosť sa viaže na porušenie povinnosti, pričom prípadné dôvody omeškania alebo miera zavinenia môžu byť relevantné najmä pri individualizácii sankcie.

10.1.4.8 Nesplnenie povinnosti uloženej opatrením na nápravu [§ 31 ods. 1 písm. h)]

Tento správny delikt je naviazaný na dohľadové konanie podľa § 29j ZoKB. Ak NBÚ zistí nedostatky, môže PZS uložiť konkrétnu povinnosť (vykonať audit a realizovať odporúčania, prijať nápravné opatrenia, informovať dotknuté osoby/verejnosť alebo dočasne zakázať poskytovanie služby; pri kritickej základnej službe pri nesplnení povinností aj zákaz výkonu funkcie určeným osobám).

Objektom je zabezpečenie reálnej vynútiteľnosti nápravy a ochrana kybernetickej bezpečnosti prostredníctvom odstránenia zistených nedostatkov. **Subjektom** je špeciálny subjekt – PZS, ktorému bola povinnosť uložená rozhodnutím NBÚ. **Objektívna stránka** spočíva v porušení uloženej povinnosti, typicky jej nesplnením v určenej lehote alebo

nesplnením v predpísanom rozsahu; na naplnenie skutkovej podstaty postačuje samotné porušenie, pričom praktické dopady sa zohľadnia pri výmere pokuty. **Subjektívna stránka** nie je viazaná na úmysel; režim je objektivizovaný, miera zavinenia má význam najmä pri individualizácii sankcie.

10.1.4.9 Zlyhanie ťažiskových povinností PZS [§ 31 ods. 2 písm. a)]

Tento správny delikt predstavuje ťažiskovú skutkovú podstatu sankčného režimu ZoKB. Nadväzuje na „jadro" povinností PZS: na jednej strane povinnosť v zákonom stanovenej lehote zaviesť a reálne vykonávať všeobecné (a prípadne sektorové) bezpečnostné opatrenia na základe analýzy rizík (§ 19 ods. 1 ZoKB), na druhej strane vybrané incidentné, koordinačné a organizačné povinnosti (§ 19 ods. 6 písm. a) až e) a písm. g) až i) ZoKB). Ide o povinnosti, ktoré sú koncipované tak, aby PZS zabezpečil kybernetickú bezpečnosť a odolnosť služby nielen formálne, ale aj v prevádzke – najmä pri riešení incidentu, pri plnení notifikačných a kooperačných povinností, pri zabezpečení dôkazov, pri komunikácii s orgánmi činnými v trestnom konaní a pri vnútornom riadení bezpečnosti (vrátane mechanizmov informovania vedenia PZS a oznamovania zmien štatutárnych orgánov).

Subjektom deliktu je PZS ako špeciálny subjekt regulácie. **Objektom** je ochrana kybernetickej bezpečnosti a odolnosti základných služieb, a tým aj ochrana verejného záujmu na stabilite, dostupnosti, dôvernosti a integrite sietí a informačných systémov v regulovaných sektoroch. **Objektívna stránka** spočíva v porušení konkrétnej povinnosti z § 19 ods. 1 ZoKB alebo z § 19 ods. 6 ZoKB v označenom rozsahu; v praxi pôjde typicky o nezavedenie alebo nevykonávanie bezpečnostných opatrení v požadovanom rozsahu, o nezvládnutie povinností pri incidente (riešenie, hlásenie, súčinnosť, zabezpečenie dôkazov, oznámenie OČTK), alebo o zanedbanie organizačných mechanizmov riadenia bezpečnosti. Následok nie je konštrukčným znakom deliktu; rozhodujúce je porušenie povinnosti, pričom reálne dopady na službu alebo zvýšenie rizika sa zohľadňujú pri hodnotení závažnosti a individualizácii pokuty. **Subjektívna stránka** je pri tejto skutkovej podstate objektivizovaná: zodpovednosť sa viaže na nesplnenie zákonnej povinnosti, pričom miera zavinenia (ak sa hodnotí) sa typicky premieta do úvahy o výške sankcie.

10.1.4.10 Nedostatky v prijatí bezpečnostnej dokumentácie ako podmienky realizácie opatrení [§ 31 ods. 2 písm. b)]

Tento správny delikt je naviazaný na dokumentačný pilier kybernetickej bezpečnosti. Ustanovenie § 20 ZoKB vychádza z toho, že bezpečnostné opatrenia nie sú len technické nástroje, ale aj *úlohy, procesy a role* v organizačnej, personálnej a ďalších oblastiach, prijímané na základe analýzy rizík s cieľom prevencie, detekcie, reakcie a obnovy po incidente (§ 20 ods. 1 ZoKB). Aby boli tieto opatrenia vykonateľné, § 20 ods. 3 ZoKB vyžaduje ich prijatie a realizáciu *na základe schválenej bezpečnostnej dokumentácie,* ktorá musí byť aktuálna a zodpovedať reálnemu stavu; tým sa vytvára požiadavka, aby interný bezpečnostný režim PZS mal formu overiteľných a auditovateľných pravidiel.

Subjektom deliktu je PZS ako špeciálny subjekt regulácie. **Objektom** je ochrana riadneho zabezpečenia kybernetickej bezpečnosti a odolnosti základnej služby, osobitne garancia, že bezpečnostné opatrenia budú systémovo nastavené a kontrolovateľné. **Objektívna stránka** spočíva v porušení povinnosti **prijať (mať schválenú)** bezpečnostnú dokumentáciu ako predpoklad realizácie opatrení v rozsahu a spôsobom podľa § 20 ods. 3 ZoKB; naplnenie deliktu je viazané na absenciu alebo nesplnenie tohto dokumentačného rámca, nie na vznik incidentu. **Subjektívna stránka** je objektivizovaná: rozhodujúce je porušenie povinnosti, pričom prípadné dôvody a miera zavinenia sa môžu prejaviť najmä pri úvahe o výške sankcie.

10.1.4.11 Nenahlásenie závažného kybernetického bezpečnostného incidentu [§ 31 ods. 2 písm. c)]

Tento delikt tvorí jadro manažmentu režimu incidentov: štát sleduje, aby mal orgán dohľadu včasné, priebežné a záverečné informácie o udalostiach, ktoré dosahujú kvalitu ***závažného*** incidentu (§ 24 ods. 1 a 2 ZoKB). Závažnosť je viazaná buď na rozsiahly incident, alebo na incident s reálnym či potenciálnym závažným narušením fungovania PZS, prípadne s významnými majetkovými dopadmi na PZS alebo tretie osoby (§ 24 ods. 2 ZoKB). Hlásenie je prísne časovo štruktúrované: včasné varovanie, následné oznámenie, prípadné priebežné doplnenia a záverečná správa (§ 24 ods. 3 ZoKB). V osobitných situáciách sa počíta aj s alternatívnym režimom (zmluva o odlišnom spôsobe hlásenia podľa § 24 ods. 4 ZoKB) a pri subjektoch regulovaných nariadením DORA s hlásením cez príslušný orgán (§ 24 ods. 8 ZoKB). Ak je to vzhľadom na povahu alebo dôležitosť subjektu potrebné, zákon umožňuje aj

automatizované vyhodnocovanie a nahlasovanie incidentov rozhodnutím NBÚ (§ 24a ZoKB). Na § 24a ZoKB však nadväzuje osobitná skutková podstata správneho deliktu.

Subjektom je PZS ako špeciálny subjekt. **Objektom** je ochrana kybernetickej bezpečnosti a odolnosti základných služieb cez funkčný systém včasnej notifikácie a koordinácie riešenia incidentov. **Objektívna stránka** spočíva v neohlásení incidentu, ktorý spĺňa znaky ***závažného incidentu*****,** resp. v nesplnení zákonom predpísanej formy a časovej postupnosti hlásenia (§ 24 ods. 1 a 3 ZoKB). Následok nie je konštrukčným znakom; postačuje porušenie povinnosti, pričom reálne dopady sa prejavia najmä pri hodnotení závažnosti a výmere sankcie. **Subjektívna stránka** je objektivizovaná – zodpovednosť sa viaže na nesplnenie notifikačnej povinnosti; dôvody zlyhania (procesné, organizačné, technické) sú spravidla relevantné pri individualizácii pokuty.

10.1.4.12 Nesplnenie povinnosti automatizovaného vyhodnocovania a hlásenia incidentov [§ 31 ods. 2 písm. d)]

Táto skutková podstata nadväzuje na notifikačný režim podľa § 24 ZoKB, no posúva ho do automatizovanej, technologicky podporenej roviny. Ak je to vzhľadom na povahu alebo dôležitosť PZS potrebné a nebola uzatvorená zmluva o odlišnom spôsobe hlásenia podľa § 24 ods. 4 ZoKB, NBÚ môže rozhodnutím uložiť povinnosť automatizovaným spôsobom vyhodnocovať výskyt kybernetického bezpečnostného incidentu a nahlasovať kybernetický bezpečnostný incident (§ 24a ods. 1 ZoKB). Cieľom je zabezpečiť včasnosť a spoľahlivosť informácií pre riešenie incidentov a koordináciu reakcie, pričom NBÚ na tento účel zverejňuje relevantné výstrahy a varovania v jednotnom informačnom systéme kybernetickej bezpečnosti. Takýto spôsob automatizovaného poskytovania informácií zároveň eliminuje ľudský faktor a je *de facto* v nepretržitej pohotovosti čo, z hľadiska reakčného času, vytvára pozitívny predpoklad na zvládnutie bezpečnostného incidentu a elimináciu väčšieho rozsahu škôd.

Subjektom deliktu je PZS ako špeciálny subjekt, ktorému bola povinnosť uložená individuálnym rozhodnutím NBÚ. **Objektom** je ochrana kybernetickej bezpečnosti a efektívna funkčnosť informačných tokov potrebných na riešenie incidentov. **Objektívna stránka** spočíva v porušení rozhodnutím uloženej povinnosti *zasielať automatizovaným spôsobom určené systémové informácie*, teda v neplnení automatizovaného vyhodnocovania a nahlasovania v určenom spôsobe, rozsahu alebo trvaní (§ 24a ods. 3 ZoKB), prípadne v

obchádzaní či deaktivovaní mechanizmu. Následok nie je konštrukčným znakom; relevantný je samotný nesúlad s uloženou povinnosťou, pričom praktické dopady sa zohľadnia pri závažnosti a výmere pokuty. **Subjektívna stránka** je objektivizovaná – zodpovednosť sa viaže na nesplnenie povinnosti uloženej rozhodnutím, bez potreby preukazovať úmysel.

10.1.4.13 Nesplnenie povinností pri riešení incidentu a reaktívnych opatreniach uložených rozhodnutím NBÚ [§ 31 ods. 2 písm. e)]

Tento správny delikt je viazaný na „intervenčný" režim podľa § 27 ZoKB, v ktorom NBÚ pri závažnom kybernetickom bezpečnostnom incidente alebo významnej kybernetickej hrozbe ukladá adresné povinnosti formou rozhodnutia. Podstata skutkovej podstaty spočíva v tom, že jednotka CSIRT, PZS, príp. aj tretia strana s významným vplyvom nerešpektuje rozhodnutím uložený príkaz buď riešiť incident (§ 27 ods. 3 ZoKB), vykonať reaktívne opatrenie (§ 27 ods. 5 ZoKB), alebo následne bezodkladne oznámiť a preukázať vykonanie reaktívneho opatrenia a jeho výsledok (§ 27 ods. 6 ZoKB). Ide teda o delikt spätý s presadzovaním práva v reálnom čase, kde zlyhanie udržiavania regulačnej zhody môže viesť k pokračovaniu, šíreniu alebo opakovanému výskytu incidentu.

Subjektom deliktu je PZS ako špeciálny subjekt regulácie; v samotnom § 27 ZoKB však NBÚ môže adresovať povinnosť aj tomu, kto plní úlohy jednotky CSIRT alebo tretej strane, čo zodpovedá širšiemu okruhu adresátov rozhodnutia (§ 27 ods. 3 a 5 ZoKB). **Objektom** je ochrana kybernetickej bezpečnosti a odolnosti základných služieb, osobitne záujem na účinnej a včasnej reakcii na závažné incidenty a na funkčnosti krízového riadenia. **Objektívna stránka** sa napĺňa porušením povinnosti uloženej rozhodnutím: nečinnosťou, zjavne neúspešným riešením (ktoré je dôvodom ukladania reaktívneho opatrenia), nevykonaním uloženého reaktívneho opatrenia, alebo nesplnením oznamovacej a preukaznej povinnosti o jeho vykonaní a výsledku prostredníctvom jednotného informačného systému kybernetickej bezpečnosti. Následok nie je konštrukčným znakom; rozhodujúce je porušenie príkazu NBÚ, pričom dopady na rozsah incidentu sa zohľadnia pri závažnosti a sankcii. **Subjektívna stránka** je pri tejto skutkovej podstate objektivizovaná a viazaná na neplnenie povinnosti uloženej rozhodnutím; prípadná miera zavinenia sa spravidla premieta najmä do individualizácie výšky pokuty.

10.1.4.14 Nesplnenie povinností pri ochrannom opatrení [§ 31 ods. 2 písm. f)]

Tento správny delikt je prepojený s mechanizmom *ochranného opatrenia* (§ 27 ods. 1 písm. d) ZoKB), ktoré smeruje k zabráneniu ďalšieho pokračovania, šírenia alebo opakovaného výskytu závažného kybernetického bezpečnostného incidentu. Zákon tu upravuje dvojfázový režim: (i) PZS má na výzvu NBÚ v určenej lehote predložiť navrhované ochranné opatrenie na schválenie; (ii) NBÚ ho rozhodnutím schváli a určí lehotu na jeho vykonanie (§ 27 ods. 8 ZoKB). NBÚ si tak necháva absolútny dohľad nad výkonom a podobou ochranných opatrení. Je preto logické, že táto kompetencia prináleží najvyššej štátnej autorite. Skutková podstata v § 31 ods. 2 písm. f) ZoKB postihuje obe fázy – nepredloženie návrhu na schválenie a/alebo nevykonanie schváleného ochranného opatrenia.

Subjektom deliktu je PZS ako špeciálny subjekt regulácie. **Objektom** je ochrana kybernetickej bezpečnosti a odolnosti základných služieb, osobitne záujem na tom, aby po incidente nasledovali účinné preventívno-stabilizačné kroky minimalizujúce riziko rekurencie alebo eskalácie. **Objektívna stránka** sa napĺňa porušením povinnosti viazanej na výzvu NBÚ (nepredloženie ochranného opatrenia v určenej lehote) alebo porušením povinnosti viazanej na rozhodnutie NBÚ (nevykonanie schváleného opatrenia v určenej lehote). Následok nie je konštrukčným znakom; rozhodujúce je porušenie procesne a časovo determinovanej povinnosti, pričom praktické dopady (napr. pretrvávanie zraniteľnosti, opakovanie incidentu) sa premietnu najmä do závažnosti a výmery pokuty. **Subjektívna stránka** je pri tejto skutkovej podstate objektivizovaná – zodpovednosť sa viaže na neplnenie povinnosti v určenej lehote, pričom prípadné dôvody zlyhania a miera zavinenia majú význam predovšetkým pri individualizácii sankcie.

10.1.4.15 Nesplnenie oznamovacej povinnosti pri zmene údajov osoby podľa § 2 ods. 2 [§ 31 ods. 4]

Skutková podstata sleduje, verejný záujem spočívajúci v potrebe NBÚ disponovať aktuálnymi a použiteľnými údajmi o osobách poskytujúcich služby alebo vykonávajúcich činnosti podľa § 2 ods. 2 ZoKB. Nejde len o „cezhraničných" poskytovateľov: § 2 ods. 2 ZoKB primárne vymedzuje vecný okruh služieb (napr. DNS, registrácia domén, cloud, dátové centrá, CDN, riadené a bezpečnostné služby, online trh, vyhľadávače, sociálne platformy) a až sekundárne upravuje osobitné väzby na SR/EÚ pre subjekty bez sídla v SR [kritériá písm. a) členský štát EÚ a písm. b) nečlenský štát EÚ]. Povinnosť podľa § 21 ods. 3 ZoKB má

udržiavací charakter s vplyvom na regulačnú zhodu a aktivuje sa na výzvu NBÚ; následne treba oznámiť zmeny určených údajov cez jednotný informačný systém.

Objektom je riadny výkon dohľadu a komunikácie NBÚ (vrátane možnosti koordinácie podľa § 21 ods. 2 ZoKB a oznamovania Agentúre ENISA podľa § 21 ods. 4) ZoKB. **Subjektom** je osoba podľa § 2 ods. 2 ZoKB, na ktorú sa vzťahuje pôsobnosť ZoKB (spravidla PO alebo podnikajúca FO; pri zahraničných subjektoch sa väzba na SR/EÚ posudzuje podľa § 2 ods. 2 písm. a) alebo b) ZoKB a to aj cez zástupcu podľa § 21 ods. 1 ZoKB). **Objektívna stránka** spočíva v tom, že subjekt na výzvu NBÚ neoznámi zmenu údajov podľa § 21 ods. 3 ZoKB (alebo oznámi zmenu oneskorene či mimo predpísanej formy). Následok nie je znakom skutkovej podstaty, no sťaženie dohľadu sa zohľadní pri sankcii. **Subjektívna stránka** je typicky objektivizovaná – rozhoduje porušenie povinnosti, nie preukázanie úmyslu.

10.1.4.16 Neurčenie zástupcu pre poskytovateľa služieb podľa § 2 ods. 2 mimo EÚ [§ 31 ods. 5]

Táto skutková podstata je zameraná na situáciu, keď sa na území SR poskytujú vybrané digitálne služby (DNS, registrácia domén, cloud, dátové centrá, CDN, riadené a bezpečnostné služby, online trh, vyhľadávače, sociálne platformy) subjektom, ktorý nemá trvalý pobyt, miesto podnikania ani sídlo v členskom štáte EÚ. Zákon v takom prípade vyžaduje z hľadiska udržania štandardov zodpovednostných vzťahov ustanovenie kontaktného subjektu smerom k jurisdikcii EÚ/SR – určením zástupcu počas celej doby poskytovania služieb alebo výkonu činností.

Objektom je zabezpečenie účinného výkonu verejnej moci v kybernetickej bezpečnosti pri subjektoch mimo EÚ, najmä presadzovanie povinností, doručovanie, dohľad a koordinácia (vrátane väzby na evidenčné a oznamovacie mechanizmy podľa § 21 ZoKB). **Subjektom** je špeciálna osoba poskytujúca služby alebo vykonávajúca činnosti podľa § 2 ods. 2 ZoKB na území SR, ktorá zároveň nemá väzbu na EÚ vo forme trvalého pobytu/miesta podnikania/sídla; ZoKB predpokladá, že podmienky pôsobnosti sa napĺňajú najmä cez § 2 ods. 2 písm. b) ZoKB (t. j. potreba zástupcu). **Objektívna stránka** spočíva v opomenutí: subjekt si neurčí zástupcu s trvalým pobytom, miestom podnikania alebo sídlom na území SR alebo v inom členskom štáte EÚ, v ktorom tiež poskytuje služby/vykonáva činnosti, alebo stratou kontinuity: zástupca prestane vykonávať svoju funkciu a nebude ustanovený nový. Následok nie je znakom skutkovej podstaty; postačuje samotná absencia zástupcu, pričom

praktické dôsledky (sťaženie dohľadu a presadzovania) sa premietnu do závažnosti a výšky pokuty. **Subjektívna stránka** je objektivizovaná – delikt sa viaže na nesplnenie povinnosti *mať určeného zástupcu* počas celej doby poskytovania, bez potreby dokazovať úmysel.

10.1.4.17 Nevedenie osobitnej evidencie registračných údajov domény [§ 31 ods. 6 písm. a)]

Táto skutková podstata zavádza sankčnú zodpovednosť správcov TLD a registrátorov domén za nesplnenie evidenčnej povinnosti pri registrácii názvu domény. Zmyslom § 22 ZoKB je vytvoriť spoľahlivý identifikačný a kontaktný rámec k držiteľovi domény a k samotnej registrácii, ktorý je použiteľný pre dohľad a výkon štátnej správy v kybernetickej bezpečnosti (vrátane nadväzujúcich povinností overovania údajov, zverejňovania neosobných údajov a poskytovania údajov oprávneným orgánom).

Objektom je ochrana riadneho výkonu verejnej správy v kybernetickej bezpečnosti, najmä transparentnosť a dohľadateľnosť doménových registrácií a schopnosť štátu operatívne pracovať s registračnými údajmi pri riešení incidentov, hrozieb a presadzovaní povinností. **Subjektom** je špeciálny subjekt – správca TLD a osoba poskytujúca službu registrácie názvu domény; ide typicky o právnické osoby pôsobiace v regulovanom segmente. **Objektívna stránka** spočíva v porušení povinnosti „evidovať a viesť osobitnú evidenciu registračných údajov" pri registrácii domény; delikt sa naplní už tým, že evidencia nie je vedená vôbec, je vedená len formálne, je neúplná alebo nevzniká v súvislosti s jednotlivými registráciami. Následok (napr. sťaženie dohľadu alebo oneskorenie reakcie pri incidente) nie je znakom skutkovej podstaty, ale je relevantný pri posudzovaní závažnosti a individualizácii pokuty. **Subjektívna stránka** je objektivizovaná: zodpovednosť sa viaže na nesplnenie zákonnej evidenčnej povinnosti bez toho, aby zákon vyžadoval preukázanie úmyslu.

10.1.4.18 Neprijatie a nezverejnenie vnútorných predpisov a postupov overovania údajov [§ 31 ods. 6 písm. b]

Táto skutková podstata nadväzuje na evidenčný režim registračných údajov a posúva ho do roviny kvality vstupu: správca TLD a registrátor nemajú iba údaje evidovať, ale musia mať nastavené a formálne prijaté interné pravidlá a postupy, ktoré zabezpečia overenie údajov predkladaných pri registrácii domény aspoň v rozsahu overenia údajov o držiteľovi

domény (§ 22 ods. 3 ZoKB). Súčasne zákon vyžaduje, aby vnútorné predpisy a informácia o postupoch pri poskytovaní údajov oprávneným orgánom boli bezodplatne zverejnené na webovom sídle (§ 22 ods. 7 ZoKB).

Subjektom deliktu je špeciálny subjekt – správca TLD alebo osoba poskytujúca službu registrácie názvu domény. **Objektom** je ochrana dôveryhodnosti registračných údajov domén a tým aj bezpečnostných záujmov v kybernetickej bezpečnosti, keďže doménová infraštruktúra je citlivá na zneužívanie anonymitou alebo falošnými identitami. **Objektívna stránka** spočíva v porušení povinnosti: (i) neprijať vnútorné predpisy alebo (ii) nezaviesť osobitné postupy overovania údajov. Následok nie je konštrukčným znakom; postačuje samotné porušenie, pričom praktické dopady (sťažená identifikácia držiteľov, zvýšené riziko zneužitia domén) sa premietnu najmä do posúdenia závažnosti a výmery pokuty. **Subjektívna stránka** je typicky objektivizovaná: zodpovednosť sa viaže na nesplnenie zákonnej povinnosti, pričom prípadná miera zavinenia sa môže zohľadniť najmä pri individualizácii sankcie.

10.1.4.19 Nezverejnenie neosobných registračných údajov po registrácii domény [§ 31 ods. 6 písm. c)]

Táto skutková podstata postihuje porušenie povinnosti správcu TLD alebo registrátora bezodkladne po registrácii názvu domény bezodplatne zverejniť údaje predkladané pri registrácii domény, ktoré nie sú osobnými údajmi (§ 22 ods. 4 ZoKB). Ide o prvok transparentného režimu v doménovej oblasti: zákonodarca vytvára minimálny verejne dostupný informačný rámec o registrovaných doménach, pričom zverejňovanie osobných údajov je z ich povahy vylúčené.

Subjektom deliktu je špeciálny subjekt – správca TLD a osoba poskytujúca službu registrácie názvu domény. **Objektom** je ochrana bezpečnosti a dôveryhodnosti doménovej infraštruktúry prostredníctvom včasnej a bezplatnej dostupnosti neosobných registračných údajov, ktoré môžu slúžiť ako podklad na orientáciu v doménovom prostredí a podporovať rýchlejšiu identifikáciu rizikových doménových operácií (napr. pri incidentoch, zneužívaní domén alebo phishingových kampaniach). **Objektívna stránka** spočíva v opomenutí alebo oneskorení zverejnenia neosobných registračných údajov *bezodkladne po registrácii* alebo v zverejnení v rozpore s požiadavkou bezodplatnosti. Následok nie je konštrukčným znakom; rozhodujúce je samotné porušenie povinnosti, pričom praktické dopady (napr. sťaženie

reakcie na incident, horšia dohľadateľnosť základných údajov) budú relevantné pri posúdení závažnosti a výške pokuty. **Subjektívna stránka** je spravidla objektivizovaná: delikt sa viaže na nesplnenie povinnosti zverejniť údaje v predpísanom režime, pričom okolnosti pochybenia môžu mať význam najmä pri individualizácii sankcie.

10.1.4.20 Neposkytnutie registračných údajov NBÚ alebo ústrednému orgánu na požiadanie [§ 31 ods. 6 písm. d)]

Táto skutková podstata nadväzuje na neverejnú rovinu registračných údajov domén. Kým § 22 ods. 4 ZoKB smeruje k zverejneniu len neosobných údajov, § 22 ods. 5 ZoKB zakotvuje prístup NBÚ a ústredného orgánu k údajom predkladaným pri registrácii názvu domény na účely výkonu štátnej správy podľa ZoKB. Správca TLD a registrátor sú preto povinní tieto údaje na požiadanie bezodplatne poskytnúť a dodržať zákonom určenú lehotu (najneskôr do 72 hodín od doručenia žiadosti). Ide o štandardný dohľadový nástroj, ktorý má umožniť rýchle získanie relevantných údajov v situáciách, keď je to potrebné pre výkon kompetencií v oblasti kybernetickej bezpečnosti.

Subjektom deliktu je špeciálny subjekt – správca TLD a osoba poskytujúca službu registrácie názvu domény. **Objektom** je ochrana efektívneho výkonu štátnej správy v kybernetickej bezpečnosti, konkrétne schopnosť NBÚ a ústredného orgánu včas získať registračné údaje potrebné na identifikáciu a riešenie rizík spojených s doménovou infraštruktúrou (napr. pri incidentoch, zneužití domén, koordinácii opatrení alebo výkone dohľadu). **Objektívna stránka** spočíva v nesplnení povinnosti poskytnúť vyžiadané údaje – typicky ich neposkytnutím vôbec, poskytnutím po lehote alebo poskytnutím v neúplnom rozsahu, ktorý fakticky znemožňuje účel žiadosti; pre naplnenie skutkovej podstaty nie je nevyhnutné preukázať vznik škody, postačuje porušenie povinnosti viazanej na žiadosť oprávneného orgánu. **Subjektívna stránka** je v tejto skutkovej podstate objektivizovaná: zodpovednosť sa viaže na porušenie povinnosti ako takej, pričom prípadné dôvody zlyhania (napr. organizačné nastavenie, interné procesy, chybné spracovanie žiadosti) sa uplatnia najmä pri hodnotení závažnosti a individualizácii pokuty.

10.1.4.21 Neposkytnutie informácií na účely vypracovania národnej stratégie a národného plánu [§ 31 ods. 7 písm. a)]

Táto skutková podstata chráni funkčnosť strategického riadenia kybernetickej bezpečnosti na úrovni štátu. § 7 ods. 4 ZoKB ukladá ústredným orgánom a iným orgánom štátnej správy povinnosť spolupracovať s NBÚ pri vypracovaní národnej stratégie kybernetickej bezpečnosti a na tento účel poskytnúť NBÚ informácie v potrebnom rozsahu. Správny delikt podľa § 31 ods. 7 písm. a) ZoKB potom postihuje situáciu, keď adresát tejto povinnosti informácie neposkytne.

Subjekt v tomto prípade predstavuje veľmi špecifický okruh povinných. Zaväzuje ústredný orgán alebo iný orgán štátnej správy vystupujúci ako vykonávateľ verejnej správy v režime ZoKB. Ide teda o špeciálny subjekt. **Objektom** je ochrana riadneho výkonu koordinačných a koncepčných úloh štátu v kybernetickej bezpečnosti – najmä schopnosť NBÚ pripraviť stratégiu a plán reakcie na rozsiahle incidenty na základe relevantných a aktuálnych vstupov. **Objektívna stránka** spočíva v opomenutí poskytnúť požadované informácie po výzve NBÚ; na naplnenie deliktu postačuje samotné nesplnenie povinnosti (napr. neposkytnutie vôbec), bez potreby preukazovať následok vo forme konkrétnej škody. **Subjektívna stránka** je v tejto skutkovej podstate typicky objektivizovaná – zodpovednosť sa viaže na nesplnenie povinnosti adresovaného orgánu, pričom dôvody nečinnosti majú význam najmä pri posúdení závažnosti a individualizácii pokuty.

10.1.4.22 Neposkytnutie súčinnosti alebo informácií [§ 31 ods. 7 písm. b)]

Ide o procesný správny delikt, ktorým zákon zabezpečuje vynútiteľnosť spolupráce pri riešení kybernetického bezpečnostného incidentu. Podľa § 10a ods. 1 ZoKB sú orgán verejnej moci, PZS a právnická osoba v sektore podľa prílohy č. 1 alebo č. 2 povinní poskytnúť NBÚ požadovanú súčinnosť a informácie získané z vlastnej činnosti, ak sú nevyhnutné na zabezpečenie kybernetickej bezpečnosti a riešenie incidentu. Povinnosť je limitovaná tým, že poskytnutím informácií nesmie dôjsť k ohrozeniu úloh podľa osobitných predpisov ani spravodajských úloh a k odhaleniu zdrojov/prostriedkov či osôb; žiadosť NBÚ musí byť riadne odôvodnená a konkrétna (§ 10a ods. 2 ZoKB).

Subjektom je ktorýkoľvek z povinných subjektov podľa § 10a ods. 1. **Objektom** je ochrana riadneho výkonu pôsobnosti NBÚ a efektívneho riešenia incidentov. **Objektívna stránka** spočíva v neposkytnutí požadovanej súčinnosti alebo informácií (úplne, čiastočne,

oneskorene alebo mimo požadovaného rozsahu), čím sa sťaží alebo marí riešenie incidentu. **Subjektívna stránka** je typicky objektivizovaná; dôvody odmietnutia a miera zavinenia sa spravidla premietnu najmä do úvahy o závažnosti a výške pokuty.

10.1.4.23 Používanie zakázaného alebo obmedzeného produktu, služby, procesu alebo tretej strany [§ 31 ods. 7 písm. c)]

Tento správny delikt nadväzuje na osobitný mechanizmus riadenia rizika prostredníctvom štátneho zásahu do technologických závislostí. NBÚ môže rozhodnutím podľa § 27a ods. 1 ZoKB zakázať alebo obmedziť používanie konkrétneho produktu, procesu, služby alebo tretej strany na poskytovanie služby, ak ich používanie zásadne sťažuje udržanie kybernetickej bezpečnosti a ohrozuje chránené hodnoty (napr. život, hospodárske fungovanie štátu, verejný poriadok, bezpečnosť) alebo ohrozuje bezpečnostné záujmy SR. Rozhodnutie má osobitný režim: konanie sa oznamuje a zverejňuje, predchádza mu analýza rizík s medziinštitucionálnymi vstupmi a NBÚ je viazaný stanoviskom vlády (§ 27a ods. 2 až 3 ZoKB); rozhodnutie sa vyhlasuje v Zbierke zákonov a účinky nastávajú vyhlásením (§ 27a ods. 5 ZoKB).

Subjektom deliktu je PZS, ktorému § 27a ods. 4 ZoKB ukladá povinnosť zdržať sa používania alebo používanie obmedziť. **Objektom** je ochrana kybernetickej bezpečnosti a bezpečnostných záujmov štátu prostredníctvom eliminácie identifikovaných systémových rizík v dodávateľskom reťazci. **Objektívna stránka** spočíva v tom, že PZS napriek účinnému rozhodnutiu pokračuje v používaní zakázaného produktu/procesu/služby alebo tretej strany, prípadne nedodrží uložený rozsah obmedzenia; rozhodujúce je porušenie povinnosti podľa § 27a ods. 4 ZoKB, nie vznik incidentu. **Subjektívna stránka** je v zásade objektivizovaná.

10.1.4.24 Nepravdivé EÚ vyhlásenie o zhode pri vlastnom posúdení [§ 31 ods. 8]

Skutková podstata postihuje situáciu, keď výrobca alebo poskytovateľ produktov IKT, služieb IKT alebo procesov IKT vydá v režime *vlastného posúdenia zhody* EÚ vyhlásenie o zhode, ktoré je v rozpore s požiadavkami schémy certifikácie kybernetickej bezpečnosti prijatej Komisiou podľa čl. 49 ods. 7. Aktu o kybernetickej bezpečnosti. Vlastné posúdenie je pritom koncipované ako výnimka pre nízke riziko a stupeň dôveryhodnosti základný, pričom zodpovednosť za súlad nesie výlučne výrobca/poskytovateľ (čl. 53 ods. 1 a 2 ZoKB).

Subjektom deliktu je výrobca alebo poskytovateľ, ktorý vyhlásenie vydáva. Ide teda o špeciálny subjekt. **Objektom** je ochrana dôveryhodnosti európskeho certifikačného rámca a sekundárne ochrana kybernetickej bezpečnosti používateľov, ktorí sa na deklarovaný súlad spoliehajú. **Objektívna stránka** spočíva v samotnom vydaní vyhlásenia, hoci požiadavky schémy splnené nie sú (alebo nie sú preukázané v požadovanom rozsahu); vznik škody či incidentu nie je znakom deliktu, ale zvyšuje závažnosť. **Subjektívna stránka** nie je viazaná na úmysel; v praxi pôjde o objektivizovanú zodpovednosť za nesprávnu deklaráciu súladu, pričom miera zavinenia sa môže premietnuť najmä do výšky pokuty.

10.1.4.25 Nezverejnenie alebo neaktualizovanie doplňujúcich informácií o kybernetickej bezpečnosti [§ 31 ods. 9]

Skutková podstata nadväzuje na informačný režim orientovaný na koncových užívateľov v súvislosti s európskou certifikáciou: pri certifikovaných produktoch, službách a procesoch (alebo pri produktoch, pre ktoré bolo vydané EÚ vyhlásenie o zhode) sa nevyžaduje len počiatočné splnenie schémy, ale aj priebežná transparentnosť voči používateľom. Čl. 55 Aktu o kybernetickej bezpečnosti preto ukladá povinnosť zverejňovať v elektronickej podobe doplňujúce kybernetickobezpečnostné informácie (najmä odporúčania pre bezpečné používanie, trvanie bezpečnostnej podpory, kontakty a kanály na hlásenie zraniteľností a odkazy na registre zraniteľností a bezpečnostné upozornenia) a tieto informácie udržiavať dostupné a aktualizované prinajmenšom do skončenia platnosti certifikátu alebo EÚ vyhlásenia o zhode.

Subjektom deliktu je výrobca alebo poskytovateľ certifikovaného produktu/služby/procesu, prípadne výrobca alebo poskytovateľ produktu/služby/procesu, pre ktorý bolo vydané EÚ vyhlásenie o zhode. **Objektom** je ochrana informovanosti koncových užívateľov a z nej odvodená schopnosť bezpečnej konfigurácie, prevádzky a údržby, ako aj funkčnosť ekosystému koordinovaného oznamovania a riešenia zraniteľností.

Objektívna stránka spočíva buď v nezverejnení požadovaných doplňujúcich informácií v elektronickej podobe, alebo v ich neudržiavaní v aktuálnom stave (napr. neaktualizovanie údajov o podpore či odkazov na registre zraniteľností), hoci povinnosť trvá počas platnosti certifikátu/vyhlásenia. **Subjektívna stránka** nie je viazaná na úmysel; ide o objektivizovanú zodpovednosť za porušenie informačnej povinnosti, pričom prípadné zavinenie sa typicky prejaví najmä pri individualizácii výšky pokuty.

10.1.4.26 Nesplnenie informačnej povinnosti a marenie auditu vo vzťahu k národnej autorite pre certifikáciu [§ 31 ods. 10 písm. a) a b)]

Táto skutková podstata nadväzuje na minimálne dohľadové právomoci národnej autority pre certifikáciu kybernetickej bezpečnosti podľa čl. 58 ods. 8 Aktu o kybernetickej bezpečnosti. V zákone sa vytvára procesná „vynútiteľnosť" dohľadu nad certifikačným režimom: na jednej strane prostredníctvom povinnosti poskytnúť autorite informácie potrebné na plnenie jej úloh (písm. a), na druhej strane prostredníctvom zákazu marenia vyšetrovania v podobe auditu (písm. b).

Subjektom deliktu je špeciálny okruh regulovaných osôb – orgán posudzovania zhody, držiteľ európskeho certifikátu kybernetickej bezpečnosti alebo vydavateľ EÚ vyhlásenia o zhode. **Objektom** je ochrana účinného výkonu dohľadu nad certifikáciou, t. j. schopnosť štátu a príslušnej autority overovať dodržiavanie pravidiel schém certifikácie a udržiavať dôveryhodnosť vydaných certifikátov a vyhlásení. **Objektívna stránka pri písm. a)** spočíva v neposkytnutí požadovaných informácií, ktoré národná autorita potrebuje na plnenie svojich úloh (typicky odmietnutie, neúplné alebo oneskorené poskytnutie, prípadne poskytnutie informácií v rozsahu, ktorý neumožňuje reálne vykonať dohľad). **Pri písm. b)** ide o znemožnenie vedenia vyšetrovania v podobe auditu – teda konanie alebo opomenutie, ktorým sa audit autority fakticky zablokuje alebo stane neuskutočniteľným (napr. odmietnutie prístupu k podkladom, priestorom, systémom či dokumentácii, alebo iné procesné marenie kontrolného úkonu). Následok nie je konštrukčným znakom; postačuje samotné porušenie povinnosti, pričom intenzita zásahu do dohľadu sa prejaví najmä pri hodnotení závažnosti a pri individualizácii pokuty. **Subjektívna stránka** je pri tejto skutkovej podstate typicky objektivizovaná: zodpovednosť sa viaže na neplnenie povinností spolupráce a strpenia dohľadu, pričom miera zavinenia (ak sa v konkrétnej veci hodnotí) má praktický význam najmä pri určovaní výšky sankcie a pri posúdení, či išlo o izolované zlyhanie alebo o systematické marenie dohľadu.

10.1.4.27 Neumožnenie prístupu do priestorov pre účely dohľadu [§ 31 ods. 11]

Tento správny delikt nadväzuje na osobitnú vyšetrovaciu právomoc národnej autority pre certifikáciu kybernetickej bezpečnosti získať prístup do priestorov orgánov posudzovania zhody alebo držiteľov európskych certifikátov kybernetickej bezpečnosti na účely

vykonávania vyšetrovaní v súlade s procesným právom Únie alebo členského štátu (čl. 58 ods. 8 písm. d) Aktu o kybernetickej bezpečnosti). Zmyslom skutkovej podstaty je zabezpečiť, aby dohľad nad certifikačným režimom neostal formálny, ale bol reálne vykonateľný aj v situáciách, keď je potrebné preveriť súlad v prostredí kontrolovaného subjektu.

Subjektom deliktu je špeciálny okruh osôb – orgán posudzovania zhody alebo držiteľ európskeho certifikátu kybernetickej bezpečnosti. **Objektom** je ochrana účinného výkonu verejného dohľadu nad certifikáciou, najmä možnosti národnej autority vykonávať preverenia na mieste a tým udržiavať dôveryhodnosť a integritu systému certifikácie kybernetickej bezpečnosti. **Objektívna stránka** spočíva v tom, že povinný subjekt národnej autorite neumožní prístup do priestorov v rozsahu potrebnom na vykonanie vyšetrovania; môže ísť o priame odmietnutie vstupu, vytváranie prekážok, podmieňovanie prístupu neodôvodnenými požiadavkami alebo iné konanie, ktoré prístup fakticky znemožní alebo zmarí. Následok nie je konštrukčným znakom deliktu; postačuje samotné neumožnenie prístupu, pričom intenzita marenia sa premietne najmä do hodnotenia závažnosti a výšky pokuty. **Subjektívna stránka** je typicky objektivizovaná: zodpovednosť sa viaže na porušenie povinnosti strpieť kontrolný úkon, pričom prípadné dôvody odmietnutia alebo miera zavinenia môžu mať význam predovšetkým pri individualizácii sankcie.

10.2 Zákon o informačných technológiách vo verejnej správe

ZoITVS vytvára osobitný regulačný rámec, v ktorom sa administratívnoprávna zodpovednosť viaže na správu, prevádzku a rozvoj informačných technológií verejnej správy. Ťažiskom nie je „jednorazové" porušenie izolovanej povinnosti, ale dlhodobé riadenie životného cyklu ITVS v súlade so zásadami transparentnosti, proporcionality a hospodárnosti, s národnou koncepciou a so štandardmi.

Zodpovednostný režim je konštruovaný ako cyklus:

1. plánovanie a koncepcia rozvoja,
2. obstarávanie a implementácia,
3. prevádzka (bezpečnosť, kontinuita, služby),
4. zverejňovanie a metainformačné povinnosti,
5. kontrola a náprava,
6. sankcia.

ZoITVS pracuje s osobitnou štruktúrou subjektov. Kľúčové je rozlíšenie **orgánu vedenia** - MIRRI SR a **orgánov riadenia** (široko vymedzený okruh subjektov verejnej správy), ktoré vystupujú ako **správcovia ITVS**; popri tom zákon pozná aj **prevádzkovateľa** určeného správcom alebo osobitným predpisom, pričom určenie prevádzkovateľa nezbavuje správcu zodpovednosti za plnenie zákonných povinností. **Zodpovednosť je teda viazaná na „správcovstvo" a na riadiace kompetencie nad ITVS**, nie na všeobecný okruh osôb. Súčasne zákon explicitne vymedzuje vecné a bezpečnostné výnimky (napr. obrana, bezpečnosť štátu, utajované skutočnosti) a deklaruje koexistenciu s režimami kybernetickej bezpečnosti (správcovia, ktorí sú PZS alebo poskytovateľmi digitálnej služby, týmto zákonom o svoje osobitné povinnosti neprichádzajú).

Didakticky je vhodné vnímať všeobecný objekt ochrany ZoITVS ako ochranu:

1. plynulej, bezpečnej a spoľahlivej prevádzky ITVS,
2. efektívneho a hospodárneho nakladania s verejnými zdrojmi v IT,
3. interoperability a integrovaného prostredia ITVS podľa spoločných princípov a štandardov,
4. transparentnosti a kontrolovateľnosti správy ITVS (vrátane metainformačných a zverejňovacích povinností), a
5. riadenia rizík, kvality a bezpečnosti v prevádzke.

Vzťah ZoKB a ZoITVS je vzťahom funkčného prekryvu, nie úplnej hierarchie *lex generalis – lex specialis* v celom rozsahu. ZoKB upravuje všeobecný regulačný rámec riadenia a zabezpečenia kybernetickej bezpečnosti (bezpečnostné opatrenia, hlásenia incidentov, reakcie, dohľad, certifikácia, národné politiky a koordinácia), teda predstavuje prierezový bezpečnostný režim naprieč sektormi a typmi subjektov. ZoITVS koncentruje úpravu na organizáciu správy informačných technológií verejnej správy, na práva a povinnosti orgánu vedenia a orgánov riadenia a na základné požiadavky kladené na ITVS a na jej správu; ide teda o rámec organizačno-riadiacich pravidiel pre verejnú správu, s výnimkami pre obranu, bezpečnosť a utajované/limitované/citlivé informácie (§ 1 ods. 2 ZoITVS).

Kľúčové je explicitné koordinačné pravidlo v § 1 ods. 3 ZoITVS: zákon sa vzťahuje aj na správcov, ktorí sú zároveň PZS alebo poskytovateľmi digitálnej služby podľa zákona o KB, pričom ich povinnosti a oprávnenia podľa ZoKB týmto nie sú dotknuté. Z toho vyplýva, že dotykové plochy sa riešia kumulatívnou aplikáciou: ZoITVS upravuje najmä „ako" má verejná správa informačné technológie organizovať, spravovať a riadiť, kým ZoKB určuje „aké"

bezpečnostné povinnosti musia byť splnené v kybernetickej bezpečnosti a aké sú mechanizmy dohľadu a sankcionovania. V oblasti kybernetickej bezpečnosti preto ZoITVS pôsobí ako *lex specialis* len v tom zmysle, že pre prostredie verejnej správy špecifikuje správne a organizačné povinnosti pri ITVS; bezpečnostné jadro (opatrenia, incidenty, audit, dohľad) však zostáva primárne v režime ZoKB, ktorý sa vo verejnej správe uplatní popri ZoITVS, nie namiesto neho.

Ujasnenie tohto režimu fungovania medzi ZoKB a ZoIVTS je kľúčové pre predchádzanie kompetenčným konfliktom, ktoré by mohli vznikať pri výkone verejnej moci realizovanej NBÚ na pôdoryse ZoKB a výkone verejnej moci realizovanej MIRRI SR na pôdoryse ZoIVTS.

Metodologicky nadväzujeme na postup zo ZoKB, no prispôsobujeme ho § 29 ZoITVS, ktorý je prevažne blanketový. Východiskom preto nie je „jeden skutok", ale najprv identifikácia konkrétnej porušenej povinnosti a jej zaradenie do tematického okruhu správy ITVS (koncepčno-riadiaci, projektový, prevádzkový, bezpečnostný, informačno-transparentnostný) a do fázy životného cyklu ITVS. Až následne povinnosť subsumujeme pod konkrétne ustanovenie ZoITVS. Pri každom delikte používame jednotnú mapu znakov skutkovej podstaty (objekt – subjekt – objektívna stránka – subjektívna stránka), s dôrazom na presné určenie adresáta povinnosti (správca / orgán riadenia / prevádzkovateľ ISVS / osvedčujúca osoba). Subjektívna stránka nie je viazaná na úmysel; rozhoduje porušenie povinnosti, kým okolnosti sa premietajú najmä do správnej úvahy o pokute podľa § 29 ods. 3 ZoITVS.

10.2.1 Správne delikty

Ustanovenie § 29 ZoITVS vytvára jednotný sankčný rámec správnych deliktov, pričom sankciou je výlučne pokuta. Zákonodarca zároveň diferencuje sankčné rozpätia podľa povahy adresáta a typu povinnosti:

- **pri najzávažnejších porušeniach** povinností správcu (najmä v oblasti základných povinností správy ITVS a bezpečnosti ITVS) je pokuta v rozpätí 500 až 35 000 eur (§ 29 ods. 1 písm. a) ZoITVS);
- pri informačných, koncepčných a odpisových povinnostiach a pri osobitných povinnostiach prevádzkovateľa informačných systémov verejnej správy je rozpätie 250 až 35 000 eur (§ 29 ods. 1 písm. b) ZoITVS);

- pri povinnostiach interoperability, súčinnosti, projektovej disciplíny, štandardov a vybraných obmedzení je rozpätie 250 až 25 000 eur (§ 29 ods. 1 písm. c) ZoITVS); a napokon
- pri „zvyškových" povinnostiach orgánu riadenia alebo osvedčujúcej osoby, ktoré nie sú pokryté písm. a) až c), je pokuta 125 až 5 000 eur (§ 29 ods. 1 písm. d) ZoITVS).

Táto stupňovitá konštrukcia je metodicky významná: už pri kvalifikácii deliktu núti správny orgán presne identifikovať porušenú povinnosť a správne ju zaradiť pod príslušné písmeno, keďže od toho sa odvíja nielen právna kvalifikácia, ale aj horná hranica sankcie. Konanie o uložení pokuty sa vedie podľa **Správneho poriadku** (§ 29 ods. 2 ZoITVS), pričom zákon stanovuje aj osobitné kritériá správnej úvahy pri ukladaní sankcie: orgán vedenia prihliada na závažnosť, spôsob, trvanie a následky protiprávneho konania, ako aj na opakované porušenie alebo porušenie viacerých povinností (§ 29 ods. 3 ZoITVS). Takýto koncept nadväzuje na tradičný priestupkový model ukladania sankcie tým, že stavia na individualizácii podľa závažnosti a typových kritérií (spôsob, následky). Súčasne ho prispôsobuje regulácii správy ITVS: dopĺňa trvanie, explicitne pracuje s opakovanosťou a kumuláciou porušení a pridáva nápravný korektív v podobe možnosti upustenia od pokuty, ktorý je v rámci správneho trestania upravený v § 11 ods. 3 PriesZ – tento inštitút posilňuje preventívno-nápravný rozmer sankčného mechanizmu. Keďže ZoITVS upravuje správne delikty v zásadách ukladania sankcií absentujú prvky viazané na fyzickú osobu (zavinenie, pohnútky, osobné pomery) a reflexia disciplinárneho/kárneho postihu, čo zodpovedá odlišnému charakteru adresátov a objektivizovanejšiemu typu zodpovednosti v ITVS.

Z hľadiska lehôt je pokuta splatná do 15 dní od právoplatnosti rozhodnutia (§ 29 ods. 4 ZoITVS) a možno ju uložiť najneskôr do troch rokov odo dňa porušenia povinnosti (§ 29 ods. 6 ZoITVS), čím zákon zavádza prekluzívnu hranicu zodpovednosti, ktorú musí orgán vedenia v každom prípade rešpektovať.

10.2.1.1 Porušenia povinností správcu v životnom cykle ITVS [§ 29 ods. 1 písm. a)]

Ustanovenie § 29 ods. 1 písm. a) ZoITVS v spojení s § 6 ods. 1, § 12 ods. 1 písm. a), § 14 ods. 6, § 15 ods. 2, § 16 ods. 3 písm. e) a § 19 až 21, § 23, § 23a ZoITV konštruuje správny delikt ako typický blanketový delikt: zákon neformuluje vlastné zakázané konanie, ale viaže zodpovednosť na porušenie katalógu povinností rozptýlených v základnej, prevádzkovej, zmluvnej, obstarávacej a bezpečnostnej časti zákona. Didakticky preto pristupujeme k

tomuto deliktu „od mapy povinností k znakom skutkovej podstaty": najprv identifikujeme, do ktorého tematického okruhu patrí porušená povinnosť, a až následne ju subsumujeme pod všeobecnú skutkovú podstatu § 29 ods. 1 písm. a) ZoITVS.

Z hľadiska obsahu možno povinnosti zahrnuté pod § 29 ods. 1 písm. a) ZoITVS prehľadne zoskupiť na:

1. zásady správy informačných technológií verejnej správy (§ 6 ods. 1 ZoITVS – transparentnosť, proporcionalita, hospodárnosť a efektívnosť);
2. prevádzkovú povinnosť zabezpečiť plynulú, bezpečnú a spoľahlivú prevádzku vrátane ochrany proti zneužitiu (§ 12 ods. 1 písm. a ZoITVS);
3. zmluvno-službový režim (identifikácia a zoznam služieb, definovanie úrovní poskytovania, monitoring, hodnotenie a zverejňovanie údajov v centrálnom metainformačnom systéme – § 14 ods. 6 ZoITVS);
4. povinnosti vo fáze prípravy a obstarávania projektu, vrátane kľúčových zmluvných podmienok (najmä otvorenie zdrojového kódu v určenom rozsahu, výhradná dispozícia s informáciami a súčinnosť pri zmene dodávateľa – § 15 ods. 2 ZoITVS);
5. riadenie prevádzky prostredníctvom systémov na správu problémov, servisných a zmenových požiadaviek vrátane oznamovania pripravovaných zmien orgánu vedenia (§ 16 ods. 3 písm. e ZoITVS) a
6. osobitný bezpečnostný režim informačných technológií verejnej správy (systém riadenia informačnej bezpečnosti, bezpečnostná dokumentácia, riadiace/ výkonné/ kontrolné zložky, identifikácia aktív a riadenie rizík, bezpečnostné opatrenia, bezpečnostné testovanie, audity, bezpečnostný projekt a súvisiace kompetencie a súčinnosť – § 19 až 21, § 23 a § 23a ZoITVS).

Objektom deliktu je ochrana riadnej správy informačných technológií verejnej správy v materiálnom zmysle: zákonnosť, transparentnosť a hospodárnosť postupov pri správe ITVS, kontinuita a spoľahlivosť prevádzky, ako aj udržanie bezpečnosti ITVS prostredníctvom bezpečnostnej dokumentácie, procesov riadenia rizík, kontroly a auditu. Sekundárne sa chráni aj dôveryhodnosť poskytovania služieb verejnej správy a schopnosť orgánu vedenia vykonávať svoju koordinačnú a metodickú funkciu na základe porovnateľných a overiteľných informácií o stave služieb a bezpečnosti.

Subjektom deliktu je správca v zmysle zákona. Pri aplikácii § 29 ods. 1 písm. a) ZoITVS je však rozhodujúce vždy presne určiť adresáta konkrétnej porušenej povinnosti: niektoré

povinnosti sú výslovne uložené orgánu riadenia (§ 12 ods. 1 písm. a) ZoITVS), iné sa viažu na správcu pri nastavení zmluvných vzťahov alebo prevádzkových procesov (§ 14 ods. 6, § 15 ods. 2, § 16 ods. 3 písm. e) ZoITVS), a bezpečnostný režim (§ 19 až 21, § 23, § 23a ZoITVS) operuje s interným rozčlenením úloh a zodpovedností v rámci organizácie správcu. Prakticky to znamená, že delikt nie je možné kvalifikovať abstraktne: v rozhodnutí musí byť presne definované, ktorá konkrétna povinnosť bola porušená a ktorému subjektu ju ZoITVS ukladá.

Objektívna stránka spočíva v porušení niektorej z povinností, na ktoré § 29 ods. 1 písm. a) ZoITVS odkazuje. Typové formy porušenia sa v praxi prejavia najmä ako:

1. neprijatie alebo nezavedenie požadovaného postupu či systému (napr. nezavedenie systému riadenia prevádzkových problémov a zmenových požiadaviek podľa § 16 ods. 3 písm. e) ZoITVS); nezavedenie systému riadenia informačnej bezpečnosti podľa § 19 ods. 1 ZoITVS;
2. nedodržanie zákonného princípu alebo povinného postupu (napr. postup nezlučiteľný s princípom transparentnosti, s princípom proporcionality či princípu hospodárnosti a efektívnosti podľa § 6 ods. 1 písm. a) ZoITVS);
3. nesplnenie prevádzkovej povinnosti zabezpečiť plynulú, bezpečnú a spoľahlivú prevádzku (vrátane ochrany proti zneužitiu) podľa § 12 ods. 1 písm. a) ZoITVS;
4. neudržiavanie zmluvného režimu (neidentifikovanie služieb, nedefinovanie úrovní poskytovania, nemonitorovanie alebo nezverejnenie údajov podľa § 14 ods. 6 ZoITVS);
5. neakceptovanie alebo obídenie povinných zmluvných podmienok vo fáze obstarávania (§ 15 ods. 2 ZoITVS); alebo
6. nesplnenie bezpečnostných povinností v plánovaní, implementácii a prevádzke (bezpečnostná dokumentácia, testovanie, audity, bezpečnostný projekt – § 19 až 21 a § 23 ZoITVS).

Následok nie je konštrukčným znakom skutkovej podstaty; podstatné je porušenie povinnosti. Praktické dopady (napr. zníženie bezpečnosti, narušenie kontinuity služieb, sťaženie kontroly alebo porovnateľnosti údajov) však majú význam pri hodnotení závažnosti a individualizácii pokuty.

Subjektívna stránka nie je v texte tejto skutkovej podstaty viazaná na úmysel. Pri tomto type správnych deliktov sa preto v aplikačnej praxi uplatňuje objektivizovaný prístup: zodpovednosť sa viaže na porušenie konkrétnej povinnosti, kým miera zavinenia (ak sa v

konkrétnej veci hodnotí) sa spravidla prejaví najmä v úvahe o výške pokuty, a to najmä podľa toho, či ide o izolované pochybenie alebo o systémové zlyhanie správy a bezpečnostných procesov.

Aplikačne možno kvalifikáciu deliktu metodicky viesť v šiestich krokoch:

1. zaradiť zistenie do tematického okruhu (1. – 6.);
2. identifikovať presné ustanovenie a obsah porušenej povinnosti;
3. určiť adresáta povinnosti (orgán riadenia / správca / orgán vedenia v rozsahu jeho úloh);
4. skutkovo popísať spôsob porušenia (konanie alebo opomenutie, čas, rozsah);
5. preukázať porušenie relevantnými podkladmi (dokumentácia, záznamy, výstupy z centrálneho metainformačného systému, interné procesy, bezpečnostné dokumenty, výsledky testovania alebo auditu);
6. vyhodnotiť závažnosť podľa trvania, rozsahu a praktických dopadov a tomu prispôsobiť výmeru pokuty.

10.2.1.2 Nesplnenie informačných, koncepčných a odpisových povinností [§ 29 ods. 1 písm. b)]

Ustanovenie § 29 ods. 1 písm. b) ZoITVS v spojení s § 12 ods. 1 písm. b), g), h), § 13, § 14 ods. 3, § 15 ods. 11 a § 26 ods. 2, 6, 7 ZoITVS spája dve skupiny povinností:

1. **povinnosti orgánu riadenia/správcu** smerom k transparentnosti a funkčnosti informatizácie (sprístupňovanie a aktualizácia informácií v centrálnom metainformačnom systéme, poskytovanie elektronických odpisov a výstupov, zabezpečenie dostupnosti ITVS na elektronickú komunikáciu), a
2. **povinnosti prevádzkovateľa informačného systému verejnej správy** pri vydávaní elektronických odpisov a výstupov (najmä bezpečný prenos, ochrana obsahu a zisťovanie totožnosti).

Zároveň ustanovenie pokrýva aj **strategickú rovinu** – vypracovanie, predkladanie, priebežné posudzovanie a aktualizovanie koncepcie rozvoja a súčinnosť pri jej tvorbe a uskutočňovaní.

Objektom je riadny výkon verejnej správy v digitálnom prostredí: aktuálnosť a použiteľnosť informácií o ITVS a e-službách, dostupnosť ITVS pre elektronickú komunikáciu, právna istota a praktická využiteľnosť elektronických odpisov a výstupov, ako aj plánovitosť

a koordinácia rozvoja ITVS prostredníctvom koncepcie rozvoja v súlade s národnou koncepciou.

Subjektom sú dva alternatívne okruhy:

1. **Správca** (resp. orgán riadenia v postavení správcu) pri porušení povinností podľa § 12 ods. 1 písm. b), g), h) ZoITVS, pri povinnosti vypracovať a udržiavať koncepciu rozvoja (§ 13 a nadväzujúce ustanovenia ZoITVS) a pri povinnosti spolupráce podľa § 14 ods. 3 ZoITVS (a ďalších odkazovaných povinnostiach).
2. **Prevádzkovateľ** informačného systému verejnej správy pri porušení povinností podľa § 26 ods. 2, 6 alebo 7 ZoITVS, teda v rámci režimu vydávania elektronických odpisov a výstupov.

Objektívna stránka spočíva v porušení konkrétnej povinnosti typicky v:

1. nesprístupnení alebo neaktualizovaní údajov o ITVS a e-službách cez centrálny metainformačný systém (§ 12 ods. 1 písm. b) ZoITVS);
2. neposkytovaní elektronických odpisov/výstupov na účely podľa osobitných predpisov (§ 12 ods. 1 písm. g) ZoITVS);
3. nezabezpečení dostupnosti ITVS pre elektronickú komunikáciu (§ 12 ods. 1 písm. h) ZoITVS);
4. nevypracovaní, nepredložení na schválenie, neaktualizovaní alebo neplnení priebežného posudzovania súladu koncepcie rozvoja (§ 13 ZoITVS); alebo
5. nesplnení povinnosti spolupráce pri tvorbe a uskutočňovaní koncepcie (§ 14 ods. 3 ZoITVS).

Pri prevádzkovateľovi informačných systémov verejnej správy ide najmä o:

1. porušenie povinnosti odoslať osvedčujúcej osobe elektronický odpis v predpokladanej forme (§ 26 ods. 2 ZoITVS);
2. odoslanie bez primeranej ochrany obsahu pri neverejných častiach informačných systémov verejnej správy (§ 26 ods. 6 ZoITVS); alebo
3. nezistenie totožnosti žiadateľa, ak to vyžaduje osobitný predpis (§ 26 ods. 7 ZoITVS).

Následok nie je konštrukčným znakom deliktu; význam má najmä pri úvahe o závažnosti a výmere pokuty (napr. sťaženie využívania e-služieb, zníženie právnej istoty odpisov, riziko neoprávneného prístupu).

Subjektívna stránka nie je viazaná na úmysel; v praxi ide o objektivizovaný režim, kde sa zodpovednosť odvíja od nesplnenia povinnosti a miera zavinenia sa spravidla zohľadňuje

až pri individualizácii sankcie (najmä pri opakovaných alebo systémových zlyhaniach procesov správy ITVS).

10.2.1.3 Porušenie povinností interoperability, súčinnosti a projektovej disciplíny [§ 29 ods. 1 písm. c)]

Skutková podstata je „zhluková": pod jednu sankčnú klauzulu zhromažďuje povinnosti z viacerých oblastí (sprístupňovanie a zdieľanie údajov, číselníky, projektové riadenie, pripravenosť na incidenty, štandardy a cloudové obmedzenia). Spoločným menovateľom je **cieľ, aby ITVS fungovali ako koordinované a prevádzkovo spoľahlivé prostredie, v ktorom orgány verejnej moci vedia zákonne využívať údaje, poskytovať ich iným orgánom a realizovať projekty kontrolovateľným spôsobom**. ZoITVS používa pojem *elektronická služba verejnej správy* (§ 8 ods. 2 ZoITVS) a nadväzne operuje s informáciami o ITVS a poskytovaných elektronických službách (porov. aj § 12 ods. 1 písm. b), § 13a ods. 2 ZoITVS).

Objektom deliktu je riadna správa ITVS ako verejnoprávneho systému, najmä:

1. dostupnosť a zdieľateľnosť údajov v zákonnom režime;
2. transparentná a aktuálna evidencia a metainformačný rámec (číselníky);
3. kontrolovateľná a hospodárna realizácia projektov;
4. prevádzková odolnosť pri incidentoch a
5. unifikácia postupov prostredníctvom štandardov (vrátane režimu vládneho cloudu).

Subjekt je diferencovaný podľa adresáta povinnosti:

1. **správca**, ak poruší § 12 ods. 1 písm. e) alebo f) ZoITVS alebo povinnosť dodržiavať štandardy;
2. **orgán riadenia, ak poruší** § 8 ods. 2, § 12 ods. 1 písm. c) alebo j), § 15 ods. 4 písm. d) alebo e), § 16 ods. 3 písm. d) alebo § 24a ods. 5 ZoITVS;
3. **orgán riadenia, ak opakovane poruší** § 13a ods. 2 ZoITVS a nevykoná nápravu ani po výzve orgánu vedenia.

Metodicky je preto kľúčové vždy určiť, v akej „role" subjekt vystupuje, ktorú konkrétnu povinnosť porušil a či nedochádza zo strany subjektu k recidíve.

Objektívna stránka spočíva v porušení konkrétnej povinnosti (konaním alebo opomenutím). Typicky ide o:

1. **nesprístupnenie údajov** verejnosti (§ 12 ods. 1 písm. e) ZoITVS) alebo **nezabezpečenie ich dostupnosti** iným orgánom verejnej moci a bezodplatné sprístupnenie/poskytnutie (§ 12 ods. 1 písm. f) ZoITVS);
2. **neposkytnutie súčinnosti** orgánu vedenia a neposkytnutie údajov cez elektronickú službu verejnej správy (§ 8 ods. 2 ZoITVS), porušenia pri číselníkoch (§ 12 ods. 1 písm. c) ZoITVS) alebo **nenahlásenie zmien** úsekov a agend (§ 12 ods. 1 písm. j) ZoITVS);
3. **porušenie projektovej disciplíny** – nerozdelenie veľkého projektu na čiastkové plnenia so zákonnými parametrami alebo začatie realizácie bez schválenia orgánom vedenia (§ 15 ods. 4 písm. d), e) ZoITVS);
4. **nezabezpečenie informácií** pre náhradné riešenie dostupnosti pri prevádzkovom incidente (§ 16 ods. 3 písm. d) ZoITVS);
5. **nedodržanie štandardov**, osobitne režimu, keď možno v určitých konaniach odoberať len vládne cloudové služby (§ 24a ods. 5) ZoITVS);
6. **opakované neposkytnutie súčinnosti** pri vytváraní a poskytovaní elektronických služieb v rámci „životnej situácie" podľa § 13a ods. 2 ZoITVS spojené s nevykonaním nápravy ani po výzve (bod 3).

Subjektívna stránka nie je viazaná na úmysel; v praxi ide spravidla o objektivizované porušenie povinnosti, pričom miera zavinenia a najmä opakovanosť (v bode 3 aj ako kvalifikačný prvok) sa uplatní pri posúdení závažnosti a uložení pokuty.

10.2.1.4 „Zvyškový" správny delikt – porušenie inej povinnosti podľa zákona [§ 29 ods. 1 písm. d)]

Ustanovenie § 29 ods. 1 písm. d) ZoITVS plní v sankčnom systéme reziduálnu funkciu: umožňuje postihnúť porušenia povinností, ktoré zákon adresuje orgánu riadenia alebo osvedčujúcej osobe, no ktoré nie sú výslovne zahrnuté do katalógov v § 29 ods. 1 písm. a) až c) ZoITVS. Nejde teda o „voľnú" generálnu klauzulu, ale o záchytné ustanovenie viazané na presne identifikovateľnú zákonnú povinnosť; v rozhodnutí musí byť vždy explicitne pomenované, ktorá konkrétna povinnosť podľa zákona bola porušená a prečo nepatrí pod písmená a) až c).[750] Okruh zvyškových povinností vieme preto vymedziť:

[750] Didaktická poznámka k metodike: pri § 29 ods. 1 písm. d) ZoITVS je najvyššie riziko „neurčitosti" v odôvodnení rozhodnutia. Preto odporúčame pri každom použití tejto skutkovej podstaty uviesť v texte aspoň stručnú vetu typu: *„porušená povinnosť nie je zahrnutá do katalógov podľa § 29 ods. 1 písm. a) až c), keďže …"*, aby bola zjavná zákonnosť subsumpcie a zachovaná zásada určitého vymedzenia skutku.

- **negatívne** – správnym deliktom podľa tohto ustanovenia nie je správny delikt, ktorý je uvedený v § 28 ods. 1 písm. a) až c) ZoITVS a
- **pozitívne** – správnym deliktom podľa tohto ustanovenia je každá povinnosť, ktorá ako správny delikt nie je ustanovená v § 28 ods. 1 písm. a) až c) ZoITVS.

Objektom deliktu je ochrana riadneho výkonu správy ITVS a súvisiacich procesov, ktoré ZoITVS osobitne viaže na orgán riadenia a osvedčujúcu osobu, najmä zachovanie zákonnosti, spoľahlivosti a predvídateľnosti postupov, ktoré podporujú elektronické procesy verejnej správy. V porovnaní s písm. a) až c) ide typicky o povinnosti „doplnkové" alebo špecifické, ktoré však môžu mať významné dopady na použiteľnosť a dôveryhodnosť elektronických výstupov a postupov.

Subjektom je orgán riadenia alebo osvedčujúca osoba; okruh subjektov je teda užší než pri písm. a) až c) a je daný priamo textom skutkovej podstaty. Pri subsumpcii je rozhodujúce overiť, či povinnosť, ktorá mala byť porušená, je adresovaná práve jednému z týchto dvoch subjektov.

Objektívna stránka spočíva v porušení „inej povinnosti podľa zákona" – konaním alebo opomenutím. Keďže skutková podstata je reziduálna, pre jej naplnenie sú kľúčové tri kroky:

1. **presné určenie povinnosti** (ustanovenie, obsah, adresát);
2. **skutkové vymedzenie porušenia** (čo sa malo vykonať, čo sa vykonalo/nevykonalo, kedy a v akom rozsahu);
3. **negatívne vylúčenie,** že nejde o povinnosť subsumovateľnú pod písm. a) až c).

Následok nie je konštrukčným znakom; praktické dopady sa uplatnia najmä pri úvahe o závažnosti v rámci relatívne nižšieho sankčného rozpätia.

Subjektívna stránka nie je viazaná na úmysel. V aplikačnej praxi sa preto uplatní objektivizovaný prístup: zodpovednosť sa viaže na samotné porušenie povinnosti, pričom miera zavinenia a okolnosti prípadu majú význam najmä pri individualizácii pokuty.

11. MEDZINÁRODNOPRÁVNE ASPEKTY KYBERNETICKEJ BEZPEČNOSTI

11.1 Bezpečnosť štátu v kontexte kybernetických operácií

Pre skúmanie medzinárodnoprávnych aspektov kybernetickej bezpečnosti je potrebné vychádzať z toho, že zvrchovanosť štátu sa rozširuje aj na kyberneticky priestor[751]. Napriek tomu, že kybernetický priestor sa vníma ako nehmotný, zvrchovanosť štátu vyplýva predovšetkým z výkonu zvrchovanosti nad fyzickou kybernetickou infraštruktúrou.
Aktivity v kybernetickom priestore podliehajú regulácii štátu. Pri protiprávnych aktivitách v kybernetickom priestore je relevantné rozlišovanie pôvodcu a intenzity kybernetických aktivít.

Z hľadiska pôvodcu je možné kybernetické operácie rozlíšiť na kybernetické operácie pripísateľné štátu a na kybernetické operácie, ktoré pripísateľné štátu nie sú.

Pripísateľnosť je jedným z predpokladov zodpovednosti štátu za protiprávnu kybernetickú aktivitu. V tomto ohľade je potrebné pamätať aj na existenciu jurisdikčných imunít štátu, čo má význam pre výber justičného fóra, respektíve metódy riešenia sporov.
Z hľadiska intenzity môže ísť o kybernetické operáciu, ktorých škodlivosť dosahuje intenzitu ozbrojeného útoku a na kybernetické operácie, ktoré nedosahujú takúto intenzitu. V tomto ohľade bude potrebné skúmať aplikáciu osobitného právneho režimu - medzinárodného humanitárneho práva[752], ako aj možnosť aplikovania inštitútu sebaobrany štátu v zmysle čl. 51 Charty OSN, prípadne osobitných dojednaní ako je čl. 5 Severoatlantickej zmluvy[753].

Medzinárodné právo priznáva štátom nielen oprávnenie regulovať činnosť v kybernetickom priestore a brániť ho proti neoprávneným zásahom zo strany iných štátnych alebo neštátnych entít, ale stanovuje aj limity na tieto opatrenia, ktoré vyplývajú z Charty

[751] Porovnaj Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, bod. 20.
[752] ICRC: International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC position paper, November 2019. Online: https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf. GISEL, Laurent – RODENHÄUSER, Tilman – DÖRMANN, Knut: Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. International Review of the Red Cross (2020), 102 (913), 287–334. Online: https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/twenty-years-ihl-effects-of-cyber-operations-during-armed-conflicts-913.pdf.
[753] NATO: Wales Summit Declaration, 05 September 2014, body 72-73; NATO: Brussels Summit Communiqué, 14 June 2021, bod 32.

OSN,[754] medzinárodného práva ľudských práv a iných relevantných medzinárodnoprávnych noriem. Významným prameňom orientácie sa v tejto oblasti medzinárodného práva, ktorá ešte nie je ustálená vo všetkých svojich aspektoch, je **Tallinský manuál**[755], ktorý vypracovala skupina expertov pod záštitou NATO Cooperative Cyber Defence Centre of Excellence. Nejde o právne záväzný dokument, ale o expertný doktrinálny dokument, ktorého význam spočíva aj v snahe slúžiť ako vodítko pre zosúladenie odlišných pozícií štátov pri prístupe k rozličným aspektom. Vo veľkej miere táto kapitola reflektuje expertnú pozíciu Tallinského manuálu, avšak je potrebné mať na pamäti, že pri konkrétnej otázke môže byť pozícia toho-ktorého štátu odlišná a týmto manuálom právne viazaný nie je.

Popri zodpovednosti štátu môže kybernetická aktivita založiť aj zodpovednosť jednotlivca. Zodpovednosť jednotlivca môže byť medzinárodnoprávna a vnútroštátna. V prípade, ak ide o konanie jednotlivca, ktorého konanie je štátu pripísateľné, tak je potrebné skúmať aj otázku procesných imunít. Medzinárodnoprávna trestná zodpovednosť jednotlivca je založená v prípade, ak protiprávnou kybernetickou aktivitou bola naplnená skutková podstata zločinu podľa medzinárodného práva. Ak nedošlo k jej naplneniu, stále môže byť jednotlivec trestne zodpovedný, a to z titulu porušenia národného trestného práva, kam spadajú aj zmluvne založené trestné činy (*treaty-based crimes*), napríklad v oblasti bezpečnosti maloletých v online priestore.

11.1.1 Zvrchovaný kybernetický priestor

S rozvojom schopnosti ľudstva dobývať nové priestory, tieto priestory buď podliehali suverénnej moci, alebo sa chápali ako vec patriaca všetkým. Osobitne more bolo predmetom nielen akademických (Grotius a Seldon), ale aj medzištátnych sporov a konfliktov, ktoré vyústili vo víťazstvo myšlienky slobody morí. Jedným z ťažiskových argumentov bola faktická nemožnosť šíre more kontrolovať. H. Grotius ho pripodobnil vzduchu, ktorý nemožno držať, a tak ho nemožno privlastniť a patrí všetkým. Na druhej strane bola priznaná suverenita nad

[754] Porovnaj Open-ended working group on developments in the field of information and telecommunications in the context of international security, A/AC.290/2021/CRP.2, bod. 34-37.

[755] SCHMITT, Michael N. (ed.): *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013. 278 s. SCHMITT, Michael N. – VIHUL, Liis (eds.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017. 606 s. V súčasnosti sa pripravuje 3. edícia, ktorá by mala byť finalizovaná v roku 2026. Možno očakávať, že Tallinský manuál 3.0 sa dotkne aj nedostatočne rozpracovanej témy AI kybernatických operácií.

teritoriálnymi vodami, a to tradične do vzdialenosti do ktorej vedeli vystreliť delá daného štátu, teda do vzdialenosti, kde sa vedel štát efektívne mocensky presadiť.

Podobne aj v prípade kybernetického priestoru medzinárodné spoločenstvo stojí pred otázkou, či podlieha suverenite štátov, alebo ide o priestor patriaci všetkým, ktorý nepodlieha suverenite žiadneho konkrétneho štátu. V súčasnosti prevláda názor, že kybernetický priestor suverenite štátu podliehať môže a tento má právo na jeho ochranu, a názory tvrdiace, že kybernetický priestor je špecifickým priestorom na ktorý zvrchovanosť nemožno aplikovať možno skôr považovať za odmietnuté[756]. Ak by sme použili analógiu s morom, tak k odlíšeniu vôd podliehajúcich suverenite a šíreho mora, došlo z dôvodu možnosti výkonu kontroly. Tento predpoklad tak podobne vyplýva z faktickej možnosti štátov kybernetickú činnosť kontrolovať a využívať. Vyplýva taktiež aj z predĺženia tradične uznaného, teritoriálneho základu suverenity štátu. Tým sa myslí, že **uplatňovanie štátnej suverenity nad kybernetickým priestorom vyplýva z kontroly kybernetickej infraštruktúry, ktorá sa nachádza na ich území**. Tým sa nemyslí len skutočnosť, že hardvér sa fyzicky nachádza na území štátu, ale aj skutočnosť, že kybernetické operácie majú následky vo fyzickom svete. Kybernetický priestor stále je rozšírenou dimenziou, ktorá je závislá od fyzickej infraštruktúry, ktorá sa niekde nachádza. Konštatovanie rozšírenia suverenity vyplýva aj z personálneho princípu, keďže kybernetické aktivity sú realizované, alebo inicializované, osobami, ktoré podliehajú suverenite štátu. V tejto rovine však narážame na otázky autonómnych a AI systémov, ak vykonávajú operácie bez inicializácie. Tento záver vyplýva aj z praxe štátov, ktoré ku kybernetickému priestoru nepristupujú ako k medzinárodnému priestoru typu *res communis omnium*. Názory o kybernetickom priestore ako priestore patriacemu všetkým, mimo suverenity štátu, či dokonca „mimo práva" [757], vznikali najmä v skoršej etape digitálnej revolúcii, kedy si štáty ešte plne neuvedomovali význam tejto novej dimenzie. Ich mlčanie tak nebolo ani tak prejavom ich *opinio juris*, ako skôr nezáujmu o tento priestor. To sa postupne mení a keď sa stáva tento priestor pre štáty relevantný, tak v reakcii na kybernetické incidenty reagujú spôsobom uzurpujúcim si

[756] Pravidlá týkajúce sa suverenity v kontexte kybernetického priestoru patrili k najproblematickejším bodom diskusie. Bližšie k diskusii pozri JENSEN, Eric Talbot: The Tallinn Manual 2.0: Highlights and Insights. In: *Georgetown Journal of International Law*, vol. 48, no. 3, 2017, s. 740-744. CHIRCOP, Luke: Territorial sovereignty in cyberspace after Tallinn Manual 2.0. In: *Melbourne Journal of International Law*, vol. 20, 2019, s. 6 a nasl.

[757] Pozri napr. BARLOW, John Perry: *A Declaration of the Independence of Cyberspace*, Electronic Frontier Foundation (web page), 8 Feb. 1996. Online: https://www.eff.org/cyberspace-independence.

suverenitu aj nad „ich" časťami kybernetického priestoru, ktorý mal byť narušený a dovolávajú sa zodpovednosti a aplikácie ich národného právneho poriadku. S ohľadom na túto všeobecnú prax štátu, ktorá je spojená aj s odovlávaním sa na porušovanie princípov medzinárodného práva (teda súvisiacim *opino juris*) možno názory o kybernetickom priestore ako *rec communis omnium* odmietnuť a prikloniť sa k názoru o sformovaní obyčajového pravidla rozširujúceho suverenitu štátov aj na kybernetický priestor.

Stály dvor medzinárodnej spravodlivosti uviedol: „zvrchovanosť vo vzťahoch medzi štátmi znamená nezávislosť. Nezávislosť s ohľadom na časť zemegule je právo tam vykonávať funkcie štátu s vylúčením akéhokoľvek iného štátu."[758] James Crawford zas definuje vnútornú a vonkajšiu suverenitu nasledovne:, „vnútorná suverenita je najvyššou autoritou štátu regulovať ľudí a veci na svojom území, zatiaľ čo vonkajšia suverenita je právomoc štátu konať vo vzťahu k iným rovnako suverénnym štátom na medzinárodnej úrovni."[759] Ide o koncept ktorý je uvedený aj medzi základnými zásadami na ktorých stojí Charta OSN, zakotvený v jej čl. 2 ods. 1. Ak popri štáte vykonávajú činnosť, respektíve sú autoritou v určitých oblastiach, aj iné konkrétne entity, tieto podliehajú vôli suveréna. Suverenita štátu sa v súčasnosti nevníma absolútne, ale je podriadená abstraktnej vláde práva. Rozvitie myšlienky, či právo (vrátane medzinárodného práva) vyplýva výlučne z vôle štátu, alebo existuje aj právo, ktoré je od vôle štátu nezávislé, presahuje rámec a cieľ tejto učebnice. Vo vzťahu k vzťahom medzi štátmi je podstatné, že „prvým a najdôležitejším obmedzením, ktoré medzinárodné právo ukladá štátu, je, že... nemôže vykonávať svoju moc v žiadnej forme na území iného štátu."[760] Suverenita štátu nad časťou kybernetického priestoru obmedzuje voľnostné správanie sa iných štátov, ako aj akýchkoľvek iných entít, v kybernetickom priestore, ktorý podlieha jeho zvrchovanosti. Tomu zodpovedá jeho právo chrániť kybernetické aktivity a infraštruktúru, ktorá podlieha jeho suverenite, bez ohľadu nato, či ide o infraštruktúru a operácie verejné alebo súkromné. Taktiež má právo regulovať činnosť v kybernetickom priestore, vyvodzovať zodpovednosť voči subjektom, ktoré v kybernetickom priestore vykonávajú protiprávne operácie, ako aj regulovať kybernetickú infraštruktúru, tzn. stanoviť podmienky jej

[758] Permanent Court of Arbitration: Island of Palmas (or Miangas) Case (United States v. Netherlands), Award of 4 April 1928, Reports of International Arbitral Awards, Vol. II, p. 838.
[759] CRAWFORD, James R.: *Brownlie's Principles of Public International Law*. 8th ed., Oxford University Press, 2012, s. 448.
[760] Permanent Court of International Justice: SS 'Lotus' (France v Turkey) (Judgment) [1927] PCIJ (ser A) No 10, 18.

používania, vlastnenia a môže ju odpojiť, alebo ju zakázať. Nesmie však pritom zasahovať do suverenity druhého štátu a ani porušovať normy medzinárodného práva, vrátane medzinárodných práv jednotlivca. Zákaz prístupu na internet ako taký možno vnímať ako neprimeraný zásah do základných práv jednotlivca[761], alebo obmedzenie komunikácie zastupiteľného úradu s vysielajúcim štátom ako porušenie diplomatického práva[762]. Na druhej strane zákaz šírenia detskej pornografie, alebo podmienenie používania online služieb dosiahnutím určitého veku, je prejavom zvrchovaného práva štátu.

Kybernetický priestor nie je ani priestorom „zdieľanej suverenity" (čo popiera aj samotný koncept suverenity) a ani medzinárodným priestorom, ale z hľadiska suverenity fragmentovaným priestorom. Preto je osobitne dôležité poznanie odkiaľ kam siaha suverenita konkrétneho štátu[763]. Vo všeobecnosti sa akceptuje, že štát môže vykonáva preskriprívnu a adjukatívnu jurisdikciu aj extrateritoriálne, naproti tomu vykonávacia jurisdikcia je viazaná len na územie štátu[764].

V tomto kontexte existuje diskusia, či je suverenita samostatným právom štátu, alebo východiskovým princípom z ktorého vyplývajú konkrétne práva štátu. Túto diskusiu na tomto mieste necháme nerozpracovanú. Je však potrebné podotknúť, že z hľadiska **intenzity zásahu** je možné rozlišovať prípady narušenia teritoriálnej suverenity spĺňajúce intenzitu *de minimis* a závažnejšie prípady narušenia teritoriálnej integrity, ktoré sú spojené s použitím sily. Príkladom konania ktoré býva uvádzané ako príklad konania ktoré medzinárodnoprávne nenapĺňa ani intenzitu *de minimis* je kyberšpionáž spočívajúca len v sledovaní a odcudzovaní

[761] ECHR: CASE OF AHMET YILDIRIM v. TURKEY, no. 3111/10, Judgment (Merits and Just Satisfaction), 18.12.2012; ECHR: Jankovskis v. Lithuania, no. 21575/08, Judgment 17.1.2017.

[762] Čl. 27, Viedenský dohovor o diplomatických stykoch z roku 1961. DENZA, Eileen: *Diplomatic Law: Commentary on Vienna Convention on Diplomatic Relations*: *A Commentary*. Oxford: OUP, 2016, s. 180. Všetky primerané prostriedky komunikácie zahŕňajú aj elektronickú poštu. Na druhej strane bezdrôtové vysielače (*wireless transmitter*) môžu podliehať súhlasu prijímajúceho štátu, aj keď obvykle štáty umožňujú ich používanie bez osobitného súhlasu.

[763] Bližšie SCHMITT, Michael N. – VIHUL, Liis (eds.): *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017, s. 11-29.

[764] Porovnaj „Now the first and foremost restriction imposed by international law upon a State is that-failing the existence of a permissive rule to the contrary-it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial ; it cannot be exercised by a State outside its territory... It does not, however, follow that international law prohibits a State from exercising jurisdiction in its own territory, in respect of any case which relates to acts which have taken place abroad, and in which it cannot rely on some permissive rule of international law. Such a view would only be tenable if international law contained a general prohibition to States to extend the application of their laws and the jurisdiction of their courts to persons, property and acts 'outside their territory." The Case of the S.S. "Lotus", Publications of the Permanent Court of International Justice, Series A- No. 10, September 7th, 1927, s. 18-19.

dát. Tým nie je dotknutá možno protiprávnosť v rovine vnútroštátneho práva. V kontexte kybernetických operácií tak možno rozlíšiť z hľadiska intenzity konania tri situácie:

1. Medzinárodne nevľúdne (nie protiprávne) konanie.
2. Medzinárodne protiprávne konanie.
3. Porušenie zásady zákazu hrozby a použitia sily.

Pre lepšie ilustrovanie možno uvádzať **Chircopovu škálu intenzity závažnosti kybernetických operácií**:

1. Sledovanie alebo odcudzenie dát. Ide o operácie kybernetickej špionáže, pri ktorých sú dáta uložené na cieľovej kybernetickej infraštruktúre alebo prechádzajúce cez ňu monitorované na diaľku. Patria sem kybernetické operácie, ktoré vedú ku kopírovaniu alebo úniku dát do vzdialeného kybernetického systému na účely uloženia alebo kontroly.
2. Vloženie dát. Ide o kybernetické operácie, pri ktorých sú údaje, niekedy obsahujúce nepravdivé alebo „falošné" informácie, dočasne alebo natrvalo umiestnené do cieľových kybernetických systémov.
3. Zmena dát. Ide o kybernetické operácie, pri ktorých sú údaje uložené v cieľových kybernetických systémoch dočasne alebo trvalo manipulované (ale nie vymazané).
4. Vymazanie dát. Ide o kybernetické operácie, pri ktorých sú údaje uložené v cieľových kybernetických systémoch poškodené tak, že ich nemožno použiť, alebo sú úplne vymazané.
5. Spôsobenie dočasnej straty funkcionality. Ide o kybernetické operácie, ktoré spôsobujú dočasnú stratu funkčnosti cieľovej kybernetickej infraštruktúry. Medzi bežné príklady tohto druhu operácií patria útoky typu distribuované odmietnutie služby („DDoS") a útoky ransomvérom.
6. Spôsobenie trvalej straty funkcionality. Ide o kybernetické operácie, ktoré spôsobujú trvalú stratu funkčnosti cieľovej kybernetickej infraštruktúry spôsobom, ktorý si vyžaduje opravu alebo výmenu fyzických komponentov.
7. Spôsobenie materiálnej (fyzickej) škody alebo ujmy[765]. Ide o kybernetické operácie, ktoré spôsobujú fyzické poškodenie cieľovej kybernetickej infraštruktúry (alebo iných

[765] CHIRCOP, Luke: Territorial sovereignty in cyberspace after Tallinn Manual 2.0. In: *Melbourne Journal of International Law*, vol. 20, 2019, s. 10-12.

fyzických komponentov, ktorých fungovanie je závislé od cieľovej infraštruktúry) alebo spôsobujú fyzické zranenia ľuďom.

Nie je dosiaľ jednoznačné od stupňa ktorej intenzity ido o konanie narúšajúce suverenitu štátu[766]. V rámci uvedenej škály konanie prvej intenzity bude najskôr vyhodnotené „iba" ako medzinárodne nevľúdna (nie protiprávna) kybernetická operácia (typu *malicious cyber activity*), avšak neporušujúca suverenitu štátu a ani jeho medzinárodné práva. Naopak ak ide o konanie siedmej intenzity, jeho závažnejšie formy napĺňajú kvalifikačné znaky kybernetického útoku (ku kvalifikačným znakom bližšie ďalej). Medzi kybernetickým útokom (*cyber attack*) ako najzávažnejšou formou použitia sily a medzinárodné právo neporušujúcou, no škodlivou kybernetickou aktivitou (*malicious cyber activity*), existujú aj nepriateľské kybernetické operácie (*hostile cyber operations*)767, ktoré môžu byť protiprávne, aj keď nedosahujú intenzitu kybernetického útoku. Kde presne podľa medzinárodnej obyčaje ide o konanie ktoré je „iba nevľúdne" a kde začína už protiprávne konanie, nie je možné v súčasnosti ešte definitívne uviesť, pravdepodobne sa však deliaca línia nachádza niekde na úrovni 2. stupňa Chircopovej škály.

11.1.2 Zodpovednosť štátu za protiprávnu kybernetickú operáciu

V kontexte kybernetickej bezpečnosti má zodpovednosť štátu špecifické črty vyplývajúce z povahy kybernetických operácií. Kyberoperácie sú často anonymizované, prebiehajú cez distribuovanú infraštruktúru, využívajú kompromitované zariadenia v rôznych štátoch a často sa do nich zapájajú neštátni aktéri konajúci buď samostatne, alebo s rôznou mierou podpory štátu. Tieto faktory spôsobujú, že identifikácia pôvodcu a následne aj určenie medzinárodnoprávnej zodpovednosti je náročnejšie než v tradičných formách protiprávnych operácií.

[766] K štyrom prístupom pozri CHIRCOP, Luke: Territorial sovereignty in cyberspace after Tallinn Manual 2.0. In: *Melbourne Journal of International Law*, vol. 20, 2019, s. 12-16.

767 Vzhľadom na absenciu dostatočnej praxe a súdnych rozhodnutí, nie je možné vnímať koreláciu medzi medzinárodne nevľúdnym konaním a malicous cyber activity a medzinárodne protiprávnym konaním a hostile cyber operations strikne, ale výlučne ilustratívne. Nie je preto vylúčené, že určitá malicious cyber activity bude už vyhodnotená ako protiprávne, alebo naopak niektorá hostile cyber operation by ako protiprávna vyhodnotená nebola.

Štát je medzinárodnoprávne zodpovedný za nedodržanie (*non-compliance*)[768] akéhokoľvek medzinárodnoprávneho záväzku, ktorým je viazaný. Pre konštatovanie vzniku zodpovednosti štátu za medzinárodne protiprávne konanie[769] je tak nevyhnutné identifikovať medzinárodnoprávnu normu s ktorou konanie štátu nie je v súlade. Štát je zodpovedný za nedodržanie akýchkoľvek noriem medzinárodného práva, ktorými je viazaný, bez ohľadu na ich formu či charakter[770].

Štát zodpovedá len za svoje konanie. Je potrebné konštatovať, že štát je abstraktnou entitou, ktorá nemá vlastné vedomie, vôľu a ani telesnú schránku. Presnejším vyjadrením je preto, že je potrebné identifikovať osoby, ktorých konanie možno štátu pričítať[771]. Záväzok môže vyžadovať rozličné formy zavinenia relevantnej osoby, spravidla postačuje určitá forma nedbanlivosti (*culpability, negligence, due diligence*) [772].

Na tomto mieste len zdôrazníme, že **je potrebné rozlišovať medzi technickou atribúciou a právnou pričítateľnosťou** (atribúciou, *attributability*). Technická atribúcia je významným dôkazným prvkom tvoriacim zásadnú súčasť právneho vyhodnotenia situácie, avšak z technickej atribúcie nemožno bez ďalšieho vyvodiť záver o právnej pričítateľnosti.

Medzinárodnoprávna zodpovednosť je založená na identifikovaní **či konala osoba, ktorej konanie je štátu pričítateľné** (subjektívny prvok) a **či toto konanie porušilo medzinárodnoprávny záväzok** (objektívny prvok)[773]. Výzvou pre tradičnú teóriu pričítateľnosti bude situácia, keď je kybernetická operácia vykonaná umelou inteligenciou alebo autonómnym systémom bez priameho prejavu vôle konkrétnej osoby. V takýchto

[768] Nedodržanie je vo všeobecnosti azda najvhodnejším termínom, keďže dobre vyjadruje aj omisívnu formu konania, ktorá je obdobne početná, ako komisívna forma. V angličtine sa využívajú aj termíny ako non-execution of international obligations, acts incompatible with international obligations, violation of an international obligation, alebo breach of an engagement. Vo francúzskej terminológii je vhodným termínom fait internationalement illicite.

[769] Alebo tiež aj „správanie" KLUČKA, Ján: *Medzinárodné právo verejné (všeobecná a osobitná časť)*. Košice: Wolters Kluwer, 2017, s. 175 a nasl.

[770] „...na medzinárodnom poli nerozlišujeme medzi zmluvnou a mimozmluvnou (*tortious*) zodpovednosťou, porušenie akéhokoľvek záväzku štátom, akéhokoľvek pôvodu, zakladá zodpovednosť štátu..." Rainbow Warrior affair, UNRIAA, vol. XX (Sales No. E/F.93.V.3), s. 215 (1990)

[771] „...a aby bolo možné pričítať konanie štátu je nevyhnutné určiť, s rozumnou istotou, konajúcich a ich prepojenie so štátom..." Kenneth P. Yeager v. The Islamic Republic of Iran, Iran-U.S. C.T.R., vol. 17 , s. 101–102.

[772] Napríklad vo veci Korfského prielivu MSD konštatoval, že postačuje že Albánsko „vedelo alebo muselo vedieť" o prítomnosti mín, ktoré spôsobili škody Spojenému kráľovstvu. Corfu Channel Case (United Kingdom v. Albania), I.C.J. Reports 1949, s. 22-23.

[773] „Na fakty sa musí Súdny dvor pozerať z dvoch hľadísk. Po prvé, musí určiť, do akej miery je možné po právnej stránke považovať predmetné akty za konanie pričítateľné iránskemu štátu. Po druhé, musí zvážiť ich zlučiteľnosť alebo nezlučiteľnosť s povinnosťami Iránu podľa platných zmlúv alebo podľa akýchkoľvek iných uplatniteľných pravidiel medzinárodného práva." United States Diplomatic and Consular Staff in Tehran, Judgment, I. C. J. Reports 1980, s. 29.

prípadoch zatiaľ nie je definitívne ustálené, ako sa má posudzovať prípadná zodpovednosť štátu a podľa ktorých kritérií určovať, či a v akom rozsahu možno konanie autonómneho systému štátu pripočítať. Keďže medzinárodné právo je technologicky neutrálne, absencia ľudského aktéra sama osebe nevylučuje zodpovednosť štátu, za vytvorenie, nasadenie, umožnenie fungovania alebo nedostatočnú kontrolu autonómneho systému, ktorý spôsobil následok v rozpore s medzinárodným právom, avšak konkrétne pravidlá sa ešte len formujú a možno očakávať, že problematike UI systémov sa bude venovať aj pripravovaný Tallinský manuál 3.0.

Z prvku pričítateľnosti vyplýva nutnosť preukázania väzby medzi nedodržaním medzinárodnoprávneho záväzku a konaním relevantnej osoby. Väzbu k štátu má relatívne rozsiahla množina osôb. Táto je väzba môže byť založená na štátnej príslušnosti, pobyte, sídle podnikania a podobne. Štát však nebude zodpovedať za konanie všetkých osôb, ktoré k nemu majú akúkoľvek väzbu. Takto definovaný rozsah pričitateľnosti by bol príliš široký a predstavoval by vo vzťahu k štátu neprimerané bremeno zodpovednosti.

Štát zodpovedá v prvom rade za konanie svojich orgánov. Orgánmi štátu sú všetky osoby, ktorým takéto postavenie vyplýva z vnútroštátneho práva. Štát zodpovedá za všetky svoje orgány od najvyššej až po najnižšiu úroveň, a to bez ohľadu na ich zaradenie v rámci deľby štátnej moci (zákonodarná, výkonná, súdna alebo iná moc), vrátane územných jednotiek[774]. Napríklad zodpovednosť štátu vznikne, ak príslušníci vojenskej kybernetickej jednotky uskutočnia ofenzívnu operáciu smerujúcu k narušeniu funkčnosti systému iného štátu v rozpore s medzinárodným právom.

Štát za svoj orgán zodpovedá aj v prípade, ak prekročil svoje právomoci (konanie ***ultra vires***). Postavenie orgánu ako nezávislého od ostatných orgánov nezbavuje štát zodpovednosti za tento orgán. Je vecou štátu akým spôsobom usporiada organizáciu svojich orgánov, z pohľadu medzinárodného práva je však subjektom, a teda aj nositeľom medzinárodnoprávnej zodpovednosti, štát ako taký. Skutočnosť, že orgány štátu konajú v rozpore s vnútroštátnym právom alebo nerešpektujú pokyny nadriadených orgánov,

[774] „...Taliansky štát je zodpovedný za implementovanie Mierovej zmluvy, aj pre Sicíliu, bez ohľadu na autonómiu, ktorá je priznaná Sicílii v jej vnútroštátnych vzťahoch podľa verejného práva Talianskej republiky..." UNRIAA, vol. XIII (Sales No. 64.V.3), s. 161 (1951). „Medzinárodná zodpovednosť štátu je založená konaním kompetentných orgánov a predstaviteľov konajúcich v danom štáte, nech sú akékoľvek... guvernér Arizony má povinnosť konať v súlade s medzinárodnými záväzkami Spojených štátov." LaGrand (Germany v. United States of America), Provisional Measures, Order of 3 March 1999, I.C.J. Reports 1999, s. 495.

nezbavuje štát zodpovednosti[775]. Napríklad ak jednotka vojenského kybernetického velenia vykoná neoprávnený zásah do systému zahraničnej elektrárne, ide o konanie pričítateľné štátu, aj keď operátor prekročil explicitné príkazy.

Druhým východiskom je, že **štát nezodpovedá za konanie súkromných osôb**, respektíve osôb, ktoré nekonajú v pozícii štátneho orgánu. **Pričitateľnosť konania súkromných osôb je potrebné odlišovať od zanedbania preventívnej povinnosti**. V prípade, ak štátne orgány vedeli a mohli zakročiť, napríklad proti kybernetickému útoku, tak štát bude niesť zodpovednosť. Nie však za konanie kybernetických operátorov ako súkromných osôb, ale za neadekvátnosť konania svojich štátnych orgánov[776]. Napríklad ak štát vedel o veľkom botnete s IP rozsahmi v jeho sieti, ale nerobil nič na jeho obmedzenie, prípadne nereagoval na upozornenia zahraničného CERTu.

V praxi konkrétne osoby v pozícii orgánu štátu, prirodzene, nekonajú vždy v tejto pozícii. **Je potrebné odlišovať, či daná osoba koná ako orgán štátu (*in official capacity*) alebo v súkromnej sfére (*in private capacity*).** Je tak potrebné rozlišovať svojvôľu operatívca, ktorý zneužije svoju právomoc alebo zverené prostriedky, od situácie, kedy koná mimo súvisu so svojou funkciou. Či osoba koná v súkromnej alebo v úradnej pozícii závisí od okolností.[777] Východiskom je tak pričítateľnosť konania osôb v postavení štátneho orgánu. Štátu ale bude možné pripočítať aj konanie ďalších skupín osôb.

Ďalšou skupinou je **konanie osôb, ktoré síce nie sú orgánmi štátu, avšak štát na ne preniesol výkon štátnych (vládnych) právomocí**[778]. Naďalej platí, že pričítateľné je len to ich konanie, ktoré vykonávajú v rámci tohto preneseného výkonu. Ak štát poverí súkromnú firmu prevádzkou národného CERT/CSIRT a táto v rámci incident response prekročí svoje

[775] „Tento záver [o porušení Dohovoru] nezávisí od toho, či orgán alebo úradník porušil ustanovenia vnútroštátneho práva alebo prekročil limity svojich právomocí: podľa medzinárodného práva štát je zodpovedný za konanie svojich zástupcov, konajúcich v ich úradnej kapacite a pre ich nekonania, aj keď títo zástupcovia prekročili svoju právomoc alebo porušil vnútroštátne právo." Velásquez Rodríguez v. Honduras case, Inter-American Court of Human Rights, Series C, No. 4.

[776] K preventívnej povinnosti bližšie v časti o zodpovednosti za škodu.

[777] Inšpirované prípadom Francisco Mallén (United Mexican States) v. U.S.A. 27 April 1927, Reports of international arbitral awards, VOLUME IV s. 174-177.

[778] „...štát, ako mimoriadne opatrenie, zveruje súkromným organizáciám verejnoprávne oprávnenia, povinnosti alebo právomoci, aby vykonávali zvrchované práva, ako v prípade súkromných železničných spoločnosti oprávnených udržiavať policajnú jednotku... štát je zodpovedný za škodu spôsobenú cudzincom, ako dôsledku konaní alebo nekonaní... autonómnych inštitúcií pri výkone verejných funkcií majúcich legislatívnu alebo administratívnu povahu." League of Nations, Conference for the Codification of International Law, Bases of Discussion for the Conference drawn up by the Preparatory Committee, vol. III: Responsibility of States for Damage caused in their Territory to the Person or Property of Foreigners (document C.75.M.69.1929.V), s. 90-92.

právomoci a prenikne do zahraničnej siete, zodpovednosť vzniká štátu. Platí to však len v rozsahu delegovaných právomocí, ak koná mimo spojitosti s delegovanou prevádzkou národného systému, konanie štátu pričítateľné nie je.

Zodpovednosť vzniká aj v situáciách, keď štátu iný **štát poskytne inému svoj štátny orgán, ktorý koná v mene a v záujme prijímajúceho štátu**. Napríklad pri spoločných incident response tímoch alebo dočasnom presune kapacít (napr. forenzných tímov) môže dôjsť k situáciám, kde sa bude potrebné určovať, ktorému štátu pripočítať zásah do zahraničných systémov. Napriek tomu, že nejde o jeho štátny orgán, v danom období koná podľa jeho pokynov a pod jeho kontrolou. Preto za jeho konanie bude niesť zodpovednosť prijímajúci štát. Nepôjde o situácie, kedy štátny orgán vysielajúceho štátu pôsobí na území iného štátu, alebo v jeho prospech, v rámci dohody o spolupráci, ale ostáva pod kontrolou poskytujúceho štátu[779]. Ak poskytujúci štát odovzdal svoj orgán do kontroly iného štátu s vedomím, že má byť použitý na protiprávne konanie, tak možno hovoriť zodpovednosti, a to za pomoc a podporu pri protiprávnom konaní prijímajúceho štátu.

Od kontroly a riadenia je teda potrebné odlišovať pomoc a podporu pri protiprávnom konaní. Ak štát, ktorý poskytol pomoc alebo podporu, vedel o tom, že **pomoc alebo podpora** bude použitá na protiprávne konanie, poskytol ich na tento účel, a za predpokladu, že takéto konanie by bolo protiprávnym aj pre pomáhajúci štát, tak pomáhajúci štát bude zodpovedať, ale len v rozsahu poskytnutej pomoci alebo podpory[780]. Východiskom je zodpovednosť toho štátu, ktorý konal protiprávne. Ak konajú protiprávne viaceré štáty, hovoríme o spoločnej zodpovednosti, nie o zodpovednosti za pomoc alebo podporu. V prípade spoločnej zodpovednosti zodpovedajú štáty spoločne a nerozdielne (solidárne).

Štát zodpovedá aj za **konanie osôb, ktoré bolo riadené alebo kontrolované štátom**. Ako sme už zmienili, štát zásadne zodpovedá za orgány štátu a nie za konanie súkromných osôb. V prípade ak je ich konanie riadené alebo kontrolované štátom, tak v tomto rozsahu je ich konanie štátu pričítateľné. Problematickou sa však ukazuje otázka, aká miera kontroly je pre tento účel rozhodujúca. Medzinárodný súdny dvor uplatňuje štandard efektívnej

[779] Napríklad kontrolovanie imigrácie na mori Talianskom v prospech Albánska bolo pričítateľné Albánsku, aj keď kontrolu nevykonával albánsky štátny orgán. Xhavara and Others v. Italy and Albania, application No. 39473/98, Eur. Court H.R., decision of 11 January 2001.

[780] Medzi výnimky patri agresia, ktorá nie je definovaná len ako pozemná inváziа a pod., ale aj ako umožnenie použitia svojho územie na tento účel. Štát, ktorý umožní použitie svojho územia na účely, napr. invázie, nebude zodpovedný „len" za pomoc a podporu pri použití sily v rozpore s Chartou OSN, ale aj on sám bude zodpovedným za porušenie tohto záväzku. Rezolúcia Valného zhromaždenia OSN A/RES/29/3314.

kontroly[781], ktorú definoval negatívnym spôsobom. Za efektívnu kontrolu, nad napríklad povstaleckým hnutím, sa *nebude* považovať výber a dosadzovanie lídrov, financovanie, poskytnutie výcviku odbornej prípravy, plánovanie operácií, výber cieľov či operačnú podporu. Musí ísť o taký stupeň kontroly, pri ktorej neštátna entita stráca svoju vôľovú autonómiu a stáva sa nástrojom vôle štátu (*de facto* orgánom štátu)[782]. Za kontrolu pre účely pričítateľnosti sa nebude považovať ani väčšinový podiel štátu v obchodnej spoločnosti, iba ak s výnimkou, ak zariadenie obchodnej spoločnosti alebo konanie prostredníctvom nej bolo

[781] „Súd musí v tomto bode rozhodnúť, či bol vzťah Contras k vláde USA charakterizovaný jednak takým stupňom závislosti, a jednak takým stupňom kontroly, že by bolo pre právne účely náležité hľadieť na Contras ako na orgán vlády USA alebo na orgán konajúci v mene tejto vlády... Napriek mnohým dodávkam a podpore, ktorá bola Contras zo strany USA poskytnutá, neexistuje žiadny jasný dôkaz, že by USA skutočne vykonávali vo všetkých oblastiach taký stupeň kontroly, ktorý by oprávňoval považovať Contras za konajúcich v mene USA. Aby žalobca preukázal existenciu takejto kontroly, argumentoval pred Súdom tým, že politickí lídri Contras boli vyberaní, dosadzovaní a platení USA... Otázka výberu, dosadzovania a platenia lídrov Contras predstavuje jeden z mnohých aspektov charakterizujúcich stupeň závislosti týchto ozbrojených síl. Táto čiastočná závislosť na orgánoch USA, ktorej presný rozsah Súd nemôže zistiť, môže byť zaiste odvodená okrem iného z faktu, že lídri boli vyberaní USA. Môže sa však vyvodiť aj z iných faktorov, z ktorých niektoré boli preskúmané Súdom, ako je organizácia, odborná príprava a vybavenie ozbrojených síl, plánovanie operácií, výber cieľov a poskytovaná operačná podpora. Súd dospel k názoru, že účasť USA, aj keď prevažuje alebo je rozhodujúca pri financovaní, organizácii tréningu, zásobovaní a vyzbrojovaní Contras, pri výbere ich vojenských alebo polovojenských cieľov a pri plánovaní celých ich operácií je sama o sebe nepostačujúca na to, aby na základe dôkazov, ktorými Súd disponuje, mohli byť USA pripísané akty Contras spáchané počas ich vojenských a polovojenských operácií v Nikaragua. Všetky vyššie uvedené formy účasti USA a dokonca aj všeobecná kontrola zo strany žalovaného štátu nad jednotkami s vysokým stupňom závislosti na ňom by samy o sebe neznamenali, bez ďalších dôkazov, že USA riadili alebo presadzovali spáchanie činov, ktoré sú v rozpore s ľudskými právami a humanitárnym právom, ktoré tvrdí žalujúci štát. Tieto akty by totiž mohli byť dosť dobre spáchané členmi Contras aj bez kontroly USA. Aby teda také konanie zakladalo právnu zodpovednosť USA, bolo by v zásade nutné dokázať, že daný štát mal efektívnu kontrolu nad vojenskými a polovojenskými operáciami, v rámci ktorých k údajným porušeniam práva došlo." Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment, I.C.J. Reports 1986, s. 62-65.

[782] V prípade Tadić Medzinárodný trestný tribunál pre bývalú Juhosláviu uplatnil režim celkovej kontroly, pri ktorej by takáto miera podpory bola postačujúca. Nejde však o rozpor, hoci sa tak na prvý pohľad môže javiť. Štandard efektívnej kontroly je rozhodujúci pre otázku pričítateľnosti konania štátu a štandard celkovej kontroly je rozhodujúci pre otázku charakteristiky ozbrojeného konfliktu ako medzinárodného – teda aj pre aplikovania správnych prameňov medzinárodného humanitárneho práva a s tým súvisiace otázky individuálnej trestnej zodpovednosti.. „Požiadavka medzinárodného práva pre pričítateľnosť konaní súkromných jednotlivcov štátu je výkon kontroly štátu nad jednotlivcami... Odvolací senát nevidí dôvod, prečo by za každých okolností medzinárodné právo malo vyžadovať [rovnako] vysoký štandard pre test kontroly... logika veci nevyžaduje, aby rovnaký test bol použitý pre riešenie dvoch otázok, ktoré sú veľmi odlišné vo svojej podstate: stupeň a povaha zapojenia sa štátu v ozbrojenom konflikte na území iného štátu, ktorá je vyžadovaná preto, aby konflikt bol považovaný za medzinárodný, sa môže veľmi dobre, a bez logickej nekonzistencie, odlišovať od stupňa a povahy zapojenia sa požadovaného pre vznik zodpovednosti štátu za konkrétny čin spáchaný v rámci konfliktu." ICTY, The Prosecutor v. Dusko Tadić, IT-94-1-A, Appeals Chamber, Judgement, 15 July 1999, ods. 405.

zneužité pre účely podvodu alebo *in fraudem legis*[783], respektíve v širšom zmysle na protiprávne konanie s úmyslom vyhnúť sa zodpovednosti. V kyberpriestore je časté využívanie tzv. „patriot hackers", hacktivistov alebo hackerských skupín, ktoré môžu konať v súlade s politickými záujmami štátu. Samotná ideová blízkosť však na pričítateľnosť nestačí, musí ísť o *efektívnu kontrolu* nad konkrétnou operáciou. Ak štát poskytuje skupine nástroje, vyberá ciele, kontroluje priebeh operácie, kyberútok môže byť pričítaný štátu. Nepostačuje však ak takejto skupine napríklad len poskytne financie. Efektívnu kontrolu je potrebné vyhodnocovať podľa situácie a konštatovanie jej výkonu je výsledkom kombinácie viacerých faktorov, ktoré nemožno definovať abstraktne. Príkladom tak môže byť hackerská skupina, ktorá používa nástroje poskytnuté vládou a ciele útokov schvaľuje ministerstvo obrany.

Štát zodpovedá aj za **konanie neštátnych entít, ktoré z dôvodu neprítomnosti či absencie orgánov štátu a vzhľadom na okolnosti, začnú svojpomocne vykonávať ich funkcie**. Ide o špecifické situácie, kedy štát nie je (dočasne) schopný vykonávať funkcie na danom území, preto z dôvodu nevyhnutnosti výkonu týchto funkcií vezmú do vlastných rúk súkromné osoby[784]. Osobitným prípadom je *levée en masse*, kedy sa obyvateľstvo štátu postaví na odpor proti útočiacim ozbrojeným silám pred tým, ako dokážu adekvátne zareagovať regulárne ozbrojené sily napadnutého štátu. V kontexte kybernetických operácií pôjde o zriedkavý dôvod pričítateľnosti. Možno si ale predstaviť, že miestna komunita IT špecialistov preberie riadenie kritickej kyberinfraštruktúry. ich excesy, napr. neoprávnené monitorovanie komunikácie, môžu byť štátu pričítateľné.

Štát zodpovedá aj za **konanie povstaleckého alebo iného hnutia[785], ktoré by uspelo vo svojej snahe nahradiť vládu alebo vytvoriť nový štát.** Hnutie, ak disponuje medzinárodnoprávnou subjektivitou[786], má svoju vlastnú právnu zodpovednosť, odlišnú od

[783] Uplatňuje sa tak rozlišovanie medzi subjektivitou a zodpovednosťou právnickej osoby a jej podielnikov (tzn. tu štátu) s primeraným aplikovaním inštitútu *lifting/piercing corporate veil*. Barcelona Traction, Light and Power Company, Limited, Judgment, I.C.J. Reports 1970, s. 39-40. K prípadom, kedy konanie štátom vlastnenej obchodnej spoločnosti nebolo pričítané štátu pozri napr.: SEDCO, Inc. v. National Iranian Oil Company, Iran-U.S. C.T.R.., vol. 15, s. 23 (1987). Naopak, konanie bolo pričítané v prípade, ak obchodná spoločnosť bola zneužitá na určitý účel, napr.: Foremost Tehran, Inc. v. The Government of the Islamic Republic of Iran, Iran-U.S. Iran-U.S. C.T.R., vol. 10, s. 228 (1986).

[784] „[neštátna revolučná garda] ale aspoň vykonávala prvky vládnych právomocí za absencie štátnych orgánov o výkone ktorých nová vláda musela mať vedomosť a proti ktorým osobitne neprotestovala." Kenneth P. Yeager v. The Islamic Republic of Iran, Iran-U.S. C.T.R., vol. 17 , s. 92

[785] Táto výnimka sa primerane vzťahuje na povstalecké (opozičné) hnutia, ktoré sa snažia zvrhnúť vládu, ako aj (národnooslobodzovacie) hnutia, ktoré sa snažia o vytvorenie nového štátu. Pojem hnutie sa pre účel medzinárodnoprávnej zodpovednosti môže vykladať extenzívne.

[786] Bližšie pozri v časti o medzinárodnoprávnej subjektivite.

zodpovednosti štátu[787], ktorý sa ho spravidla snaží potlačiť. V prípade porážky hnutia, to ako subjekt zaniká bez právneho nástupcu, a tým zaniká aj zodpovednosť za protiprávne konanie. Štát sa stáva právnym nástupcom do zodpovednosti hnutia, ak je zachovaná kontinuita medzi úspešným hnutím a novou vládou[788]. Musí ísť o reálnu a podstatnú kontinuitu medzi hnutím a štátom. Nepôjde o situáciu, keď sa vláda štátu dohodne s opozičným hnutím, v rámci podmienok ukončenia konfliktu, že hnutiu budú poskytnuté niektoré vládne funkcie. Ak separatistické hnutie prevádzkuje vlastnú „vládnu" kyberinfraštruktúru (CERT, digitálnu administratívu) a neskôr sa stane vládou štátu, právna zodpovednosť za predchádzajúce kyberoperácie prechádza na novovzniknutý štát, respektíve v prípade povstaleckého štátu, na štát, v ktorom sa hnutie chopilo moci.

Štát nesie zodpovednosť v situácii, ak vie a môže zasiahnuť proti konaniu hnutia, ktoré porušuje ľudské práva alebo poškodzuje iný štát. V takom prípade, avšak, nejde o pričítateľnosť konania hnutia, ale o nesplnenie **preventívnej povinnosti** jeho štátnymi orgánmi.

V sumarizácii je v kybernetickom priestore povinnosťou štátu prijať primerané opatrenia na prevenciu škodlivých aktivít, ktoré z jeho územia zasahujú do práv iných štátov. *Due diligence* v kybernetickom priestore môže zahŕňať napríklad monitorovanie škodlivých operácií z vlastného územia, povinnosť zakročiť proti botnetom využívajúcim infraštruktúru štátu alebo povinnosť spolupracovať so zahraničnými orgánmi a CERT tímami pri riešení incidentu, či vymáhanie bezpečnostných štandardov[789]. Štát nenesie zodpovednosť za

[787] „Súd sa nedomnieva, že pomoc poskytnutá USA Contras odôvodňuje záver, že tieto sily podliehajú USA v takom rozsahu, že akékoľvek činy, ktoré spáchali, sú pričítateľné tomuto štátu. Súd je toho názoru, že bremeno zodpovednosti za činy Contras zostáva na nich, a že USA nenesú zodpovednosť voči Nikarague za konania Contras, ale len za svoje vlastné..." Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment, I.C.J. Reports 1986, s. 65.

[788] „Národ je zodpovedný za záväzky úspešnej revolúcie od jej počiatku, pretože teoreticky, reprezentoval ab initio meniacu sa vôľu národa, vyústiacu v konečný úspešný výsledok." UNRIAA, vol. IX (Sales No. 1959.V.5), s. 453. „Ak škody pochádzajú, napríklad, z konfiškácie alebo vyžiadaných nútených príspevkov... revolucionármi pred ich konečným úspechom, alebo boli spôsobené... previneniami spáchanými úspešnými revolučnými silami, zodpovednosť štátu... nemôže byť vylúčená." UNRIAA, vol. V (Sales No. 1952.V.3), s. 353 (1928).

[789] Napríklad v zmysle záväzkov vyplývajúcich zo smernice Európskeho parlamentu a Rady (EÚ) 2022/2555 z 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii alebo z Budapeštianskeho dohovoru o počítačovej kriminalite (2001) v zmysle protokolov. K hmotnoprávnym a procesným záväzkom vyplývajúcim z Budapeštianskweho dohovoru pozri KRÁLIK, Ján: Aktuálne výzvy v oblasti kybernetickej kriminality: návrh druhého dodatkového protokolu k Dohovoru Rady Európy o počítačovej kriminalite In: *Míľniky práva v stredoeurópskom priestore 2021: zborník z medzinárodnej vedeckej konferencie*. Bratislava: Právnická fakulta UK v Bratislave, 2021, s. 12-13.

konanie súkromných aktérov, *pokiaľ neexistujú dôvody pričítateľnosti*, ale môže niesť zodpovednosť za zanedbanie vlastnej preventívnej povinnosti.

A napokon, posledným prípadom je situácia, ak by **štát konanie neštátnej entity uznal alebo prijal ako svoje vlastné**. V rozsahu prijatia bude konanie pričítané štátu. Takéto prijatie nemusí byť nevyhnutne explicitné, ale musí ísť o jednoznačné prijatie konania alebo stavu[790]. Nepôjde o situácie obyčajného vyjadrenia podpory alebo súhlasu s takýmto konaním. Neidentifikovaná hackerská skupina vykoná útok na zahraničné úrady. Ak následne štátne inštitúcie vyhlásia, že „operácia bola legitímnou reakciou", a vedome naďalej tolerujú a podporujú takúto situáciu, môže to predstavovať implicitné prijatie.

Naopak, štátu nebude pričítané konanie jeho orgánov, ktoré síce konali protiprávne, avšak boli pod riadením a kontrolou iného štátu[791] alebo boli k tomu iným štátom donútené[792].

Naopak, predpokladom vzniku subjektívnej medzinárodnoprávnej zodpovednosti nie je vznik škody, hoci jej vznik ovplyvní obsah zodpovednostného vzťahu. **Škoda** je fakultatívnym znakom subjektívnej medzinárodnoprávnej zodpovednosti.

Napriek tomu, že by boli naplnené oba predpoklady vzniku zodpovednosti, konanie štátu nebude protiprávne, ak je prítomná niektorá z **okolností vylučujúcich protiprávnosť**. O naplnení niektorej z okolností má zmysel hovoriť až v prípade, ak konštatujeme naplnenie predpokladov vzniku zodpovednosti. Preto by skúmanie prítomnosti okolností vylučujúcich

---

[790] "Politika ohlásená ajatolláhom Chomejnim ohľadom pokračovania v okupovaní veľvyslanectva a zadržiavaní jeho obyvateľov ako rukojemníkov pre účely vytvárania tlaku na vládu Spojených štátov bola v súlade s ostatnými iránskymi orgánmi a bola nimi podporované opakovane vo vyhláseniach robených v rozličných kontextoch. Výsledkom tejto politiky bola podstatná zmena právnej povahy situácie, ktorá vznikla okupovaním veľvyslanectva a zadržiavaním jeho diplomatického a konzulárneho personálu ako rukojemníkov. Súhlas daný týmto skutočnostiam.... zmenila pretrvávajúcu okupáciu veľvyslanectva a zadržiavanie rukojemníkov na konanie štátu." United States Diplomatic and Consular Staff in Tehran, Judgment, I. C. J. Reports 1980, s. 35.

[791] Môže byť však zodpovedný za pomoc alebo podporu, porovnaj druhú skupinu opísanú vyššie. Tu môže ísť napríklad o situácie počas okupácie, kedy orgány štátu vykonávajú vôľu okupanta. Nepostačuje však, že okupant má schopnosť orgány kontrolovať, ale túto schopnosť musí aj reálne vykonávať. Inak okupovaný štát ostáva zodpovedným za konanie svojich orgánov, napríklad za nezákonné rozhodnutia alebo postupy orgánov verejnej moci. Napr. Taliansko bolo zodpovedné za zhabanie majetku na Sicílii, aj keď v tom čase bolo pod kontrolou Spojeneckých síl. Heirs of the Duc de Guise, UNRIAA, vol. XIII (Sales No. 64.V.3) (1951). Naopak, za porušenie suverenity Svätej stolice nepovoleným vstupom talianskej polície do Baziliky sv. Petra vo Vatikáne bolo zodpovedné Nemecko. AGO, Roberto: L'occupazione bellica di Roma e il Trattato lateranense, Comunicazioni e Studi. Milan: Giuffrè, 1945, vol. II, s. 167–168.

[792] V tejto situácii vznikajú dva právne vzťahy, jeden založený konaním donutiteľa voči donútenému, za ktorú nesie zodpovednosť donutiteľ a druhý založení konaním donúteného voči tretiemu, za ktorú taktiež nesie zodpovednosť donutiteľ. Komisia OSN pre medzinárodné právo vo svojom komentári prepája donútenie s force majeur, avšak podľa nášho názoru, by sa malo posudzovať skôr cez prizmu tiesne alebo núdze. Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries In Yearbook of the International Law Commission, 2001, vol. II, Part Two, as corrected, s. 70.

protiprávnosť malo predstavovať až druhý krok právnej analýzy situácie. Z procesného hľadiska platí zásada, že dôkazné bremeno znáša ten, kto tvrdí. Preto zásadne, až na špecifické situácie presunu dôkazného bremena[793], žalujúci štát musí preukázať naplnenie prvkov zodpovednosti. Následne sa žalovaný štát môže vyhnúť zodpovednosti dokázaním aplikovateľnosti okolnosti vylučujúcej protiprávnosť. V medzinárodnom práve rozlišujeme šesť okolností vylučujúcich protiprávnosť – súhlas, sebaobrana, protiopatrenia, vyššia moc (*force majeur*, *vis maior*), tieseň a núdza. Napríklad ak štátny administrátor admin v odpojí internetové pripojenie, aby zabránil šíreniu ransomvéru, ktorá by mohla ohroziť fungovanie nemocničného informačného systému a teda životy ľudí, možno situáciu vyhodnotiť ako konanie v tiesni, za ktoré medzinárodná zodpovednosť štátu nevzniká. Naopak, odpojenie internetového pripojenia bez takejto justifikácie možno považovať za porušenie medzinárodne uznaných ľudských práv.

Naopak, okolnosťou vylučujúcou protiprávnosť nie je znenie vnútroštátneho práva. **Štát sa nemôže dovolávať svojho vnútroštátneho práva ako dôvodu pre neplnenie medzinárodnoprávnych záväzkov**. Nie je pritom relevantné, akú právnu silu mala vnútroštátna právna norma. Štátny orgán sa tak môže dostať do situácie, kde sa musí rozhodnúť, či bude rešpektovať medzinárodnoprávnu normu alebo vnútroštátnu normu, hoci

[793] Napríklad v prípade Corfu Channel Case (United Kingdom v. Albania), I.C.J. Reports 1949, s. 4 sa MSD uspokojil s tým, že Albánsko „muselo vedieť" o prítomnosti mín, v jeho teritoriálnych vodách, ktoré spôsobili škodu Spojenému kráľovstvu. Spojené kráľovstvo tak nemuselo prvok vedomosti preukazovať.

na úrovni ústavy, ktorá mu môže diktovať práve opačný postup[794]. Táto zásada bola pretavená aj do čl. 27 Viedenského dohovoru o zmluvnom práve z roku 1969[795].

Pri uplatňovaní zodpovednosti je potrebné rešpektovať **jurisdikčné imunity štátu**, ktoré majú zásadný vplyv na výber príslušného fóra na riešenie sporu. Jurisdikčné imunity štátu sa uplatňujú bez ohľadu na povahu medzinárodného záväzku, teda či došlo k porušeniu dispozitívnej alebo kogentnej medzinárodnoprávnej normy[796]. Význam má však či sa porušenie týka konania pri výkone zvrchovanej moci (*acta iure imperii*) alebo pri výkone komerčnej činnosti (*acta iure gestionis*), pri ktorých sa jurisdikčné imunity štátu neuplatňujú a prípadný spor môže byť predmetom konania aj na vnútroštátnom fóre iného štátu. Ak ide o *acta iure imperii,* tak vec možno prejednať len na jeho vlastnom fóre, alebo s jeho súhlasom na inom vnútroštátnom fóre alebo typicky na medzinárodnom fóre. Podmienka súhlasu sa uplatňuje pre ktorýkoľvek z medzinárodných prostriedkov mierového riešenia sporov, počnúc rokovaniami, mediáciou až po arbitráž alebo medzinárodné súdne konanie.

11.1.3 Kybernetický ozbrojený útok a možnosti reakcie

Kybernetický útok je kyberoperácia (ofenzívna alebo defenzívna), **od ktorej sa možno rozumne očakávať**, že **spôsobí zranenie alebo smrť osôb** alebo **škodu či zničenie vecí (objektov)**. Toto nadväzuje na čl. 49 ods. 1 Dodatkového protokolu I (1977) k Ženevským dohovorom z roku 1949, kde **„útok" znamená akty násilia (*acts of violence*) proti**

[794] "...podľa všeobecne prijatých zásad, štát sa nemôže dovolávať, proti inému štátu, na ustanovenia jeho ústavy, ale len na medzinárodné právo a riadne prijaté medzinárodné záväzky riadne prijatých... Treatment of Polish Nationals and Other Persons of Polish Origin or Speech in the Danzig Territory, Advisory Opinion, 1932, P.C.I.J., Series A/B, No. 44, s. 24. "...neutralita, vyhlásená jednotlivým štátom, nemôže mať prednosť pred dojednaniami mierovej zmluvy... podľa článku 380 Versaillskej zmluvy, bolo povinnosťou [Nemecka] umožniť [preplavenie sa lode Wimbledon cel Kielský kanál]. Nemohlo uplatniť svoje nariadenie neutrality namiesto záväzkov, ktoré prijalo podľa tohto článku.", 1923, P.C.I.J., Series A, No. 1, s. 29-30. "Dodržiavanie vnútroštátneho práva a dodržiavanie dojednaní zmluvy sú odlišné otázky. Čo je porušením zmluvy môže byť legálnym podľa vnútroštátneho práva a čo je nezákonné podľa vnútroštátneho práva vôbec nemusí byť v rozpore so zmluvným dojednaním. Aj keby prefekt považoval rekvizíciu za úplne oprávnenú v talianskom práve, nevylučovalo by to možnosť, že ide o porušenie zmluvy o priateľstve, obchode a navigácii... skutočnosť, že konanie orgánu verejnej moci by mohlo byť nezákonným podľa vnútroštátneho práva, nevyhnutne neznamená, že toto konanie bolo protiprávnym podľa medzinárodného práva... rovnako z rozhodnutia vnútroštátneho súdu konštatujúceho neoprávnenosť, nesprávnosť alebo arbitrárnosť konania nevyhnutne nevyplýva, že takéto konanie je arbitrárne aj podľa medzinárodného práva... " Elettronica Sicula S.p.A. (ELSI), Judgment, I.C.J. Reports 1989, s. 51, 74.

[795] „Strana sa nemôže dovolávať ustanovení svojho vnútroštátneho práva ako dôvodu pre neplnenie zmluvy. Toto pravidlo nie je na ujmu článku 46." Viedenský dohovor o zmluvnom práve z roku 1969. Čl. 46 sa týka relatívnej neplatnosti medzinárodnej zmluvy. Ide tak o problematiku samotnej platnosti záväzku, ako jedného z predpokladov vzniku medzinárodnoprávnej zodpovednosti. Nemožno sa ho dovolávať ako okolnosti vylučujúcej protiprávnosti porušenia platných záväzkov.

[796] Jurisdictional Immunities of the State (Germany v. Italy :Greece intervening), Judgment, I.C.J. Reports 2012, p. 99.

protivníkovi. Definujúce sú účinky, nie to, či sú prostriedky „fyzicky násilné" samy o sebe. Inak povedané, pojem násilia v tejto definícii sa môže vzťahovať buď na prostriedky vedenia vojny, alebo na ich účinky, čo znamená, že operácia spôsobujúca násilné účinky sa môže kvalifikovať ako útok, aj keď prostriedky použité na vyvolanie týchto účinkov nie sú ako také násilné[797]. Medzi štátmi nie je jednotné, či musí ísť o situáciu, kde vzniká materiálna škoda, alebo aj situácie kde došlo k vyradeniu funkčnosti cieľa. Medzinárodný výbor Červeného kríža sa prikláňa k druhej skupine štátov[798].

Napríklad smrť pacientov na jednotkách intenzívnej starostlivosti spôsobená kybernetickou operáciou v elektrickej sieti, ktorá má za následok prerušenie dodávky elektriny do nemocnice[799]. Pôjde o ozbrojený útok, pretože napriek tomu, že sa použil nenásilný prostriedok (kód), bolo rozumne predvídateľné, že toto konanie spôsobí násilný účinok. V prípade kybernetických útokov tak možno aplikovať príslušné pravidlá medzinárodného humanitárneho práva, vrátane zásad rozlišovania, primeranosti či opatrnosti. Kybernetický priestor prestavuje osobitnú výzvu pre uplatňovanie noriem humanitárneho práva a bola by vhodná jeho explicitná precizácia. To však neznamená, že kybernatické oparácie sú mimo regulácie medzinárodného humanitárneho právo. Na všetky prostriedky vedenia vojny sa vzťahujú všeobecné zásady humanitárneho práva, ktoré sme už zmienili, a aj na kybernetické operácie je aplikovateľná Martensova klauzula. Akékoľvek pochybnosti o aplikovateľnosti humanitárneho práva v konkrétnej situácii by nemali byť vyriešenie spôsobom znižujúcu ochranu obetí vojny, ale naopak zvýšením potrebného štandardu opatrnosti pri plánovaní kybernetických útokov[800]. V neposlednom rade platí, že

---

[797] SCHMITT, Michael N. – VIHUL, Liis (eds.): *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017, s. XXXX

[798] K rozličným národným pozíciám štátov, ako aj spoločným pozíciám EÚ a AÚ pozri napr.: Attack (international humanitarian law). International Cyber Law: Interactive Toolkit. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2025. Online: https://cyberlaw.ccdcoe.org/wiki/Attack_%28international_humanitarian_law%29

[799] ICRC: International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC position paper. November 2019, s. 7. Online: https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf.

[800] Bližšie pozri napr. GISEL, Laurent; RODENHÄUSER, Tilman; DÖRMANN, Knut: Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. *International Review of the Red Cross*, no. 913, March 2021. Online: https://international-review.icrc.org/articles/twenty-years-international-humanitarian-law-and-protection-civilians-against-effects-cyber-913. DROEGE, Cordula: Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross*, No. 886, June 2012. Online: https://international-review.icrc.org/articles/get-my-cloud-cyber-warfare-international-humanitarian-law-and-protection-civilians. ICRC: International humanitarian law and the challenges of contemporary armed conflicts. Geneva: ICRC, October 2015. 32nd International Conference of the Red Cross and Red Crescent (32IC/15/11). s. 39-44. Online:

je zodpovednosťou bojujúcej strany, ktorá používa určitý prostriedok boja, v tomto prípade kybernatickú operáciu, aby vykonala posúdenie, či jeho použitie spĺňa podmienky medzinárodného humanitárneho práva a za týmto účelom zbraň úplne otestovala a až potom nasadila[801]. Osobitne je tu záväzok už zmienenej Martensovej klauzuly, že „*v prípadoch, ktoré nie sú upravené týmto protokolom alebo inými medzinárodnými dohodami, civilné osoby a kombatanti zostávajú pod ochranou a autoritou zásad medzinárodného práva odvodených zo zavedených obyčají, zo zásad ľudskosti a z diktátu verejného svedomia*."[802]

Nie každé použitie sily však bude možné kvalifikovať aj ako ozbrojený útok. O ozbrojenom útoku možno hovoriť len pri najzávažnejších formách použitia sily[803]. Toto rozlišovanie bude mať význam aj z hľadiska možností reakcie štátu, nakoľko nie každé porušenie zásady zákazu použitia sily (čl. 2 ods. 4 Charty OSN) aktivuje aj prirodzené právo štátu na sebaobranu (čl. 51 Charty OSN).

Za ozbrojený útok sa v kybernetickom priestore spravidla považujú len operácie, ktorých rozsah a účinky sú porovnateľné s kinetickým útokom. Typicky také, ktoré zabíjajú alebo zraňujú osoby alebo spôsobujú významnú fyzickú škodu či deštrukciu majetku či infraštruktúry[804].

Naopak, pri operáciách spôsobujúcich len dočasné narušenie služieb, ekonomické škody alebo „nepríjemnosť" bez fyzickej ujmy ide o príklady situácií, ktoré nebude možné kvalifikovať ako ozbrojený útok. Pri ich prípade bude potrebné individuálnej báze vyhodnocovať, či išlo o protiprávne použitie sily nižšej intenzity ako ozbrojený útok alebo išlo o protiprávne konanie bez toho, aby bolo vôbec kvalifikované ako použitie sily. „použitia sily", a už vôbec nie „ozbrojeného útoku" (to nevylučuje iné právne následky, ako zodpovednosť štátu, či možnoť použitia protiopatrení)

---

https://www.icrc.org/sites/default/files/document/file_list/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf.

[801] BEDNÁR, Daniel: K niektorým aspektom ozbrojených konfliktov 21. storočia v kontexte medzinárodného práva In: Valuch, Jozef, Ozoráková, Lilla (eds).: *Aktuálne bezpečnostné výzvy a medzinárodné právo*. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2021, s. 8-9.

[802] Čl. 1 ods. 2, Dodatkový protokol I z roku 1977 k Ženevským dohovorom o ochrane obetí vojny z roku 1949. Podobne aj štvrtý odsek preambuly Dodatkového protokolu II z roku 1977 k Ženevským dohovorom o ochrane obetí vojny z roku 1949.

[803] Military and Paramilitary Activities in und against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, s. 101, ods. 191. Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment, I. C. J. Reports 2003, s. 186-187, ods. 51.

[804] SCHMITT, Michael N. – VIHUL, Liis (eds.): *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017, s. XXXX

Pre vyhodnocovanie či ide o kybernetická operácia predstavuje použitie sily je možné použiť aj tzv. Schmittovu analýzu, ktorá pozostáva zo skúmania závažnosti, bezprostrednosti, priamosti, invazívnosti, merateľnosti, predpokladu legality a zodpovednosti[805].

11.1.4 Zodpovednosť jednotlivca v kontexte kybernetických operácií

Rýchly vývoj informačných a komunikačných technológií zásadne zmenil moderné konflikty, sociálnu interakciu a riadenie. Na tomto mieste sa zamierame na Medzinárodný trestný súd (ICC), ktorý má mandát stíhať najzávažnejšie zločiny v očiach medzinárodného spoločenstva. Primerane však tieto poznatky možno aplikovať aj všeobecne, nakoľko Rímsky štatút ICC vo veľkej miere reflektuje medzinárodné obyčajové právo. Taktiež ich možno primerane aplikovať aj pre trestné stíhanie týchto zločinov v národnej jurisdikcii, ktorá by mala mať v zmysle zásady komplementarity prioritu pred ich stíhaním na úrovni ICC. Zároveň na tomto mieste nie je priestor detailne rozoberať podmienky individuálnej trestnej zodpovednosti, ale zameriame sa len na špecifiká zločinov v kontexte kybernetických operácií[806].

V súčasnosti sa čoraz častejšie stretávame so situáciami, v ktorých kyberpriestor zohráva priamu alebo umožňujúcu úlohu pri páchaní zločinov podľa medzinárodného práva, čo reflektuje aj Úrad prokurátora (OTP) ICC, kde v roku 2023 prokurátor Karim Khan uviedol, že „za primeraných okolností, **konanie v kyberpriestore môže potencionálne viesť k vojnovým zločinom, zločinom proti ľudskosti, genocíde alebo zločinu agresie**“[807]. OTP ICC preto vydal v decembri 2025 koncepčný dokument s názvom Politika (*policy*) týkajúca sa zločinov umožnených kybernetickou činnosťou podľa Rímskeho štatútu[808].

Tento dokument bolo potrebné prijať s ohľadom nato, že Rímsky štatút bol vypracovaný pred digitálnou revolúciou a teda explicitne nerieši otázky kybernetických operácií či incidentov. To otvára otázky najmä vo vzťahu k zásade zákazu analógie v trestnom

[805] VALUCH, Jozef: Povaha konfliktov v 21. storočí – zmena konceptu alebo len techník ? In: Valuch, Jozef, Ozoráková, Lilla (eds).: *Aktuálne bezpečnostné výzvy a medzinárodné právo*. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2021, s. 18-20.

[806] Bližšie k podmienkam pozri napr. MAREČEK, Lukáš: *Medzinárodné trestné právo a jeho implementácia v slovenskom právnom poriadku*. Bratislava: Právnická fakulta UK v Bratislave, 2025, 266 s. Alebo SVÁK, Ján – MAREČEK, Lukáš a kol.: *Medzinárodné právo verejné a úvod do verejného medzinárodného práva*. Bratislava: Wolters Kluwer, 2024, s. XXXX

[807] ICC Cyberwar Crimes. WIRED. Online: https://www.wired.com/story/icc-cyberwar-crimes/

[808] International Criminal Court. Office of the Prosecutor*: Policy on Cyber-Enabled Crimes under the Rome Statute. The Hague: International Criminal Court*, 2025. Online: https://www.icc-cpi.int/sites/default/files/2025-12/2025-cyber-eng.pdf.

práve (čl. 22 ods. 2 Rímsky štatútu ICC). Rímsky štatút je však technologicky neutrálny a je ho možné aplikovať aj na konanie spáchané alebo umožnené digitálnymi prostriedkami, pokiaľ je naplnená skutková podstata niektorého zo zločinov v jeho jurisdikcii. Nástup fenoménu kybernetických operácií tak nie je prekážkou, ktorá by mohla byť z pohľadu Rímskeho štatútu prekonaná len jeho revíziou, respektíve prijatím ďalších dodatkov.

Pre usmernenie tento dokument objasňuje niekoľko základných konceptov:

- Cyber: Tento termín sa v širšom zmysle vzťahuje na aktivity, infraštruktúry a správanie, ku ktorým dochádza v rámci digitálnych sietí a počítačových systémov alebo prostredníctvom nich.
- Cyber-Enabled Crimes: Zločiny umožnené kybernetickou činnosťou nie sú podľa Rímskeho štatútu samostatnou kategóriou trestných činov. Tento termín namiesto toho opisuje existujúce zločiny podľa Rímskeho štatútu, tzn. tzv. ústredné zločiny (core crimes), teda zločin genocídy, zločiny proti ľudskosti, vojnové zločiny, zločin agresie a trestné činy marenia spravodlivosti podľa článku 70, respektíve priestupky podľa čl. 71 Rímskeho štatútu, ktoré môžu byť spáchané alebo uľahčené kybernetickými prostriedkami.
- Cybercrime: Bežné kybernetické zločiny (napr. hacking, krádež identity, podvody) zvyčajne nepatria do jurisdikcie Medzinárodného trestného súdu (ICC), pokiaľ nie sú súčasťou trestného činu v rámci mandátu súdu alebo priamo neumožňujú spáchanie trestného činu. ICC nestíha samostatnú kybernetickú kriminalitu. V ich prípade môže ísť o zmluvne založené trestné činy, ktoré ale sú trestné nie priamo na základe medzinárodného obyčajového práva, ale podľa vnútroštátneho práva štátu, ktorý ich na základe medzinárodnej zmluvy implementoval do svojho právneho poriadku.

Úrad prokurátora ICC sa v dokumente venuje aj problematike digitálnych dôkazov, vrátane metadát, záznamov a obsahu zo sociálnych médií, ako a zdôrazňuje ich význam a použiteľnosť pre trestné konanie. Vo vzťahu k umelej inteligencii upozorňuje, že môže slúžiť ako nástroj na páchanie trestných činov, avšak na druhej strane môže slúžiť aj ako pomôcka pri ich odhaľovaní. Aj vo vzťahu k medzinárodnému trestnému konaniu tak platí, že umelá inteligencia nie je hodnotovo dobrá alebo zlá, záleží na spôsobe jej využitia.

Pre zločiny v jurisdikcii ICC platia určité limitácie, ktoré reflektujú skutočnosť, že ICC bol zriadený nato, aby sa zaoberal tými najzávažnejšími z už tak závažných zločinov podľa medzinárodného práva (čl. 17 ods. 1 písm. d) Rímskeho štatútu ICC). Preto možno súhlasiť, že

„len malý počet závažných kybernetických operácií bude možné kvalifikovať ako činy stíhateľné pred ICC"[809]. Tým nie je dotknutá možnosť ich stíhania na úrovni národnej jurisdikcie, a to aj vo svetle univerzálnej jurisdikcie. Osobitne ak ide o požiadavku dostatočnej závažnosti v zmysle čl. 22 Rímskeho štatútu ICC. Kybernetické operácie bude možné považovať za dostatočne závažné najmä ak spôsobia stratu na živote alebo závažné poškodenie majetku. Je otázne aké konanie bude vyhodnotené ako dostatočne záväzné, príkladom nejasnej situácie môže byť kybernetický útok na infraštruktúru elektrárne, v dôsledku ktorej došlo k strate elektrického prúdu u tisícov civilných objektov, avšak jej jeho priamym následkom nebola materiálna škoda a ani spôsobenie smrti. Medzi ďalšie limitujúce faktory, ktorým by musela čeliť aj národná jurisdikcia, patrí pripísanie konania, ktoré je výzvou aj vo vzťahu k určeniu konkrétneho štátu . Okrem náročnosti samotnej technickej atribúcie, je samostatnou otázkou právne pripísanie určitému štátu a o to väčšou výzvou pripísanie konkrétnemu jednotlivcovi, ktorý by mal byť za operáciu zodpovedný[810].

Vo vzťahu k jednotlivým skutkovým podstatám zločinov v jurisdikcii ICC dokument uvádza typické príklady zločinov umožnených kybernetickou činnosťou. Digitálne platformy môžu byť použité na priame a verejné podnecovanie **genocídy**, šírenie genocídnej propagandy alebo koordináciu ničenia skupín prostredníctvom online nástrojov, prípadne vytvorením zoznamov identifikovaných členov chránených skupín, ktorí majú byť odstránení. Na tomto mieste je potrebné zdôrazniť, že zločin genocídy je definovaný ako ohrozovací trestný čin (inchoate crime), teda pre naplnenie skutkovej podstaty nie je potrebné, aby následok nastal. Trestným je aj konanie, ktoré je spôsobilé tento následok vyvolať.
Kybernetické prostriedky môžu ďalej uľahčiť rozsiahle alebo systematické útoky na civilné obyvateľstvo vrátane, online obťažujúcich kampaní, ktoré eskalujú do prenasledovania, digitálneho sledovania používaného na identifikáciu a zacielenie chránených skupín, alebo hromadnej manipulácie s informáciami umožňujúcej koordinované útoky, a tým naplniť skutkovú podstatu **zločinov proti ľudskosti**.

[809] STERIO, Milena a TRAHAN, Jennifer: Cyber Operations as Crimes at the International Criminal Court. West Point: Lieber Institute for Law & Land Warfare, 4. 10. 2023. Online: https://lieber.westpoint.edu/cyber-operations-crimes-icc/
[810] STERIO, Milena a TRAHAN, Jennifer: Cyber Operations as Crimes at the International Criminal Court. West Point: Lieber Institute for Law & Land Warfare, 4. 10. 2023. Online: https://lieber.westpoint.edu/cyber-operations-crimes-icc/

Kybernetické operácie môžu naplniť skutkovú podstatu **vojnových zločinov**, ak sa zameriavajú sa na chránenú civilnú infraštruktúru (napr. nemocnice, systémy zásobovania vodou), vytvárajú nerozlišujúce účinky porovnateľné s kinetickými útokmi, alebo zasahujú do humanitárnych operácií prostredníctvom digitálneho narušenia.

Kybernetické operácie môžu sprevádzať, umožňovať alebo byť súčasťou nezákonného použitia sily medzi štátmi, hoci takéto posúdenia zostávajú špecifické pre dané skutočnosti. Pre spáchanie **zločinu agresie** sa vyžaduje, aby porušenie Charty OSN bolo zjavné (manifest), čím sa zo skutkovej podstaty vylučujú konania ktoré sú „na hranici". Taktiež sa vedie diskusia o tom, či výpočet konaní v čl. 8bis Rímskeho štatútu ICC je taxatívny, prevažujúci názor je však v prospech jeho demonštratívneho výkladu[811]. Pre výklad pojmu „ozbrojená sila" je možné poukázať na poradný posudok Medzinárodného súdneho dvora v ktorom uviedol, že použitie sily sa posudzuje „bez ohľadu na použitú zbraň"[812]. Keďže má skutková podstata zločinu agresie definovaný špeciálny subjekt, tak ho môže spáchať len osoba v pozícii účinne kontrolovať politické alebo vojenské aktivity štátu. Naopak vylúčená je zodpovednosť predstaviteľov neštátnych entít. Ich zodpovednosť by prichádzala do úvahy len v prípade, ak by sa preukázalo, že konali pod kontrolou štátu, respektívne, že ich je potrebné posudzovať ako osoby konajúce v pozícii *de facto* orgánu štátu, ktorých konanie je štátu pripísateľné.

Napokon ak ide o digitálne zasahovanie do konaní Medzinárodného trestného súdu, ako napríklad manipulácia s dôkazmi, ovplyvňovanie svedkov online alebo hackovanie súdnych systémov, ide o **trestné činy marenia spravodlivosti**, ktoré patria do jurisdikcie Medzinárodného trestného súdu a bez potreby naplnenia prahu závažnosti (*gravity*), ktorá sa vyžaduje pre aktiváciu jurisdikcie ICC pri zmienených ústredných zločinoch (*core crimes*). Primerane to platí aj pre priestupky podľa čl. 71 Rímskeho štatútu MTS.

Zo skúsenosti Úradu prokuratúry ICC vyplýva, že kybernetické nástroje v súčasnosti slúžia skôr ako nástroje na uľahčenie než ako priame nástroje na spáchanie zločinu. Medzi príklady patria koordinácia ozbrojených skupín prostredníctvom šifrovanej komunikácie, využívanie kybernetických útokov na získaní informácií o zacielení, alebo nasadenie systémov umelej inteligencie na výber alebo sledovanie obetí. ICC môže vyvodiť

[811] ARONSSON-STORRIER, Marie: Article 8 bis (2). Lexsitus – CILRAP, aktualizované 20. 5. 2019. Dostupné na: https://cilrap-lexsitus.org/en/clicc/8-bis/8-bis-2.
[812] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1. C.J. Reports 1996, s. 244, ods. 39.

zodpovednosť páchateľov aj účastníkov, ak vedome prispievajú k spáchaniu trestných činov prostredníctvom takejto digitálnej podpory.

Od zločinov podľa medzinárodného práva je potrebné odlišovať **zmluvne založené trestné činy** (treaty based crimes), pri ktorých individuálna trestná zodpovednosť závisí od splnenia implementačnej povinnosti štátom. Ide o medzinárodné zmluvy, ktoré spravidla kombinujú hmotnoprávny aspekt (definovanie konaní, ktoré štáty majú implementovať vo svojej trestnej legislatíve), ako aj procesnoprávny aspekt (spolupráca v trestných veciach). Najvýznamnejšími prameňmi v tomto ohľade a v kontexte kybernetických operácií sú (**Budapeštiansky) Dohovor (Rady Európy) o počítačovej kriminalite** z roku 2001, v znení neskorších protokolov (najnovší z roku 2021) [813], a **(Hanojský) Dohovor OSN proti počítačovej kriminalite** z roku 2024.

V hmotnoprávnej rovine Dohovor OSN proti počítačovej kriminalite stanovuje záväzok štátov kriminalizovať konanie ako je neoprávnený prístup k systému informačných a komunikačných technológií alebo trestné činy súvisiace so sexuálnym zneužívaním detí online, ktoré budú predmetom nasledujúcej podkapitoly. Vo vzťahu k **právnickým osobám** stanovuje zväzok vyvodzovať zodpovednosť, avšak rešpektujúc tradíciu toho-ktorého štátu, táto zodpovednosť nemusí byť trestnoprávna, ale môže byť zakotvená aj v režime správneho alebo civilného práva. To možno považovať v súčasnosti za prevažujúci prístup medzinárodného práva k zodpovednosti právnických osôb[814].

11.2 Ochrana práv detí v digitálnom prostredí

Z predchádzajúcej časti vyplynulo, že digitálny priestor podlieha suverenite štátov a predstavuje prostredie, v ktorom sa aplikuje medzinárodné právo. Popri vyššie skúmanom bezpečnostnom rozmere tejto problematiky je potrebné zdôrazniť, že ide zároveň o priestor, v ktorom sa realizujú aj práva iných subjektov medzinárodného práva, predovšetkým práva jednotlivca ako nositeľa ľudských práv[815].

[813] Bližšie pozri napr. FUNTA, Rastislav: *Dohovor Rady Európy o počítačovej kriminalite (Budapeštiansky dohovor): komentár*. Bratislava: Wolters Kluwer, 2021. 136 s. KRÁLIK, Ján: Aktuálne výzvy v oblasti kybernetickej kriminality: návrh druhého dodatkového protokolu k Dohovoru Rady Európy o počítačovej kriminalite In: *Míľniky práva v stredoeurópskom priestore 2021: zborník z medzinárodnej vedeckej konferencie*. Bratislava: Právnická fakulta UK v Bratislave, 2021, s. 11-22.

[814] MAREČEK, Lukáš: Criminal liability of legal persons under international law - retrospection and current status. In: *The Lawyer Quarterly* . Vol. 10, No. 4 (2020), s. 413-425.

[815] SVÁK, Ján – MAREČEK, Lukáš a kol.: *Medzinárodné právo verejné a úvod do verejného medzinárodného práva.* Bratislava: Wolters Kluwer, 2024, s. 795.

V súčasnosti je uznávanou zásadou, že rovnaké práva, aké majú jednotlivci offline, musia byť chránené aj online[816].

Osobitne zraniteľnou skupinou v digitálnom prostredí sú deti, pre ktoré tento priestor na jednej strane vytvára nové možnosti komunikácie, vzdelávania a participácie na spoločenskom živote, na druhej strane prináša riziká, akými sú napríklad zásahy do práva na súkromie, neoprávnené spracúvanie osobných údajov, vystavenie škodlivému alebo nezákonnému obsahu, kyberšikana, online grooming či komerčné vykorisťovanie[817].

Z uvedených dôvodov sa ochrana detí v digitálnom prostredí postupne dostáva do centra pozornosti medzinárodného spoločenstva. Štáty v tejto oblasti uzatvárajú medzinárodné zmluvy zamerané na harmonizáciu trestného práva a zároveň rozvíjajú ľudskoprávne nástroje, ako aj regulačné mechanizmy vo vzťahu k činnosti súkromných aktérov.

Nasledujúce časti sa zameriavajú na univerzálny a európsky regionálny právny rámec ochrany práv dieťaťa v digitálnom prostredí a na povinnosti štátov, ktoré z neho vyplývajú, s osobitným dôrazom na reguláciu činnosti súkromných aktérov.

11.2.1 Univerzálna úroveň ochrany detí v digitálnom prostredí

Východiskový normatívny rámec pre medzinárodnoprávnu ochranu detí v digitálnom prostredí predstavuje **Dohovor o právach dieťaťa** (20. novembra 1989). Hoci bol tento dohovor prijatý ešte pred masovým rozšírením internetu a digitálnych technológií a výslovne neobsahuje ustanovenia týkajúce sa digitálneho priestoru, je plne použiteľný aj v digitálnom prostredí[818].

Z hľadiska digitálneho prostredia majú osobitný význam napríklad článok 16 Dohovoru o právach dieťaťa, garantujúci právo na súkromný a rodinný život a ochranu pred zásahmi a útokmi na česť a povesť, ktorý je plne aplikovateľný na neoprávnené spracúvanie osobných údajov či zverejňovanie citlivých informácií. Článok 17, upravujúci prístup k vhodným informáciám nadobúda osobitný význam v kontexte digitálnych platforiem. Z

[816] MAČÁK, Kubo – DIAS, Talita – KASPER, Á.: Handbook on Developing a National Position on International Law and Cyber Activities, A Practical Guide for States. University of Exeter, 2025, s. 104.
[817] HOLMARSDOTTIR, Halla: The Digital Divide: Understanding Vulnerability and Risk in Children and Young People's Everyday Digital Lives. In: HOLMARSDOTTIR, Halla – SELAND, I. – HYGGEN, Christer – ROTH, Maria (eds): *Understanding The Everyday Digital Lives of Children and Young People.* Cham: Palgrave Macmillan, 2024, s. 57-82.
[818] LIEVENS, Eva.: *Protecting Children in the Digital Era: The Use of Alternative Regulatory Instruments.* Leiden – Boston: Brill / Nijhoff, 2010. s. 265.

hľadiska ochrany detí pred vykorisťovaním má osobitný význam článok 34, ktorý zaväzuje štáty chrániť deti pred všetkými formami sexuálneho vykorisťovania a zneužívania, čo zahŕňa aj online formy takéhoto konania[819].

Osobitné postavenie v rámci univerzálneho systému ochrany detí majú opčné protokoly k Dohovoru o právach dieťaťa. Tieto možno rozdeliť na substantívne a procedurálne. Medzi substantívne patrí **Opčný protokol k Dohovoru o právach dieťaťa o zapojení detí do ozbrojených konfliktov** (25. mája 2000) a **Opčný protokol k Dohovoru o právach dieťaťa o predaji detí, detskej prostitúcii a detskej pornografie** (25. mája 2000). Procedurálny charakter má **Opčný protokol k Dohovoru o právach dieťaťa o procedúre oznámení** (19. decembra 2011).

Opčný protokol k Dohovoru o právach dieťaťa o zapojení detí do ozbrojených konfliktov (25. mája 2000) nadväzuje na článok 38 Dohovoru a zakotvuje povinnosti zmluvných štátov týkajúce sa možnosti povolávania detí do ozbrojených síl (ako zo strany štátu, tak aj zo strany skupín odlišných od štátu), záruk dobrovoľného povolávania, minimálneho veku pre dobrovoľné povolávanie, zákaz umožnenia priamej účasti v bojových akciách deťom vo veku medzi 15 a 18 rokov (ako členom ozbrojených síl) a tiež povinnosť prevencie a trestania praktík, ktoré sú podľa tohto protokolu zakázané[820]. V digitálnom prostredí nadobúda význam otázka účasti detí na kybernetických nepriateľských operáciách. Na tento aspekt reaguje Tallinský manuál zákazom umožnenia účasti osôb mladších ako 15 rokov na nepriateľských kybernetických operáciách[821].

Opčný protokol k Dohovoru o právach dieťaťa o predaji detí, detskej prostitúcii a detskej pornografii (25. mája 2000) posilňuje ochranu detí pred ich predajom, detskou prostitúciou a zneužívaním na účely detskej pornografie a to nad rámec štandardov stanovených v článku 34 Dohovoru o právach dieťaťa. Hoci tento protokol neobsahuje osobitné ustanovenia o digitálnom prostredí, už v jeho preambule vyjadrujú zmluvné štáty znepokojenie nad narastajúcou dostupnosťou detskej pornografie na internete a prostredníctvom nových technológií. V hmotnoprávnej rovine tento opčný protokol

[819] KOLTAY, András: European Law. In: HALÁSZ, Csenge: *Children in Digital Age*. Miskolc – Budapest: Central European Academic Publishing, 2025, s. 69 – 70.
[820] DUŠKOVÁ, Šárka – HOFSCHNEIDEROVÁ, Anna - KOUŘILOVÁ, Kamila: Úmluva o právech dítěte. Komentář: Praha: Wolters Kluwer ČR, 2021, dostupné cez smarteca.cz.
[821] SCHMITT, Michael – VIHUL, Liis (eds.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017. s. 524-525.

stanovuje záväzok štátov kriminalizovať konanie ako je predaj detí, detská prostitúcia a detská pornografia vrátane pokusov o ich spáchanie či účasti na nich. Protokol zakotvuje záväzok zmluvných štátov k medzinárodnej spolupráci pri trestnom konaní, vyšetrovaní a vydávacom konaní a tiež procesné práva dieťaťa – obete v trestnom konaní, ktorého predmetom je niektoré z týchto konaní a tiež právo dieťaťa na prevenciu pred týmto konaní a to na úrovni primárnej, sekundárnej a terciárnej prevencie. V kontexte aplikácie ustanovení tohto dohovoru v digitálnom prostredí je významným právne nezáväzným dokumentom Usmernenie[822] výboru pre práva dieťaťa k implementácii Opčného protokolu k Dohovoru o právnych dieťaťa o predaji detí, detskej prostitúcii a detskej pornografii[823].

Opčný protokol k Dohovoru o právach dieťaťa o procedúre oznámení posilňuje vykonateľnosť práv dieťaťa podľa Dohovoru, pretože popri existujúcej monitorovacej funkcii Výboru pre práva dieťaťa zavádza individuálny (a za určitých podmienok aj medzištátny a vyšetrovací) mechanizmus kontroly dodržiavania práv dieťaťa. Tento Opčný protokol *„je univerzálnou medzinárodnou zmluvou zakotvujúcou možnosť a postup podávania oznámení (sťažností) zo strany jednotlivcov, skupiny jednotlivcov alebo v mene jednotlivca či skupiny jednotlivcov, v prípadoch porušenia práv garantovaných Dohovorom o právach dieťaťa alebo niektorým z jeho substantívnych protokolov"*[824].

Priama vykonateľnosť jednotlivých ustanovení Dohovoru o právach dieťaťa a jeho substantívnych opčných protokolov závisí od ústavného a právneho systému jednotlivých zmluvných štátov a ich implementácia je tak do značnej miery ponechaná na zmluvné štáty[825]. Dohovor a jeho protokoly preto slúžia najmä ako základný normatívny rámec, na základe ktorého sa posudzujú legislatívne a politické opatrenia v oblasti ochrany práv detí[826]. Významným interpretačným príspevkom k aplikácii Dohovoru a opčných protokolov v digitálnom kontexte je **Všeobecný komentár č. 25 Výboru OSN pre práva dieťaťa o právach dieťaťa v súvislosti s digitálnym prostredím (2021)**. Tento dokument zdôrazňuje, že *„práva*

[822] Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (CRC/C/156)

[823] DUŠKOVÁ, Šárka – HOFSCHNEIDEROVÁ, Anna - KOUŘILOVÁ, Kamila: Úmluva o právech dítěte. Komentář: Praha: Wolters Kluwer ČR, 2021, dostupné cez smarteca.cz.

[824] DOBROVODSKÝ, Róbert: K novému medzinárodnému mechanizmu ochrany práv detí. In: JURČOVÁ, Monika – DOBROVODSKÝ, Róbert – NEVOLNÁ, Zuzana - ŠTEFANKO, Jozef (eds.): *Liber amicorum Lazar.* Trnava: Universitatis Tyrnaviensis, 2014, s. 175.

[825] LIEVENS, Eva.: *Protecting Children in the Digital Era: The Use of Alternative Regulatory Instruments*. Leiden – Boston: Brill / Nijhoff, 2010, s. 267.

[826] LIS, Wojciech: UN Convention on the Rights of the Child: Protection. In: BENYUSZ Márta – RAISZ Anikó (eds.): *International Children's Rights.* Miskolc–Budapest, Central European Academic Publishing, 2024. s. 93.

každého dieťaťa musia byť v digitálnom svete rešpektované, chránené a napĺňané" a poskytuje štátom návod pri prijímaní legislatívnych, politických a iných opatrení.

Popri uvedených nástrojoch je potrebné poukázať aj na rozvíjajúci sa univerzálny trestnoprávny rámec v podobe **(Hanojského) Dohovoru OSN proti počítačovej kriminalite z roku 2024**[827], ktorého cieľom je harmonizácia kriminalizácie páchania určitých trestných činov súvisiacich s kybernetickým priestorom a to vrátane sexuálneho zneužívania detí, groomingu a šírenia intímnych snímok bez udelenia súhlasu (články 14 až 16). Zmluvné strany tohto dohovoru sa tiež zaväzujú spolupracovať pri vyšetrovaní a stíhaní trestných činov, na ktoré sa dohovor vzťahuje.

Popri právne záväzných nástrojoch zohrávajú významnú úlohu aj právne nezáväzné dokumenty, ktoré prispievajú k formovaniu univerzálnych štandardov ochrany práv detí v digitálnom prostredí. Príkladom je **Globálny digitálny pakt** prijatý v roku 2024, v ktorom sa štáty zaviazali posilňovať právne a politické rámce ochrany práv dieťaťa v digitálnom prostredí a podporovať tvorbu a implementáciu vnútroštátnych politík a štandardov online bezpečnosti detí. Dokument zároveň zdôrazňuje potrebu prevencie a potláčania sexuálneho vykorisťovania a zneužívania detí v online prostredí a apeluje na súkromný sektor, aby rešpektoval ľudské práva a postupoval v súlade so všeobecnými zásadami OSN o podnikaní a ľudských právach. V rovnakom roku prijalo Valné zhromaždenie OSN prvú globálnu rezolúciu o umelej inteligencii, ktorá zdôrazňuje potrebu využívania umelej inteligencie v súlade s medzinárodným právom, najmä s požiadavkami ochrany ľudských práv a osobných údajov.

11.2.2 Povinnosti štátov a súkromných aktérov podľa Dohovoru o právach dieťaťa a jeho substantívnych opčných protokolov

V digitálnom priestore môže negatívne vplývať na práva detí, prípadne tieto práva priamo porušovať nielen činnosť alebo opomenutie štátov ale aj súkromných aktérov. Nositeľmi medzinárodnoprávnych povinností v oblasti ochrany ľudských práv sú však štáty. Dohovor o právach detí zakotvuje súbor práv detí, ktorým zodpovedá konkrétny rozsah povinností zmluvných štátov[828]. V súlade so všeobecnou doktrínou ochrany ľudských práv

[827] Tento dohovor k januáru 2026 nenadobudol platnosť.
[828] Všeobecný komentár č. 16 (2013) o povinnostiach štátu v súvislosti s vplyvom podnikateľského sektora na práva detí, bod 24.

majú štáty trojitý typ povinností, a to povinnosť práva dieťaťa rešpektovať, chrániť a napĺňať. V zásade ochrana každého práva vyžaduje naplnenie všetkých troch povinností, hoci jedna povinnosť môže byť výraznejšia ako ostatné v závislosti od povahy práva.[829]

Povinnosť rešpektovať predstavuje negatívnu povinnosť štátu zdržať sa zásahov do práv detí.[830] Štát pritom nesie medzinárodnoprávnu zodpovednosť za konanie alebo opomenutie svojich orgánov, a to aj v prípadoch, keď konajú *ultra vires*. Povinnosť chrániť má pozitívny charakter a vyžaduje, aby štát prijal primerané legislatívne, administratívne alebo súdne opatrenia na ochranu práv detí pred zásahmi zo strany tretích strán. Ak dôjde k porušeniu práv dieťaťa zo strany súkromného subjektu, štát nenesie zodpovednosť za samotné konanie tohto subjektu, môže však niesť zodpovednosť za nesplnenie pozitívneho záväzku štátu.[831] Povinnosť napĺňať zaväzuje štáty prijať *„všetky potrebné zákonodarné, správne a iné opatrenia*" na zabezpečenie realizácie práv garantovaných Dohovorom a jeho opčnými protokolmi pre všetky deti vo svojej jurisdikcii[832] bez diskriminácie. Rozsah týchto opatrení závisí od dostupných zdrojov.

Osobitnú otázku predstavuje postavenie súkromných aktérov. Medzinárodné právo im neukladá priame, právne záväzné povinnosti rešpektovať, chrániť a napĺňať práva dieťaťa. Povinnosť zabezpečiť, aby súkromní aktéri rešpektovali práva dieťaťa spočíva na štátoch, ktoré ju realizujú prostredníctvom regulácie, dohľadu a presadzovania práva.[833]

---

[829] SZALAYNÉ SÁNDOR Erzsébet: Regional Human Rights Protection Systems - Introduction. In: RAISZ Anikó (ed.): *Children's Rights in Regional Human Rights Systems.* Miskolc–Budapest, Central European Academic Publishing, 2024. s. 27.

[830] Všeobecný komentár č. 16 (2013) o povinnostiach štátu v súvislosti s vplyvom podnikateľského sektora na práva detí, body 26, 27

[831] ILA Group on Due Diligence in International Law. First Report. Dostupné online: olympereseauinternational.wordpress.com/wp-content/uploads/2015/07/due_diligence_-_first_report_2014.pdf d. 15 Ako uvádzajú slovenskí autori *„pozitívny záväzok nie je záväzkom určitého výsledku, ale záväzok postupu či správania sa. Štát nemá povinnosť garantovať absolútnu ochranu (čo by bolo fakticky nemožné), ale má povinnosť postupovať s náležitou starostlivosťou. Povedané zjednodušenie, štát nemá kapacity na absolútnu ochranu ľudských práv, ale má vynaložiť svoje kompetencie a inštitúcie k vykonaniu racionálnych krokov, aby neprišlo k porušeniu práva, resp. ak k porušeniu príde, tak k reštitúcii.*" ĽALÍK, T. a kol. Ochrana základných práv. 1. vydanie. Bratislava : WoltersKluwer SR s. r. o., 2026, s. 19 a 20. Ako uvádza Šturma s pojmom náležitej starostlivosti štátov sa je možné stretnúť v rôznych oblastiach medzinárodného práva a v modifikovanej podobe sa uplatňuje aj pri ochrane ľudských práv. ŠTURMA, Pavel: *„Náležitá péče*" *v mezinárodním právu: obecný pojem s variabilným obsahem.* In Právník, č. 6, 2021, s. 414.

[832] Všeobecný komentár č. 5 (2003) Výboru OSN pre práva dieťaťa, všeobecné vykonávacie opatrenia Dohovoru o právach dieťaťa (čl. 4, 42 a 44 ods. 6), bod 1

[833] KRAJEWSKI, Markus: *Mandatory Human Rights Due Diligence Laws? Blurring the Lines between State Duty to protect and Corporate Responsibility to Respect?* In: Nordic Journal of Human Rights, roč. 41, 2023, č. 3: Special Issue on Corporate Human Rights Responsobilities. s. 221 – 237.

Absenciu priamo záväzných medzinárodnoprávnych povinností pre súkromných aktérov čiastočne kompenzujú nástroje soft law, najmä Usmernenia OSN o podnikaní a ľudských právach. Tie vychádzajú z rozlíšenia medzi povinnosťou štátu chrániť ľudské práva a zodpovednosťou podnikov tieto práva rešpektovať. Jadrom tejto zodpovednosti je uplatňovanie náležitej starostlivosti (*due diligence*) v oblasti ľudských práv.

Výbor pre práva dieťaťa vo svojom všeobecnom komentári č. 16 potvrdzuje, že hoci neexistuje univerzálny právne záväzný nástroj upravujúci povinnosti podnikateľských subjektov, požiadavka rešpektovania práv dieťaťa sa v praxi vzťahuje aj na súkromný sektor. Zmluvné štáty sú povinné dbať na to, aby súkromný sektor dodržiaval svoje povinnosti súvisiace s rešpektovaním práv dieťaťa. V tejto súvislosti Výbor pre práva dieťaťa zdôrazňuje, že štáty by mali od podnikateľských subjektov vyžadovať uplatňovanie *due diligence* vo vzťahu k právam detí, čo umožní identifikovať, predchádzať a zmierňovať negatívne vplyvy ich činností na práva detí. [834]

11.2.3 Európsky regionálny systém ochrany práv dieťaťa

Na univerzálny rámec ochrany práv dieťaťa nadväzuje európsky regionálny rámec, ktorý všeobecné štandardy obsiahnuté najmä v Dohovore o právach dieťaťa a jeho opčných protokoloch ďalej rozvíja a dopĺňa o špecifické mechanizmy ochrany a kontroly. Tento rámec, tvorený najmä činnosťou Rady Európy a Európskej únie, nenahrádza univerzálnu úroveň ochrany.

11.2.3.1 Rada Európy

Na úrovni Rady Európy doposiaľ nebol prijatý medzinárodný dohovor, ktorý by komplexne upravoval práva dieťaťa alebo osobitne práva detí v digitálnom prostredí. Ochrana práv detí sa preto realizuje prostredníctvom existujúcich ľudskoprávnych nástrojov, predovšetkým **Európskeho dohovoru o ochrane ľudských práv a základných slobôd a jeho dodatkových protokolov** (ďalej len „EDĽP") a **Európskej sociálnej charty**, ako aj prostredníctvom špecializovaných dohovorov a nástrojov *soft law*.

[834] V Európskej únii je v tomto smere relevantnou Smernica Európskeho parlamentu a Rady (EÚ) 2024/1760 z 13. júna 2024 o náležitej starostlivosti podnikov v oblasti udržateľnosti a o zmene smernice (EÚ) 2019/1937 a nariadenia (EÚ) 2023/2859

EDĽP predstavuje základný pilier ochrany práv jednotlivcov v rámci Rady Európy. Hoci neobsahuje osobitnú úpravu práv dieťaťa a ani explicitne nereflektuje digitálne prostredie, viaceré jeho ustanovenia sú priamo relevantné aj v tomto kontexte. Ide napríklad o právo na rešpektovanie súkromného a rodinného života podľa článku 8 EDĽP či právo na vzdelanie podľa článku 2 Dodatkového protokolu č. 1.

Kontrolu dodržiavania záväzkov vyplývajúcich z EDĽP zabezpečuje Európsky súd pre ľudské práva (ďalej len „ESĽP"), ktorý prejednáva medzištátne a individuálne sťažnosti. Aj ESĽP vo svojej rozhodovacej činnosti rozvinul koncept pozitívnych záväzkov štátu, ktorý umožňuje presadzovanie tzv. horizontálneho účinku ľudských práv. *„V zmysle tejto teórie niektoré články EDĽP nielenže chránia jednotlivca proti štátu, ale aj zaväzujú štát chrániť jednotlivca proti konaniu tretej osoby."*[835]

V tejto súvislosti je relevantné napríklad rozhodnutie ESĽP vo veci *K.U. proti Fínsku* (z 2. decembra 2008, č. 2872/02), ktoré sa týkalo zlyhania fínskych orgánov pri zabezpečení primeranej ochrany práva 12-ročného chlapca na rešpektovanie súkromného života podľa článku 8 EDĽP. Vec sa týkala uverejnenia inzerátu na internetovej zoznamke, obsahujúceho podrobné informácie o jeho fyzickom vzhľade, ako aj ďalšie osobné údaje vrátane dátumu narodenia a kontaktných údajov. Súd konštatoval, že právo sťažovateľa podľa článku 8 EDĽP bolo porušené, pretože štát nesplnil svoje pozitívne povinnosti vyplývajúce z EDĽP zabezpečiť účinné opatrenia na ochranu súkromného života sťažovateľa.[836]

Doplnkový význam má **Európska sociálna charta** z roku 1961 v znení Revidovanej sociálnej charty z roku 1996, ktorá zakotvuje sociálne a ekonomické práva detí a zdôrazňuje pozitívne záväzky štátov zabezpečiť ich ochranu. Kontrolu dodržiavania týchto záväzkov vykonáva Európsky výbor pre sociálne práva prostredníctvom systému národných správ a kolektívnych sťažností.

Popri všeobecných ľudskoprávnych nástrojoch zohrávajú významnú úlohu aj špecializované dohovory Rady Európy, najmä Dohovor o ochrane jednotlivcov pri automatizovanom spracúvaní osobných údajov[837], Dohovor o počítačovej kriminalite z roku

[835] SVÁK, Ján – GRŰNWALD, Tomáš: *Nadnárodné systémy ochrany ľudských práv, I. zväzok. Štruktúra systémov a ochrana politických práv.* Bratislava: Wolters Kluwer, 2019, s.71.
[836] VLAŠKOVIĆ, Veljko: *Children's Rights in the Council of Europe - Framework.* In: RAISZ Anikó (ed.): Children's Rights in Regional Human Rights Systems. Miskolc–Budapest, Central European Academic Publishing, 2024. s. 49.
[837] Dohovor o ochrane jednotlivcov pri automatizovanom spracúvaní osobných údajov z roku 1981 (Convention 108), je jedinou právne záväznou mnohostrannou medzinárodnou zmluvnou v oblasti ochrany osobných údajov

2001 (tzv. Budapeštiansky dohovor)[838], Lanzarotský dohovor o ochrane detí pred sexuálnym vykorisťovaním a sexuálnym zneužívaním, ako aj Rámcový dohovor o umelej inteligencii, ľudských právach, demokracii a právnom štáte.[839] Tieto medzinárodné zmluvy dopĺňajú všeobecný rámec ochrany práv detí o konkrétne povinnosti štátov v oblastiach ochrany súkromia, boja proti kybernetickej kriminalite a prevencie sexuálneho zneužívania detí v online prostredí a zabezpečenia ochrany ľudských práv v súvislosťami s činnosťami počas životného cyklu systémov umelej inteligencie.

Popri právne záväzných nástrojoch zohrávajú významnú úlohu aj nástroje tzv. soft law, najmä odporúčania prijímané Výborom ministrov Rady Európy. Najvýznamnejším dokumentom v tejto oblasti je Odporúčanie CM/Rec(2018)7 Výboru ministrov členským štátom o Usmerneniach na rešpektovanie, ochranu a napĺňanie práv dieťaťa v digitálnom prostredí.

11.2.3.2 Európska únia

Na rozdiel od systému Rady Európy disponuje Európska únia vlastným autonómnym systémom ochrany základných práv, ktorý je záväzný nielen pre členské štáty, ale aj pre samotnú Úniu. Tento systém[840] je založený najmä na Charte základných práv Európskej únie, ktorá má od nadobudnutia účinnosti Lisabonskej zmluvy právnu silu primárneho práva (článok 6 ZEÚ).[841]

---

fyzických osôb a teda aj detí. Táto medzinárodná zmluva bola modernizovaná prijatím protokolu (tzv. Convention 108+), ktorý Slovenská republika ratifikovala, avšak zatiaľ nevstúpil do platnosti.

[838] Dohovor o počítačovej kriminalite z roku 2001 (tzv. Budapeštiansky dohovor) je prvou právne záväznou zmluvou komplexne upravujúcou problematiku kybernetickej kriminality. Dohovor je otvorený aj pre nečlenské štáty Rady Európy a presahuje regionálny rámec. Jeho hlavným prínosom je harmonizácia trestnoprávnych skutkových podstát kybernetickej kriminality a vytvorenie mechanizmov medzinárodnej spolupráce pri vyšetrovaní a stíhaní páchateľov. Dohovor výslovne kriminalizuje aj viaceré formy protiprávneho konania súvisiace s detskou pornografiou (článok 9 Budapeštianskeho dohovoru). Významným posunom je Druhý dodatkový protokol k dohovoru, ktorý modernizuje pravidlá získavania a výmeny elektronických dôkazov a reaguje tak na technologický vývoj a potrebu efektívnej cezhraničnej spolupráce.

[839] Tento dohovor k 01. 03. 2026 nevstúpil do platnosti.

[840] Bližšie k tomu pozri SVÁK, Ján – MAREČEK, Lukáš a kol.: *Medzinárodné právo verejné a úvod do verejného medzinárodného práva.* Bratislava: Wolters Kluwer, 2024 v časti 4.3.1 Regionálny systém ochrany ľudských práv na úrovni Európskej únie.

[841] SZALAYNÉ SÁNDOR Erzsébet: Regional Human Rights Protection Systems - Introduction. In: RAISZ Anikó (ed.): *Children's Rights in Regional Human Rights Systems.* Miskolc–Budapest, Central European Academic Publishing, 2024. s. 34.

Lisabonská zmluva zároveň posilnila postavenie práv dieťaťa v rámci práva EÚ, keď „ochranu práv dieťaťa" zakotvila ako jeden zo všeobecných cieľov Únie (článok 3 ods. 3 ZEÚ) a ako zásadu uplatňovanú v jej vonkajšej činnosti (článok 3 ods. 5 ZEÚ).

Osobitný význam pre ochranu práv detí má článok 24 Charty základných práv EÚ, ktorý explicitne zakotvuje práva dieťaťa a vychádza z Dohovoru o právach dieťaťa, najmä z princípu najlepšieho záujmu dieťaťa.[842]

Pre členské štáty sú ustanovenia Charty základných práv EÚ záväzné len vtedy, ak vykonávajú právo Únie (článok 51 ods. 1 Charty), čo potvrdzuje aj judikatúra Súdneho dvora Európskej únie, najmä vo veci C-617/10 *Åkerberg Fransson*. Charta preto len dopĺňa vnútroštátne systémy ochrany práv dieťaťa členských štátov EÚ, nenahrádza nich.

V prípade porušenia povinností, ktoré členským štátom vyplývajú z Charty základných práv EÚ môže Európska komisia iniciovať konanie o nesplnenie povinnosti podľa článku 258 ZFEÚ, keďže Charta má právnu silu primárneho práva.

Rozsah právomocí Európskej únie v oblasti ochrany detí v digitálnom priestore nie je vymedzený jednotne, keďže ide o prierezovú oblasť. Únia môže konať len v rozsahu právomocí zverených zakladajúcimi zmluvami, pričom relevantné opatrenia prijíma najmä v rámci jednotlivých sektorových politík.

V kontexte digitálneho prostredia ide predovšetkým o oblasti

- **vnútorného trhu** (čl. 114 ZFEÚ) v tejto oblasti boli prijaté napr. Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách) Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii)

  Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/988 z 10. mája 2023 o všeobecnej bezpečnosti výrobkov, ktorým sa mení nariadenie Európskeho parlamentu a Rady (EÚ) č. 1025/2012 a smernica Európskeho parlamentu a Rady

[842] Pozri Vysvetlivky k Charte základných práv (2007/C 303/02).

(EÚ) 2020/1828 a zrušuje smernica Európskeho parlamentu a Rady 2001/95/ES a smernica Rady 87/357/EHS

Smernica Európskeho parlamentu a Rady (EÚ) 2024/1760 z 13. júna 2024 o náležitej starostlivosti podnikov v oblasti udržateľnosti a o zmene smernice (EÚ) 2019/1937 a nariadenia (EÚ) 2023/2859

- **ochrany osobných údajov a súkromia** (čl. 16 ZFEÚ) v tejto oblasti boli prijaté napr. GDPR
- **ochrana spotrebiteľa** (čl. 169 ZFEÚ) v tejto oblasti boli prijaté napr. Smernica Európskeho parlamentu a Rady 2005/29/ES z 11. mája 2005 o nekalých obchodných praktikách podnikateľov voči spotrebiteľom na vnútornom trhu, a ktorou sa mení a dopĺňa smernica Rady 84/450/EHS, smernice Európskeho parlamentu a Rady 97/7/ES, 98/27/ES a 2002/65/ES a nariadenie Európskeho parlamentu a Rady (ES) č. 2006/2004 („smernica o nekalých obchodných praktikách")
- **priestor slobody, bezpečnosti a spravodlivosti** napr. Smernica Európskeho parlamentu a Rady 2011/93/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorou sa nahrádza rámcové rozhodnutie Rady 2004/68/SVV.

Právne akty prijaté v jednotlivých oblastiach majú zásadný význam pre ochranu detí v digitálnom prostredí, keďže z nich vyplývajú konkrétne povinnosti aj súkromným aktérom. Ide však o povinnosti vyplývajúce z práva EÚ, nie z medzinárodného práva.

Významnú úlohu v oblasti ochrana detí v digitálnom priestore zohráva aj judikatúra Súdneho dvora Európskej únie, ktorý sa pri výklade práva EÚ opakovane odvoláva na Dohovor o právach dieťaťa. Napríklad v rozsudku Súdneho dvora EÚ vo veci C-244/06 Dynamic Medien Vertriebs GmbH proti Avides Media AG Súdny dvor uznal, že obmedzenia voľného pohybu tovaru môžu byť odôvodnené ochranou detí pred škodlivým obsahom, pričom sa výslovne odvolal na článok 17 Dohovoru o právach dieťaťa.

Popri právne záväzných nástrojoch prijíma Európska únia aj dokumenty soft law, ktoré dopĺňajú právny rámec. Ide napríklad o strategické dokumenty, usmernenia a samoregulačné iniciatívy, ako napríklad stratégia EÚ pre práva dieťaťa, iniciatíva Better Internet for Kids (BIK+). Tieto nástroje síce nemajú právne záväzný charakter, no významne prispievajú k formovaniu štandardov ochrany detí a ovplyvňujú legislatívnu aj aplikačnú prax.

12. KYBERNETICKÁ KRIMINALITA

12.1 Všeobecne

Internet a v širšom ponímaní kybernetický priestor ovplyvnil všetky vrstvy spoločnosti, pretože odstránil prekážky medzi krajinami a umožnil vysokú interakciu medzi ich obyvateľmi. Rovnako tak aj mnohé biznis modely sú postavené na nepretržitej dostupnosti internetu a bezproblémovom fungovaní informačných systémov.

Závažná a organizovaná trestná činnosť sa vyvíja rýchlym tempom. Trestná činnosť sa stáva čoraz sofistikovanejšou, čo postupne ovplyvňuje i stabilitu spoločnosti, pričom nelegálne aktivity sa čoraz viac objavujú najmä online. Umelá inteligencia (AI) a iné špičkové technológie umožňujú rozvoj nezákonnej stránky digitálnej revolúcie, pričom páchatelia kybernetickej kriminality ju využívajú najmä na zvýšenie rozsahu a efektívnosti svojich aktivít. Online prostredie sa stalo neoddeliteľnou a všadeprítomnou súčasťou nášho života. V súčasnosti sa široká škála trestných činností odohráva prevažne alebo výlučne online, pričom digitálna infraštruktúra a údaje, ktoré obsahuje, sa stávajú hlavnými cieľmi páchateľov kybernetickej kriminality.

Údaje sa stali kľúčovou komoditou, ktorá slúži nielen ako objekt útoku kybernetickej kriminality. Ich hodnota spočíva v schopnosti zjednodušiť rôzne druhy trestných činností, vrátane kybernetických útokov, online podvodov, sexuálneho zneužívaní detí online a vydierania. V dôsledku toho prudko stúpa dopyt po údajoch a očakáva sa, že nelegálny obchod s nimi ešte viac porastie, čo prispeje k destabilizácii legitímnej ekonomiky. Krádeže a ohrozenie osobných údajov môže mať vážne dôsledky, ktoré narušujú fungovanie spoločnosti a majú závažný vplyv na postihnuté osoby. Páchatelia kybernetickej kriminality využívajú umelú inteligenciu na automatizáciu útokov, sociálne inžinierstvo a obchádzanie bezpečnostných opatrení, čo umožňuje kybernetické útoky škálovať a viesť ich komplexne. Techniky založené na umelej inteligencii môžu uľahčiť získavanie údajov, pričom samotné údaje môžu byť tiež použité ako zdroj v útokoch – napríklad na generovanie tzv. *deepfakes*, syntetických médií či falošnej identity.[843]

Niet pochýb o tom, že používanie sociálnych sietí, služieb v oblasti výmeny správ a iných aplikácií na komunikáciu, prácu, ako aj za účelom získavania informácií nám v mnohých smeroch uľahčuje každodenné fungovanie a je bežnou záležitosťou vo väčšine

[843] IOCTA 2025, EUROPOL, s. 6, dostupné dňa 29.11.2025 na: LINK

krajín sveta. Tieto služby navzájom spájajú stovky miliónov používateľov, poskytujú fórum na slobodu prejavu a z globálneho pohľadu predstavujú aj významný prínos v hospodárskej a sociálnej oblasti.

Páchatelia kybernetickej kriminality podnikajú rôzne aktivity smerujúce k zneužitiu informačno-komunikačných technológií a najmä dát ktoré sú buď:

- prostriedkom na páchanie protiprávnej činnosti,
- cieľom páchania protiprávnej činnosti, vrátane závažných trestných činov, ako sú teroristické útoky alebo
- komoditou s hospodárskou hodnotou.[844]

PRÍKLAD

V ostatných rokoch je v aplikačnej praxi dominantnou najmä tá forma kybernetickej kriminality, v rámci ktorej *sú informačno-komunikačné technológie prostriedkom na spáchanie inej trestnej činnosti.* Častokrát ide napríklad o trestnú činnosť majetkového charakteru, kde virtuálne prostredie a najmä jeho vyššia miera anonymity je zneužívané na páchanie trestných činov. Kyberzločin je preto takmer vždy spätý s ohrozením alebo poškodením práv, oprávnených záujmov a slobôd fyzických osôb a právnických osôb v tom najširšom možnom spektre. Odhaduje sa, že EU *scam* trh a trh s podvodnými platbami má hodnotu cca 4,5 mld. € ročne.[845] Celková škoda tzv. *cyber-enabled*[846] trestných činov v USA za rok 2024 predstavuje viac ako 16,6 mld. USD, čo predstavuje medziročný nárast škody o 33%.[847]

Vzhľadom na bezhraničnú povahu kybernetického priestoru je predmetná trestná činnosť častokrát páchaná zo zahraničia, resp. prostredníctvom zahraničia, čo významným spôsobom vplýva na možnosť získania relevantných dôkazov. Získanie neoprávneného prístupu k informačnému systému, krádež osobných údajov, požadovanie výkupného od spoločností, distribúcia detskej pornografie, to všetko je iba zlomok škodlivých aktivít páchaných v kybernetickom priestore. Páchateľmi čoraz rafinovanejších foriem kybernetickej kriminality sú zväčša profesionáli, ktorí za sebou zanechávajú minimum stôp a

[844] IOCTA 2025, EUROPOL, s. 11, dostupné dňa 29.11.2025 na: LINK
[845] 2024 REPORT ON PAYMENT FRAUD, EBA, 2024, s. 10, dostupné na: LINK
[846] Pozri ďalej.
[847] FBI Internet Crime Report 2024, s. 4 , dostupné dňa 06-02-2026 na: LINK

následné preukázanie viny v trestnom konaní sa javí byť až nadľudský výkon. Spoločným menovateľom tohto druhu trestnej činnosti sú nielen rozsiahle škody napáchané na majetku a iných právach osôb, ale v mnohých prípadoch nevyvodená akákoľvek právna zodpovednosť. Ide o druh trestnej činnosti, pri ktorom je odsúdenie osoby, o ktorej sa predpokladá, že trestný čin spáchala, mimoriadne náročným procesom a výsledok trestného stíhania býva častokrát neistý. Všetky uvedené skutočnosti sú potom v praxi reflektované v neúmernej dĺžke vyšetrovania, čo má dopad i na možnosť náležitého objasnenia skutkového stavu v rozsahu umožňujúcom vykonanie trestného stíhania proti konkrétnej osobe.

Súčasťou témy kybernetickej kriminality je i fenomén posledných rokov- kryptomeny, ktoré sa stali častým miestom uloženia výnosov z trestnej činnosti, ale i kanálom pre legalizáciu výnosov z trestnej činnosti, financovanie terorizmu, či obchádzanie reštriktívnych opatrení.

Kybernetická kriminalita je taktiež prítomná aj v oblasti medzinárodných zločinov, potom ako Medzinárodný trestný súd, začal vyhodnocovať napríklad počítačové útoky na nemocnice ako medzinárodné zločiny.[848]

Z pohľadu procesnej úpravy získavania elektronických dôkazov a digitálnych stôp je to využitie umelej inteligencie samotnými orgánmi činnými v trestnom konaní ako novej formy informačno-technického prostriedku,[849] kedy systémy s umelou inteligenciou budú vykonávať:

- profilovanie osoby, že sa stane páchateľom trestného činu[850]
- biometrickú kategorizáciu osôb,[851] alebo
- biometrickú identifikáciu osôb v reálnom čase.[852]

Vyšetrovanie počítačovej kriminality je z hľadiska rozsahu identifikovaných trestných činov a objemu generovaných údajov veľmi náročné na zdroje, čo ešte zhoršuje potreba náležitého počtu vyšetrovateľov so špecializovanými technickými a jazykovými zručnosťami.

[848] Draft Policy on the Cyber Enabled Crimes, Office of the Prosecutor, s. 20, dostupné dňa 06.02.2026 na: LINK
[849] Porovnaj §10 ods. 20 TP.
[850] Čl. 5 ods. 1, písm. d) Aktu o umelej inteligencii.
[851] Čl. 5 ods. 1, písm. g) Aktu o umelej inteligencii.
[852] Čl. 5 ods. 1, písm. h) Aktu o umelej inteligencii upravuje iba tzv. *live facial recognition* (LFR), identifikáciu v reálnom čase a nie identifikáciu osôb po spáchaní skutku tzv. *post event / after facial recognition* (AFR), čo predstavuje bežný postup orgánov presadzovania práva porovnávania tvárí napr. z bezpečnostných kamier po spáchaní skutku počas pátrania po horúcej stope. Porovnaj AI and Policing, EUROPOL, s. 24, dostupné dňa 21.10.2025 na: LINK

V tejto súvislosti sú partnerstvá základom úspešného vyšetrovania a stíhania počítačovej kriminality. Aktívna spolupráca so súkromným sektorom by mala byť prioritou, aby sa zabezpečilo, že trestné činy spáchané prostredníctvom internetu budú riadne objasnené. Poskytovatelia internetových služieb aj organizácie zaoberajúce sa bezpečnosťou internetu monitorujú internet z hľadiska podozrivej prevádzky: orgány činné v trestnom konaní môžu preto využívať ich zdroje a technické zručnosti na účinnejšie vyšetrovanie a trestné stíhanie počítačovej kriminality ako i zlepšovanie svojich operatívnych znalostí o trestných činoch spáchaných prostredníctvom internetu.[853]

12.2 Pojem kybernetická kriminalita

Je potrebné zdôrazniť, že univerzálna legálna definícia pojmu kybernetická kriminalita nebola doposiaľ prijatá. Vzhľadom na to, že existuje niekoľko teoretických prístupov k definovaniu pojmu kybernetická kriminalita, ktoré však presahujú potreby tejto učebnice, pokúsime sa ozrejmiť iba niektoré z nich a v ďalšom texte interpretovať tento pojem v intenciách Budapeštianskeho dohovoru.[854]

PRÍKLAD

Pojem kybernetická kriminalita možno vnímať podobne ako pojmy mravnostná kriminalita, ekonomická kriminalita či majetková kriminalita. Tieto názvy označujú skupiny trestných činov, ktoré majú určitého spoločného menovateľa, napríklad v podobe objektu ako chráneného záujmu či spôsobu spáchania trestného činu. V podstate tak môže ísť o naozaj rôznorodú zmes trestných činov, ktoré spája spoločná črta (napríklad počítač, program, počítačové údaje a podobne). V prípade kybernetickej kriminality potom pôjde o trestnú činnosť spáchanú v kybernetickom priestore.[855] Pojem a filozofia kybernetickej kriminality vychádza z jednoduchej premisy, že čo je trestné v skutočnom svete, musí byť trestné i v digitálnom prostredí.

Vo všeobecnosti možno uviesť, že kybernetická kriminalita je akákoľvek protiprávna činnosť, v rámci ktorej je prostriedok IKT v postavení nástroja, cieľa alebo prostriedku.[856]

[853] IOCTA 2011, s. 8, dostupné dňa 20.11.2025 na: LINK
[854] Rada Európy, Dohovor o počítačovej kriminalite, 23. november 2001, ETS 185. Dostupné na: LINK
[855] SMEJKAL, V.: Kybernetická kriminalita. 2. vyd. Plzeň : Aleš Čeněk, 2018. s. 23.
[856] POLČÁK, R. a kol.: Právo informačných technológií. Praha : Wolters Kluwer ČR, 2018, s. 541.

Polčák sa prikláňa k názoru, že kybernetická kriminalita by mohla zahŕňať nasledujúce kategórie, a to *cyber-dependent* a *cyber-enabled*, poťažmo *computer supported* kriminalitu.[857]

Za *cyber-dependent* kriminalitu možno považovať trestnú činnosť, ktorá môže byť spáchaná iba prostredníctvom počítačov, počítačových sietí alebo iných druhov informačných a komunikačných technológií. Ide teda predovšetkým o kybernetickú kriminalitu v užšom zmysle, v rámci ktorej sú technológie cieľom trestnej činnosti, ako je tomu napríklad v prípade hackingu, šírenia malvéru či útokov odmietnutia služby.[858]

Za *cyber-enabled* kriminalitu možno považovať tradičné trestné činy, ktoré majú väčší dosah alebo rozsah práve vďaka využitiu počítačov, počítačových sietí alebo iných prostriedkov IKT. Ide teda napríklad o trestné činy detskej pornografie či porušovanie autorských práv. Hoci sú spravidla tieto trestné činy páchané pomocou technológií, môžu byť spáchané aj bez nej.[859]

Možno tiež hovoriť o tretej kategórii, tzv. *computer-supported* kriminalite, kde je počítač či iná súvisiaca technológia využitá v priebehu jeho páchania iba príležitostne. Zahŕňa teda tie trestné činy, ktoré môžu byť spáchané aj iným spôsobom, avšak informačno-komunikačné technológie jeho spáchanie uľahčujú, napríklad stalking, rôzne druhy podvodov, legalizácia výnosov z trestnej činnosti či obchodovanie s drogami. Tu v zásade nejde o kybernetickú kriminalitu *per se*, avšak o spáchanom trestnom čine možno obstarať elektronické dôkazy pochádzajúce napríklad z e-mailov v počítači, lokalizačné údaje o hovoroch realizovaných v blízkosti miesta činu a podobne.[860]

12.3 Kybernetická kriminalita v medzinárodnoprávnych dokumentoch a právnych aktoch Európskej únie

12.3.1 Akty medzinárodného práva

Budapeštiansky dohovor

Zvýšenú snahu o reguláciu problematiky kybernetickej kriminality možno badať už dlhšie obdobie aj v medzinárodnom spoločenstve na pôde medzinárodných organizácií.

[857] Ibid, s. 542. K tomu pozri aj MCGUIRE, M., DOWLING, S.: Cyber crime: A review of the evidence. UK Home Office, 2013. Dostupné dňa 06.02.2026 na: LINK

[858] K tomu pozri podkapitolu 12.4 Hmotnoprávne aspekty počítačovej kriminality podľa právnej úpravy Slovenskej republiky.

[859] POLČÁK, R. a kol.: Právo informačných technológií. Praha : Wolters Kluwer ČR, 2018, s. 542.

[860] Ibid, s. 542.

Pracovná skupina Rady Európy pre počítačovú kriminalitu otvorila v roku 2001 v Budapešti na podpis Dohovor o počítačovej kriminalite (ang. *Convention on Cybercrime*), pre ktorý sa v odborných kruhoch zaužíval výraz Budapeštiansky dohovor.[861] Stal sa tak prvým komplexným medzinárodnoprávnym dokumentom, ktorý priniesol solídny základ pre kvalifikovanie a stíhanie trestnej činnosti páchanej v kybernetickom priestore, nakoľko sa okrem definícií skutkových podstát počítačových trestných činov zaoberá aj otázkou dokazovania elektronickými dôkaznými prostriedkami a problematikou jurisdikcie či medzinárodnej spolupráce v trestných veciach v boji proti tomuto druhu trestnej činnosti. K Budapeštianskemu dohovoru bol v roku 2003 prijatý Dodatkový protokol týkajúci sa kriminalizácie činov rasistickej a xenofóbnej povahy spáchaných prostredníctvom počítačových systémov a v roku 2021 aj Druhý dodatkový protokol týkajúci sa posilnenej spolupráce a sprístupňovania elektronických dôkazov.

Dohovor o počítačovej kriminalite nadobudol v zmysle čl. 36 ods. 3 platnosť dňa 1. júla 2004, pre Slovenskú republiku nadobudol v zmysle čl. 36 ods. 4 platnosť dňa 1. mája 2008. Z hľadiska systematiky je rozdelený do štyroch kapitol. Hoci ani tento dokument nepriniesol definíciu pojmu kybernetická kriminalita či počítačová kriminalita, nastavil pre zmluvné strany spoločný minimálny štandard trestných činov, ktoré je potrebné inkorporovať do vnútroštátnych právnych poriadkov zmluvných strán.

Prvá kapitola Budapeštianskeho dohovoru je venovaná vymedzeniu ústredných pojmov, ktoré sa k problematike viažu. V čl. 1 sú na účely Budapeštianskeho dohovoru ustanovené definície pojmov počítačový systém, počítačové údaje, poskytovateľ služieb či prevádzkové údaje.

Budapeštiansky dohovor v druhej kapitole, okrem rýdzo počítačových trestných činov (*core of computer-related offences*) porušujúcich alebo ohrozujúcich dôvernosť, dostupnosť a integritu[862] počítačových údajov a počítačových systémov, medzi ktoré zaraďuje trestné činy nezákonného prístupu (*illegal access*), nezákonného zachytenia údajov (*illegal interception*), zasahovania do údajov (*data interference*), zasahovania do systému (*system interference*) a zneužitie zariadení (*misuse of devices*), prišiel aj s výpočtom ďalších protiprávnych činov, ktoré majú byť zmluvnými stranami postihované (*computer-related*

[861] Oznámenie Ministerstva zahraničných vecí Slovenskej republiky č. 137/2008 Z. z. o podpísaní Dohovoru o počítačovej kriminalite.
[862] K tomu pozri kapitolu 1. Teoretické základy kybernetickej bezpečnosti.

offences), a to trestné činy falšovania počítačových údajov (*computer-related forgery*) a počítačového podvodu (*computer-related fraud*). Dohovor o počítačovej kriminalite vymedzuje aj tretiu skupinu trestných činov súvisiacich s protiprávnym obsahom (*content-related offences*), a to trestné činy týkajúce sa detskej pornografie (*offences related to child pornography*) a trestné činy týkajúce sa porušenia autorských práv a príbuzných práv (*offences related to infringements of copyright and related rights*).

PRÍKLAD

Uvedená kategorizácia nám môže slúžiť ako pomôcka, z ktorej možno vychádzať pri definovaní, aké druhy trestných činov zahŕňa pojem kybernetická kriminalita. V zásade teda pôjde o štyri kategórie trestných činov:

- rýdzo počítačové trestné činy, ktoré sú v tejto učebnici nazývané aj ako „počítačové trestné činy" alebo „počítačová kriminalita" (odkazuje na skupinu tých trestných činov, ktoré ohrozujú alebo poškodzujú dôvernosť, dostupnosť a integritu počítačových údajov a počítačových systémov),
- trestné činy súvisiace s počítačom,
- trestné činy súvisiace s obsahom,
- trestné činy súvisiace s porušovaním autorských alebo príbuzných práv.

Okrem hmotnoprávnej úpravy obsahuje druhá kapitola Dohovoru v čl. 16 až 21 aj procesnoprávne ustanovenia zamerané na zhromažďovanie dôkazov o trestnom čine v elektronickej forme, ako aj na otázku právomoci. Ukladá zmluvným stranám povinnosť prijať legislatívne opatrenia, ktoré umožňujú vnútroštátnym orgánom nariadiť urýchlené uchovanie počítačových údajov, vrátane prevádzkových údajov, ktoré boli uložené prostredníctvom počítačového systému, predloženie počítačových údajov uložených v počítačovom systéme, informácií o predplatiteľovi služby, prehliadku, v rámci ktorej je možné zaistiť počítačový systém alebo jeho časť, vyhotovenie kópie počítačových údajov, zachovanie celistvosti uložených počítačových údajov, znemožnenie prístupu k počítačovým údajom, odstránenie počítačových údajov z počítačového systému či zhromažďovanie prevádzkových údajov a zachytávanie obsahových údajov v reálnom čase. Procesné ustanovenia Budapeštianskeho dohovoru budú rozobraté v časti venovanej cezhraničnému zaisťovaniu počítačových údajov. Je potrebné zdôrazniť, že Budapeštiansky dohovor sa

použije aj vo vzťahu k štátom EU Írsko a Dánsko, ktoré neuplatňujú režim EVP na základe výhrady.[863] Rovnako sa je potrebné spomenúť, že Budapeštiansky dohovor je možné aplikovať i na zaistenie virtuálnych mien, hoci má povahu hospodárskej hodnoty a nie je určené primárne na dokazovanie trestnej činnosti.

Tretia kapitola Budapeštianskeho dohovoru sa koncentruje na otázky medzinárodnej spolupráce, poukazuje najmä na zásady uplatňované vo vzťahu k extradícii, právnej pomoci, a to aj pre prípad neexistencie medzinárodnej dohody. Rovnako u každej zo zmluvných strán predpokladá určenie kontaktného miesta dostupného 24 hodín denne 7 dní v týždni, a to najmä za účelom zhromažďovania dôkazov v elektronickej podobe.

Posledná kapitola obsahuje záverečné ustanovenia vzťahujúce sa k otázkam nadobudnutia platnosti a podmienkam pristúpenia k Dohovoru, ako aj k možnosti uplatnenia výhrad zmluvných strán k Dohovoru.[864]

Hanojský dohovor

Dohovor OSN proti počítačovej kriminalite (*United Nations Convention against Cybercrime*)[865] prijalo Valné zhromaždenie dňa 24. decembra 2024 v New Yorku uznesením č. 79/243. Tento dohovor je prvou komplexnou globálnou zmluvou v tejto oblasti, ktorá štátom poskytuje celý rad opatrení, ktoré majú prijať ako prevenciu a boj proti počítačovej kriminalite. Jeho cieľom je tiež posilniť medzinárodnú spoluprácu pri výmene elektronických dôkazov v prípadoch závažných trestných činov. Pre tento dohovor sa zaužíval výraz Hanojský dohovor, nakoľko bol štátom otvorený na podpis dňa 25. októbra 2025 na slávnostnom ceremoniáli v Hanoji, Vietnam, kde bol podpísaný štátmi v celkovom počte 72, pričom zostal otvorený na podpis v sídle OSN v New Yorku do 31. decembra 2026. Po podpise Hanojského dohovoru štáty dokončia svoje vnútroštátne procesy na jeho implementáciu a následne uložia u Generálneho tajomníka OSN listinu o ratifikácii, prijatí alebo schválení, čím sa formálne stanú zmluvnými stranami Hanojského dohovoru. V súlade s článkom 65

[863] Recitál 44 a 45 Smernice Európskeho parlamentu a Rady 2014/41/EÚ z 3. apríla 2014 o európskom vyšetrovacom príkaze v trestných veciach (Ú. v. EÚ L 130/1, 1.5.2014).

[864] V zmysle písm. e) a f) oznámenia č. 137/2008 Z. z. Ministerstva zahraničných vecí Slovenskej republiky o podpísaní Dohovoru o počítačovej kriminalite si Slovenská republika vyhradila právo odmietnuť vykonanie žiadosti o uchovanie údajov v prípadoch, v ktorých má dôvody domnievať sa, že v čase sprístupnenia nemožno splniť podmienku obojstrannej trestnosti, ako aj právo vyžadovať pre trestnosť konania uvedeného v čl. 4 ods. 1 – „Zasahovanie do údajov" Budapeštianskeho dohovoru, aby jeho následkom bola značná škoda.

[865] Uznesenie Valného zhromaždenia OSN č. 79/243 zo dňa 24. decembra 2024 o prijatí Dohovoru Organizácie spojených národov proti počítačovej kriminalite. Dostupné dňa 30.03.2026 na: LINK

Hanojského dohovoru, platnosť nadobudne deväťdesiatym dňom po dni uloženia štyridsiatej listiny o ratifikácií, prijatí, schválení alebo pristúpení.

Z pohľadu systematiky pozostáva Hanojský dohovor z preambuly a deviatich kapitol. Jednotlivé kapitoly sú organizované počnúc všeobecnými ustanoveniami, ktoré uvádzajú okrem definícií vybraných pojmov aj záväzok, aby zmluvné štáty zabezpečili, že všetky protiprávne skutky páchané *offline*, boli považované za trestný čin aj v prípadoch, keď sú spáchané *online*. Kapitola týkajúca sa podmienok trestnej zodpovednosti sa zaoberá vymedzením jednotlivých skutkových podstát skutkov kvalifikovaných ako trestné činy podľa Hanojského dohovoru, vrátane otázky trestnej zodpovednosti fyzických osôb, ako aj právnických osôb, podmienok spolupáchateľstva či účasti na týchto trestných činoch. Kapitola týkajúca sa jurisdikcie stanovuje pravidlá, ktoré vymedzujú, akým spôsobom možno trestne stíhať protiprávne skutky, ak sú tieto spáchané na území zmluvného štátu, resp. poškodzujú záujmy zmluvného štátu, resp. ak boli spáchané ich štátnymi príslušníkmi alebo cudzími štátnymi príslušníkmi na ich území. Ďalšia kapitola Hanojského dohovoru sa venuje procesným opatreniam zameraných pre orgány presadzovania práva, nasleduje kapitola týkajúca sa medzinárodnej spolupráci, kapitola o preventívnych opatreniach, technickej pomoci a výmene informácií, kapitola o mechanizme implementácie Hanojského dohovoru a záverečné ustanovenia určujúce, akým spôsobom sa štáty môžu stať zmluvnými stranami a akým spôsobom môžu od neho odstúpiť.

12.3.2 Akty práva Európskej únie

Akty primárneho práva Európskej únie

Kybernetická kriminalita je svetovým problémom, proti ktorému možno len zriedka účinne bojovať v bežnom vnútroštátnom kontexte. Vnútroštátny prístup k počítačovej kriminalite v sebe skrýva riziko vzniku roztrieštenosti a neefektívnosti, pretože rozdiely vo vnútroštátnych prístupoch a chýbajúca systematická cezhraničná spolupráca podstatne znižujú účinnosť národných protiopatrení. To je čiastočne zapríčinené technickou prepojenosťou informačných systémov nezávislou od hraníc, keďže nízka úroveň bezpečnosti v jednej krajine v sebe skrýva možnosť zvýšenia zraniteľnosti v iných krajinách. Z toho dôvodu existuje všeobecne uznávaná potreba konať zo strany Európskej únie a na medzinárodnej úrovni s cieľom zabrániť tomuto problému a vyriešiť ho, vzhľadom na to, že

viaceré útoky presahujú hranice Európskej únie. Počítačová kriminalita a posilňovanie kapacít na boj s ňou je preto aj jednou z dlhodobých priorít Európskej únie.[866]

Spomedzi aktov primárneho práva Európskej únie je na tomto mieste nevyhnutné spomenúť základný právny rámec pre ustanovovanie minimálnych harmonizačných pravidiel týkajúcich sa vymedzenia trestných činov a sankcií v oblastiach obzvlášť závažnej trestnej činnosti s cezhraničným rozmerom prostredníctvom smerníc, ktorý vyplýva z článku 83 Zmluvy o fungovaní Európskej únie (ZFEÚ).[867] Predmetný článok ZFEÚ sa týka justičnej spolupráce členských štátov Európskej únie v trestných veciach a v odseku 1 vypočítava okruhy trestných činov, na ktorých odhaľovaní a stíhaní má Európska únia záujem. Zaraďuje medzi ne okrem terorizmu, obchodovania s ľuďmi a sexuálneho zneužívania žien a detí, obchodovania s drogami, obchodovania so zbraňami, legalizácie výnosov z trestnej činnosti, korupcie, falšovania platobných prostriedkov či organizovanej trestnej činnosti aj počítačovú kriminalitu.

Akty sekundárneho práva Európskej únie

Obsah článku 83 ZFEÚ je realizovaný výlučne prostredníctvom smerníc ako nástrojom sekundárneho práva Európskej únie. Pre oblasť kybernetickej kriminality je relevantnou najmä smernica 2013/40/EÚ.[868] Táto smernica v podstate vychádza a zohľadňuje obsah Budapeštianskeho dohovoru, ktorý slúži ako vzorový dokument pre vnútroštátne právne predpisy a vytvára spoločný základ spolupráce v oblasti počítačovej kriminality v rámci Európskej únie a mimo nej. Ako to už vyplýva zo samotného názvu smernice 2013/40/EÚ, táto stanovila pravidlá harmonizácie a sankcií za protiprávne činy namierené proti informačným systémom, a to od útokov spôsobujúcich následok v podobe odmietnutia služby až po neoprávnené zachytávanie údajov. V porovnaní s Budapeštianskym dohovorom sa smernica 2013/40/EÚ odklonila od používania pojmu počítačový systém,[869] ktorý nahradila širším pojmom informačný systém.

[866] Priority nového EMPACT cyklu pre 2026-2029, s. 11. Dostupné dňa 06.02.2025 na: LINK
[867] Konsolidované znenie Zmluvy o fungovaní Európskej únie (Ú. v. EÚ C 326, 26. október 2012, s. 47).
[868] 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 (Ú. v. EÚ L 218, 14. august 2013, s. 8).
[869] K tomu pozri podkapitolu 12.4 Hmotnoprávne aspekty počítačovej kriminality podľa právnej úpravy Slovenskej republiky – výklad k ustanoveniu § 247 TZ.

Hlavnou ideou tejto smernice je efektívnejšie vyvodzovanie trestnoprávneho postihu páchateľov zodpovedných za protiprávne počítačové útoky, ktoré sa nepovažujú za menej závažné, a to aproximáciou hmotnoprávnych, ako aj procesnoprávnych noriem trestného práva v oblasti útokov na informačné systémy. Z toho dôvodu si stanovila tri okruhy právnej úpravy. Prvým je dosiahnuť spoločný prístup členských štátov k prijatiu právnej úpravy, podľa ktorej budú trestnoprávne postihované tie skutky, ktoré budú napĺňať znaky skutkových podstát nasledovných trestných činov: protiprávny prístup do informačných systémov, protiprávny zásah do systému, protiprávny zásah do údajov, protiprávne zachytávanie údajov či držby nástrojov na spáchanie uvedených trestných činov. Smernica 2013/40/EÚ pre tieto trestné činy vymedzila aj minimálnu hornú hranicu trestnej sadzby trestu odňatia slobody. V tejto súvislosti je nevyhnutné podotknúť, že smernica ponechala na úvahe členských štátov možnosť stanoviť si, čo sa rozumie pod pojmom menej závažný protiprávny čin, a to s ohľadom na ich právnu úpravu. Za menej závažný prípad možno považovať najmä tie situácie, kedy v dôsledku spáchania niektorého z počítačových trestných činov nastala škoda alebo ohrozenie verejného či súkromného záujmu, ktorý je zanedbateľný alebo takej povahy, pri ktorej by bolo uloženie trestnej sankcie zrejme neprimerané s ohľadom na princíp *ultima ratio*. Rovnako, táto smernica nemá za cieľ postihovať skutky *en bloc*, pri ktorých dôjde k formálnemu naplneniu znakov niektorej zo skutkových podstát, ak sú spáchané bez protiprávneho úmyslu, napríklad v dôsledku nevedomosti určitej osoby o tom, že ide o neoprávnený prístup a podobne. Druhým cieľom, ktorý smernica 2013/40/EÚ sleduje je, aby každý členský štát zabezpečil kontaktné miesto, ktoré bude k dispozícii 24 hodín denne 7 dní v týždni za účelom výmeny informácií týkajúcich sa počítačových trestných činov, pričom v prípade naliehavých žiadostí o pomoc je uložená povinnosť podať do 8 hodín od prijatia žiadosti (najmä z dôvodu nestabilnej povahy digitálnych stôp ako potenciálnych dôkazov) správu o tom, či žiadosť bude zodpovedaná a v akej lehote. Tretím sledovaným cieľom bolo uloženie povinnosti členským štátom zbierať štatistické údaje o počítačovej kriminalite. Aj s odstupom času však možno v podmienkach Slovenskej republiky konštatovať neuspokojivý monitoring tohto druhu trestnej činnosti. Z ukazovateľov týkajúcich sa štatistiky kriminality za príslušné časové obdobie vedených Generálnou prokuratúrou Slovenskej republiky

a Ministerstvom vnútra Slovenskej republiky je zrejmé, že doposiaľ nebola zavedená samostatná evidencia pre oblasť kybernetickej kriminality.[870]

Vzhľadom na to, že kybernetická kriminalita sa vzťahuje na široký rozsah trestnej činnosti, ktoré sa týkajú počítačov a informačných systémov v podobe nástroja alebo cieľa, nepochybne sa dotýka aj oblasti boja proti podvodom v súvislosti s ich páchaním pri bezhotovostných platbách. Navyše, podvody pri bezhotovostných platbách[871] sú častokrát zdrojom príjmov pre organizovanú trestnú činnosť a pomyselnou vstupnou bránou k páchaniu ďalšej trestnej činnosti. Hoci sú transakcie vykonávané platobnými kartami najrozšírenejšou formou bezhotovostných platieb, vyvinuli sa nové formy transakcií, medzi ktoré patria napríklad mobilné platby či virtuálne meny. Smernicu 2013/40/EÚ preto doplnila smernica Európskeho parlamentu a Rady (EÚ) 2019/713 zo 17. apríla 2019 o boji proti podvodom s bezhotovostnými platobnými prostriedkami a proti ich falšovaniu a pozmeňovaniu, ktorou sa nahrádza rámcové rozhodnutie Rady 2001/413/SVV,[872] na ktorú odkazuje hneď v niekoľkých ustanoveniach. V dôsledku transpozície smernice (EÚ) 2019/713 do Trestného zákona[873] došlo napríklad k prijatiu legálnej definície pojmu platobný prostriedok či virtuálna mena podľa ustanovení § 131 ods. 6 a 7 TZ, ako aj k podstatnej úprave znenia skutkovej podstaty trestného činu neoprávnené vyrobenie a používanie platobného prostriedku podľa ustanovenia § 219 TZ. Zároveň táto smernica nadviazala aj na smernicu (EÚ) 2016/1148,[874] konkrétne v tom, že podnecuje prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb robiť oznámenia o bezpečnostných incidentoch, pri ktorých existuje podozrenie o ich súvise so závažnou trestnou činnosťou orgánom činným v trestnom konaní. Rovnako sa tiež predpokladá aj vyššia miera zapojenia jednotiek CSIRT

[870] K tomu pozri napr. DRAŽOVÁ, P., KORDÍK, M.: Efektivita postihu počítačovej kriminality. In Efektívnosť prípravného konania – jej skúmanie, výzvy a perspektívy. Bratislava : Univerzita Komenského v Bratislave, Právnická fakulta, 2020, s. 48 – 62. Dostupné dňa 06.02.2026 na: LINK

[871] Typický prípad podvodu pri bezhotovostnej platbe je napríklad tzv. *skimming*. Páchateľ skopíruje údaje platobnej karty v krajine EÚ, vytvorí falošnú kartu s použitím týchto údajov a následne vykoná výber hotovosti touto falošnou kartou mimo EÚ s cieľom obísť bezpečnostné normy. Iným spôsobom podvodu je tzv. phishing, pri ktorom sa páchateľ snaží prostredníctvom e-mailu s odkazom, ktorý umožní presmerovanie na podvodnú stránku, vylákať a neoprávnene získať údaje adresáta e-mailu (napríklad meno majiteľa karty, číslo karty, dátum exspirácie karty, overovací kód), ktoré následne zneužije.

[872] Smernica Európskeho parlamentu a Rady (EÚ) 2019/713 zo 17. apríla 2019 o boji proti podvodom s bezhotovostnými platobnými prostriedkami a proti ich falšovaniu a pozmeňovaniu, ktorou sa nahrádza rámcové rozhodnutie Rady 2001/413/SVV (Ú. v. EÚ L 123, 10. máj 2019, s. 18).

[873] Do Trestného zákona bola transponovaná zákonom č. 312/2020 Z. z. o výkone rozhodnutia o zaistení majetku a správe zaisteného majetku a o zmene a doplnení niektorých zákonov.

[874] 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 (Ú. v. EÚ L 194, 19. júl 2016, s. 1).

do vyšetrovania s cieľom poskytovať informácie, a to najmä s ohľadom na ich odborné znalosti v oblasti informačných systémov. Vo vzťahu k virtuálnym menám a najmä ich zaisťovaniu sa aplikuje nariadenie (EÚ) 2018/1805[875] zo 14. novembra 2018 o vzájomnom uznávaní príkazov na zaistenie a príkazov na konfiškáciu, v zmysle ktorého článok 1 stanovuje pravidlá, podľa ktorých členský štát uzná a vykoná na svojom území príkazy na zaistenie a príkazy na konfiškáciu vydané iným členským štátom v rámci konania v trestných veciach.

Ďalší právny akt sekundárneho práva Európskej únie staršieho dáta, ktorý sa dotýka oblasti kybernetickej kriminality je smernica Európskeho parlamentu a Rady 2011/92/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorou sa nahrádza rámcové rozhodnutie Rady 2004/68/SVV.[876] Vzhľadom na to, že využívanie informačných a komunikačných technológií uľahčuje rôzne formy sexuálneho zneužívania a vykorisťovania detí online formou (kontaktovanie detí za účelom ich zneužitia prostredníctvom webových stránok sociálnych sietí, diskusných skupín a pod.), táto smernica uložila členským štátom hneď niekoľko povinností. Medzi najvýznamnejšie možno zaradiť jednak povinnosť stíhať širokú škálu „nových" foriem páchania tejto trestnej činnosti (sexuálne zneužívanie detí prostredníctvom webovej kamery či prezeranie obrázkov detskej pornografie online aj bez ich sťahovania) či povinnosť odstrániť obsah webovej stránky, ktorá obsahuje alebo šíri detskú pornografiu na území členského štátu, ako aj možnosť blokovať na svojom území prístup používateľov k takýmto webovým stránkam.

V rámci spoločnej zahraničnej a bezpečnostnej politiky Európska únia uplatňuje sankcie vo forme obmedzení, príkazov či zákazov, ktoré môžu byť prijaté voči tretím štátom, neštátnym subjektom, ale i jednotlivcom. O prijatí sankcií rozhoduje Rada, ktorá jednohlasne prijíma príslušné rozhodnutie na základe článku 29 Zmluvy o Európskej únii.[877] Na podklade predmetného článku došlo k vytvoreniu rámca, ktorý Európskej únii umožňuje ukladať cielené reštriktívne opatrenia na odrádzanie od kybernetických útokov, ktoré predstavujú vonkajšiu hrozbu pre Európsku úniu alebo jej členské štáty, a to vrátane kybernetických

[875] Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1805 zo 14. novembra 2018 o vzájomnom uznávaní príkazov na zaistenie a príkazov na konfiškáciu (Ú.v. EÚ L303/1)

[876] Smernica Európskeho parlamentu a Rady 2011/92/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorou sa nahrádza rámcové rozhodnutie Rady 2004/68/SVV (Ú. v. EÚ L 335, 17. december 2011, s. 1).

[877] Konsolidované znenie Zmluvy o Európskej únii (Ú. v. EÚ C 326, 26. október 2012, s. 33).

útokov voči tretím štátom alebo medzinárodným organizáciám. Jedným z týchto opatrení, ktoré boli prijaté je nariadenie Rady (EÚ) 2019/796 zo 17. mája 2019 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty,[878] ktoré stanovuje podmienky, podľa ktorých sa určuje či kybernetický útok predstavuje vonkajšiu hrozbu pre Úniu alebo jej členské štáty, aké prvky musia útoky zahŕňať, aby ich bolo možné subsumovať pod pojem kybernetický útok či okruh sankcií, ktoré môžu byť prijaté.[879]

Z procesnoprávneho pohľadu zabezpečovania dôkazov je potrebné zmieniť Európsky vyšetrovací príkaz (EVP) podľa Smernice (EÚ) 2014/41[880] ktorým sa rozumie rozhodnutie formulárového charakteru, ktoré vydal alebo overil justičný orgán členského štátu za účelom vykonania jedného alebo viacerých konkrétnych vyšetrovacích opatrení v inom členskom štáte s cieľom získať dôkazy, resp. dôkazy, ktoré sa už nachádzajú v držbe príslušných orgánov vykonávajúceho štátu.[881] Keďže čoraz viac páchateľov trestnej činnosti využíva na plánovanie a páchanie trestných činov technológie, orgány činné v trestnom konaní v dôsledku toho využívajú častejšie elektronické dôkazy. Bez povšimnutia preto nemôže zostať tzv. e-Evidence balíček pozostávajúci z e-Evidence nariadenia[882] a e-Evidence smernice.[883] Cieľom e-Evidence nariadenia je zaviesť alternatívny mechanizmus k existujúcim nástrojom medzinárodnej spolupráce a vzájomnej právnej pomoci. Účelom v zmysle jeho článku 1 je stanoviť pravidlá, na základe ktorých môže orgán členského štátu v trestnom konaní vydať európsky príkaz na predloženie dôkazov alebo európsky príkaz na uchovanie

[878] Nariadenie Rady (EÚ) 2019/796 zo 17. mája 2019 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty (Ú. v. EÚ L 129, 17. máj 2019, s. 1).

[879] V tejto súvislosti je potrebné dodať, že Európska únia dňa 30. júla 2020 vôbec po prvýkrát prijala rozhodnutím Rady (SZBP) 2020/1127 z 30. júla 2020, ktorým sa mení rozhodnutie (SZBP) 2019/797 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty (Ú. v. EÚ L 393, 23. november 2020, s. 12) sankcie zamerané proti kybernetickým útokom, konkrétne voči šiestim osobám a trom subjektom, ktoré sú zodpovedné za útoky vedené proti Organizácii pre zákaz chemických zbraní v Holandsku a útoky verejnosti známe pod názvami „*WannaCry*", „*NotPetya*" a „*Operation Cloud Hopper*". Týmto útočníkom boli uložené sankcie vo forme zákazu cestovania a zmrazenia aktív. Zároveň boli doplnené do zoznamu fyzických a právnických osôb, subjektov a orgánov uvedených v prílohe k predmetnému rozhodnutiu. K tomu pozri napr.: LINK

[880] Smernica Európskeho parlamentu a Rady 2014/41/EÚ z 3. apríla 2014 o európskom vyšetrovacom príkaze v trestných veciach (Ú. v. EÚ L 130/1, 1.5.2014).

[881] Čl. 1 Smernice (EÚ) 2014/41. Úradný vestník Európskej únie L 130/1 Smernica Európskeho parlamentu a Rady 2014/41/EÚ z 3. apríla 2014 o európskom vyšetrovacom príkaze v trestných veciach (Ú. v. EÚ L 130/1, 1.5.2014).

[882] Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1543 z 12. júla 2023 o európskych príkazoch na predloženie elektronických dôkazov a európskych príkazoch na uchovanie elektronických dôkazov v trestnom konaní a na výkon trestu odňatia slobody v nadväznosti na trestné konanie (Ú. v. EÚ L 191, 28.7.2023).

[883] Smernica Európskeho parlamentu a Rady (EÚ) 2023/1544 z 12. júla 2023, ktorou sa stanovujú harmonizované pravidlá určovania určených prevádzkarní a vymenúvania právnych zástupcov na účely zhromažďovania dôkazov v trestnom konaní (Ú. v. EÚ L 191, 28.7.2023).

dôkazov, a tým priamo nariadiť poskytovateľovi služieb, ktorý ponúka služby v Únii a je usadený v inom členskom štáte, alebo ak nie je usadený, je zastúpený právnym zástupcom v inom členskom štáte, aby predložil alebo uchoval elektronické dôkazy bez ohľadu na fyzické umiestnenie údajov. Tieto príkazy sa môžu vzťahovať na akúkoľvek kategóriu údajov vrátane údajov o predplatiteľovi a prevádzkových a obsahových údajov. Pre prevádzkové údaje (okrem údajov požadovaných výlučne na účely identifikácie užívateľa) a pre obsahové údaje bola stanovená prahová hodnota. O tieto údaje možno požiadať len v prípade trestných činov, za ktoré možno vo vydávajúcej krajine uložiť trest odňatia slobody s hornou hranicou trestnej sadzby najmenej tri roky, alebo v prípade špecifických trestných činov súvisiacich s počítačovou kriminalitou, detskou pornografiou, falšovaním bezhotovostných platobných prostriedkov alebo terorizmom. Na odpoveď na príkaz na predloženie dôkazov je stanovená lehota 10 dní. V núdzových prípadoch sa táto lehota môže skrátiť na osem hodín. Poskytovateľom služieb možno uložiť sankcie, ak príkaz nevykonajú, a to až do výšky 2 % ich celkového celosvetového ročného obratu za predchádzajúci účtovný rok. O vydanie európskeho príkazu na predloženie dôkazov alebo európskeho príkazu na uchovanie dôkazov môže požiadať aj podozrivá alebo obvinená osoba alebo advokát v jej mene v rámci uplatniteľných práv na obhajobu v súlade s vnútroštátnym trestným právom procesným. e-Evidence smernica je základným nástrojom pri uplatňovaní e-Evidence nariadenia. Stanovujú sa v nej pravidlá vymenúvania právnych zástupcov poskytovateľov služieb alebo určovania ich určených prevádzkarní, ktoré sú zodpovedné za prijímanie takýchto príkazov a za reagovanie na ne. Je to potrebné z dôvodu chýbajúcej všeobecnej právnej požiadavky, aby poskytovatelia služieb z krajín mimo Európskej únie boli v EÚ fyzicky prítomní.

Z procesnoprávneho hľadiska má taktiež význam Akt o umelej inteligencii,[884] ktorý upravuje využitie umelej inteligencie samotnými orgánmi činnými v trestnom konaní ako novej formy informačno-technického prostriedku[885] pre účely profilovania osoby[886], biometrickej kategorizácie osôb,[887] alebo biometrickej identifikácie osôb v reálnom čase.[888]

[884]Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii) (Ú. v. EÚ L 2024/1689, 12.7.2024).

[885] Porovnaj § 10 ods. 20 TP.

[886] Čl. 5 ods. 1, písm. d) Aktu o umelej inteligencii.

[887] Čl. 5 ods. 1, písm. g) Aktu o umelej inteligencii.

[888] Čl. 5 ods. 1, písm. h) Aktu o umelej inteligencii upravuje iba tzv. *live facial recognition* (LFR), identifikáciu v reálnom čase a nie identifikáciu osôb po spáchaní skutku tzv. *post event / after facial recognition* (AFR), čo

12.4 Hmotnoprávne aspekty počítačovej kriminality podľa právnej úpravy Slovenskej republiky

Kybernetická kriminalita vo vnútroštátnom kontexte predstavuje súbor trestných činov, pri ktorých je počítačový, resp. informačný systém buď predmetom útoku (*cyber-dependent crimes*), alebo prostriedkom / nástrojom spáchania trestného činu (*cyber-enabled crimes*). Legislatívna úprava prešla v roku 2016 rozsiahlou reformou, ktorá precizovala najmä skutkové podstaty tzv. rýdzo počítačových trestných činov podľa § 247 – 247d Trestného zákona.

12.4.1 K niektorým špecifikám obligatórnych a fakultatívnych znakom skutkových podstát počítačových trestných činov

V prípadoch skutkov kybernetickej kriminality je *subjekt všeobecný*, teda každá trestne zodpovedná fyzická alebo právnická osoba. Z pohľadu profilovania a vzhľadom na charakter počítačovej kriminality bude páchateľom osoba inteligentná, uvedomujúca si nebezpečnosť svojho konania, schopná využívať rôzne anonymizačné techniky s prvkami analytického myslenia v oblasti rizík, spojených najmä s oblasťou kybernetickej bezpečnosti.

PRÍKLAD

Počítačová kriminalita ako i jej páchatelia sa vyznačujú vysokou mierou latencie a anonymity, spravidla sa táto činnosť vykonáva za peniaze a trend posledných rokov je páchanie počítačovej kriminality ako *„Crime as a Service"* - profesionálnej služby za odplatu dodávanej klientele, ktorou môžu byť všetky formy organizovaných, zločineckých, teroristických skupín, alebo individuálnych entít, vrátane štátov alebo ich predstaviteľov.

Druhá skupina páchateľov počítačovej kriminality sú osoby, ktoré využívajú anonymitu sociálnych sietí pre účely nebezpečného vyhrážania, vydierania, šírenia nenávisti a extrémistických postojov, považujúc toto konanie za dovolené, resp. málo nebezpečne práve v súvislosti s anonymitou prostredia internetu a sociálnych sietí. Samostatnou skupinou sú páchatelia trestných činov detskej pornografie.

predstavuje bežný postup orgánov presadzovania práva porovnávania tvárí napr. z bezpečnostných kamier po spáchaní skutku počas pátrania po horúcej stope. Porovnaj AI and Policing, EUROPOL, s. 24, dostupné dňa 21.10.2025 na: LINK

Z teoreticko-právneho delenia sú subjekty počítačových trestných všeobecné, teda každá trestne zodpovedná fyzická osoba a pri počítačových trestných činov napĺňajúcich znaky trestných činov podvodu podľa § 221 TZ, kapitálového podvodu podľa § 224 TZ, subvenčného podvodu podľa § 225 TZ, neoprávneného prístupu do počítačového systému podľa § 247 TZ, neoprávneného zásahu do počítačového systému podľa § 247a TZ, neoprávneného zásahu do počítačového údaja podľa § 247b TZ, neoprávneného zachytávania počítačových údajov podľa § 247c TZ, výroba a držba prístupového zariadenia, hesla do počítačového systému alebo iných údajov podľa § 247d TZ, nebezpečného vyhrážania podľa § 360 TZ, výroby detskej pornografie podľa § 368 TZ, rozširovania detskej pornografie podľa § 369 TZ, prechovávania detskej pornografie, účasti na detskom pornografickom predstavení podľa § 370 TZ, teroristického útoku podľa § 419 TZ, založenia, podpory a propagácia hnutia smerujúceho k potlačeniu základných práv a slobôd podľa § 421 TZ, prejav sympatie k hnutiu smerujúcemu k potlačeniu základných práv a slobôd podľa § 422 TZ, výroby extrémistických materiálov podľa § 422a TZ, rozširovanie extrémistických materiálov podľa § 422b TZ, prechovávania extrémistických materiálov podľa § 422c TZ, popierania a schvaľovania holokaustu, zločinov politických režimov a zločinov proti ľudskosti podľa § 422d TZ, hanobenia národa, rasy a presvedčenia podľa § 423 TZ, podnecovania k národnostnej, rasovej a etnickej nenávisti podľa § 424 TZ, apartheid a diskriminácia skupiny osôb podľa § 424a TZ a neľudskosť podľa § 425 TZ aj právnická osoba.

Počítačové trestné činy podľa § 247 – 247d Trestného zákona sú *úmyselné trestné činy*, teda páchateľ chce porušiť alebo ohroziť záujem chránený Trestným zákonom alebo vedel, že svojím konaním môže také porušenie alebo ohrozenie spôsobiť a pre prípad, že ho spôsobí, bol s tým uzrozumený. Počítačové trestné činy sú taktiež typické pre určité skupiny *pohnútok* alebo *motívov*, ktoré sú prítomné buď v základnej skutkovej podstate alebo ako kvalifikačný znak, nasledovne:

- získanie majetkového prospechu,
- spôsobenie škody, poruchy alebo nefunkčnosti,
- získanie privilegovaných informácií alebo utajovaných skutočností,
- narúšanie súkromia a prístup k prejavom osobnej povahy,
- sexuálne uspokojenie,
- extrémizmus a šírenie nenávisti.

Obete počítačovej kriminality[889] v zmysle slovenskej právnej úpravy spĺňajú i definíciu obzvlášť zraniteľnej obete,[890] najmä v prípadoch trestných činov detskej pornografie, nebezpečného vyhrážania, či nebezpečného prenasledovania alebo nebezpečného elektronického obťažovania. Všetky procesné úkony s obzvlášť zraniteľnou obeťou by mali byť vykonávané ohľaduplne, citlivo a orgány činné v trestnom konaní by k nim mali pristupovať ako k neopakovateľným úkonom. Vo vzťahu k poškodeným trestného činu podvodu (v terminológií počítačovej kriminality tzv. *scam*) aplikačná prax rozvinula teóriu primeranej miery opatrnosti poškodeného, v rámci ktorej je potrebné skúmať, či vôbec konanie páchateľa je spôsobilé zapríčiniť následok predpokladaný Trestným zákonom, ak by poškodený sám vyvinul aspoň základnú opatrnosť a preveril si elementárne skutočnosti páchateľovho podvodného konania, z ktorého by mal získať podozrenie, že nejde o legitímny záujem osoby konať naznačeným spôsobom.[891]

Poškodení v trestnom konaní ako subjekty, resp. neskôr ako strany trestného konania vedeného pre počítačový trestný čin majú taktiež určité špecifické postavenie najmä v prípadoch podvodných kampaní, kedy je poškodených viac ako 100, čo má za následok procesný postup podľa § 47 ods. 3 TP, v zmysle ktorého, ak je v tej istej veci veľký počet poškodených, spravidla prevyšujúci sto, a jednotlivým výkonom ich práv by mohol byť závažným spôsobom ohrozený účel a rýchly priebeh trestného stíhania, rozhodne v prípravnom konaní na návrh generálneho prokurátora Slovenskej republiky o účasti poškodených v trestnom konaní najvyšší súd uznesením, ktoré sa doručí navrhovateľovi. Ak návrh nebol zamietnutý, generálny prokurátor zabezpečí, aby bolo uznesenie vhodným spôsobom zverejnené. Ďalej z povahy veci vyplýva, že v takýchto hromadných veciach sa má

[889] V zmysle § 2 ods. 1 písm. b) zákona č. 274/2017 Z. z. o obetiach trestných činov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov je obeťou *fyzická osoba, ktorej bolo alebo malo byť trestným činom ublížené na zdraví, spôsobená majetková škoda, nemajetková alebo iná škoda alebo boli porušené, či ohrozené jej zákonom chránené práva alebo slobody.*

[890] V zmysle § 2 ods. 1 písm. c) zákona o obetiach sa obzvlášť zraniteľnou obeťou rozumie *1. dieťa; dieťaťom sa rozumie osoba mladšia ako osemnásť rokov, a ak nie je vek osoby známy a existuje dôvod domnievať sa, že je dieťaťom, považuje sa za dieťa, až kým sa nepreukáže opak, 2. osoba staršia ako 75 rokov, 3. osoba so zdravotným postihnutím, 4. obeť trestného činu obchodovania s ľuďmi, trestného činu nedobrovoľného zmiznutia, trestného činu týrania blízkej osoby a zverenej osoby, trestného činu spáchaného organizovanou skupinou, niektorého z trestných činov proti ľudskej dôstojnosti, niektorého z trestných činov terorizmu alebo trestného činu domáceho násilia, 5. obeť trestného činu spáchaného násilím alebo hrozbou násilia z dôvodu jej pohlavia, sexuálnej orientácie, národnosti, rasovej alebo etnickej príslušnosti, náboženského vyznania alebo viery, 6. obeť iného trestného činu, ktorá je vystavená vyššiemu riziku opakovanej viktimizácie alebo druhotnej viktimizácie zistenému na základe individuálneho posúdenia obete a jej osobných vlastností, vzťahu k páchateľovi alebo závislosti od páchateľa, druhu alebo povahy a okolností spáchania trestného činu.*

[891] K tomu pozri rozhodnutie NS SR sp. zn. 2 Tdo V 21/2014.

viesť spoločné konanie, nakoľko sú splnené podmienky podľa § 18 ods. 1 TP, že spoločné konanie sa vedie proti všetkým obvineným, ktorých trestné činy spolu súvisia, sa môže vykonať spoločné konanie, ak to zrejme nebude brániť ukončeniu veci v primeranej lehote - čo predstavuje najčastejší dôvod, prečo sa jednotlivé skutky, najmä kampaňových počítačových trestných činov vedú oddelenie a čiastkovo pre skutok každého poškodeného samostatne. Ide však o prístup, ktorý nie je ani účelný a ani hospodárny.

Miesto spáchania počítačového trestného činu je determinované § 12 Trestného zákona. V zmysle tohto ustanovenia je miestom spáchania trestného činu každé miesto, na ktorom:

- páchateľ konal (subjektívna súvislosť),[892] alebo
- nastal alebo podľa predstavy páchateľa mal nastať následok predpokladaný týmto zákonom (objektívna súvislosť).[893]

Z uvedeného je zrejmé, že vzhľadom na dostupnosť spoľahlivých anonymizačných techník najmä lokalizačných údajov bude miesto, kde páchateľ konal známe, ak vôbec, v oveľa neskoršom štádiu trestného stíhania. Väčšina prípadov počítačových trestných činov sa posudzuje podľa miesta, kde nastal, alebo podľa predstavy páchateľa mal nastať škodlivý následok. Vzhľadom na skutočnosť, že počítačové trestné činy sú typickým príkladom tzv. dištančných deliktov, bude tento spôsob určenia miesta činu prevládať. Uvedené vyplýva i z toho, že interpretácia lokalizačných údajov, rozhodných pre určenie miesta činu počítačovej kriminality, je zdĺhavý, procesnými krokmi po začatí trestného stíhania, analytický proces, ktorý vykonáva vecne a miestne príslušný orgán činný v trestnom konaní na základe vybavených dožiadaní zo strany telekomunikačných operátorov[894] alebo informácií od znalca, ktorý skúma zaistené zariadenie.

12.4.2 Okolnosti vylučujúce protiprávnosť

PRÍKLAD
Okolnosti vylučujúce protiprávnosť vo vzťahu k počítačovej kriminalite zohrávajú špecifickú úlohu najmä v súvislosti s činnosťami na úseku kybernetickej bezpečnosti, akými je dôsledná analýza rizík zraniteľností napríklad vykonaním penetračného testovania.

[892] ICC, Office of the Prosecutor, Draft policy on cyber-enabled crimes under the Rome Statute, 6. marec 2025, s. 12-14, dostupné 05.12.2025 na: LINK
[893] Ibid.
[894] Lehota na uchovávanie lokalizačných údajov neexistuje. K tomu viac pozri výklad k § 116 TP.

Penetračné testovanie je autorizovaným simulovaným kybernetickým útokom na informačné systémy, siete alebo aplikácie s cieľom overiť ich reálnu úroveň bezpečnosti, identifikovať zraniteľnosti a posúdiť, do akej miery sú zneužiteľné v praxi.[895] Aby v praxi takéto penetračné testovanie, v prípade vzniku škody, bolo možné označiť za okolnosti vylučujúce protiprávnosť podľa § 27 a nasl. Trestného zákona musia byť splnené predpoklady uvedené nižšie.

Dovolené riziko

Podmienky splnenia okolnosti vylučujúcej protiprávnosť vo forme dovoleného rizika sú upravené v § 27 ods. 1 Trestného zákona. Penetračné testovanie nebude trestným činom vo forme útoku na počítačový systém alebo určité dáta, ak sa bude vykonávať v rámci výskumu alebo vývoja produktu, alebo služby za podmienky, že tento postup je plne v súlade s posledným vývojom a poznaním v oblasti kybernetickej bezpečnosť. Podmienky dovoleného rizika, ako okolnosti vylučujúcej protiprávnosť budú naplnené najmä v prípade vlastného výskumu a vývoja, počas ktorého by sa simulovali určité zraniteľnosti, riziká a došlo by ku škode, alebo obmedzeniu prevádzky, poškodeniu alebo strate dát a súčasne by tento vývoj alebo výskum nebolo možné dosiahnuť resp. vykonať bez ohrozenia záujmu chráneného Trestným zákonom.[896] Súčasne by neboli splnené ďalšie okolnosti vylučujúce protiprávnosť vo forme výkonu práv a povinností alebo súhlasu poškodeného ako špeciálnych ustanovení k dovolenému riziku.[897] V zásade bude potrebné skúmať, či zvolené postupy vlastného výskumu a vývoja sú skutočne aktuálne a súčasne sú v odbornej verejnosti konsenzuálne prijímané ako správne a možné. Tieto by mali byť popísané v odsúhlasenej metodike príslušnej analýzy rizík. Súčasne môže ísť o situáciu pri pred-produkčnom testovaní produktu tzv. *„best friends*" testovaním u iných spriaznených subjektov, ktoré má otestovať bežný záťažový chod produktu. O dovolené riziko nepôjde, ak by zvolená metóda pre analýzu

895 U.S. Department of the Interior. Penetration Testing. Dostupné dňa 31.03.2026 na: LINK In: ANDRAŠKO, J.; MESARČÍK, M.; SOKOL, P. Právo kybernetickej bezpečnosti. 1. vyd. – Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2022, s. 29.
896 TURAY, L.; MIHÁLIK, S.; CÁDRA, R.; PETRIČKO, D. a kol. Trestný zákon. Komentár. 1. vydanie. Bratislava: C. H. Beck, 2025, s. 76.
897 TURAY, L.; MIHÁLIK, S.; CÁDRA, R.; PETRIČKO, D. a kol. Trestný zákon. Komentár. 1. vydanie. Bratislava: C. H. Beck, 2025, s. 78.

rizík nezodpovedala miere skutočného rizika vzniku škody, alebo by bola v rozpore s platným právom, dobrými mravmi, verejným záujmom alebo ľudskosťou.[898]

Výkon práv a povinností

Podmienky splnenia okolnosti vylučujúcej protiprávnosť vo forme výkonu práv a povinností sú upravené v § 28 ods. 1 Trestného zákona. Nepôjde o trestný čin, ak ide o výkon práva alebo povinnosti vyplývajúcich zo všeobecne záväzného právneho predpisu, z rozhodnutia súdu alebo iného orgánu verejnej moci, z plnenia pracovných či iných úloh alebo zo zmluvy, ktorá neodporuje všeobecne záväznému právnemu predpisu ani ho neobchádza. V prípade analýzy rizík metódami testovania, ich zisťovanie zraniteľnosti či miery dopadu na chod a poskytovanie služieb sa v praxi uskutočňuje najčastejšie prostredníctvom dohôd o výkone penetračného testovania, alebo inej metódy analýzy rizík. I keď samotnou zmluvou ako súkromnoprávnym záväzkom nie je možné vylúčiť trestnú zodpovednosť alebo účinne aplikovať okolnosť vylučujúcu protiprávnosť, nakoľko táto otázka patrí do posúdenia orgánov činných v trestnom konaní a súdu, jednoznačná a detailná formulácia použitých metód a rozsahu testovania výrazne posilní právnu istotu, či už páchateľa činu inak trestného alebo poškodeného a od tohto vymedzenia sa bude odvíjať i možná aplikácia tejto okolnosti vylučujúcej protiprávnosť.

Súhlas poškodeného

Podmienky splnenia okolnosti vylučujúcej protiprávnosť vo forme súhlasu poškodeného upravené v § 29 ods. 1 Trestného zákona. Čin inak trestný nie je trestným činom, ak bol vykonaný so súhlasom poškodeného daným vopred alebo súčasne s činom. Vo vzťahu k penetračnému testovaniu a iným formám zisťovania zraniteľností a ich dopadu bude tento súhlas spravidla vhodné uviesť a vymedziť práve vo vyššie uvedenej dohode, zmluve o výkone penetračného testovania, resp. inej dohodnutej metódy, kde sa odsúhlasí a dohodne, resp. kompenzuje i možný škodlivý následok. Uvedené vyplýva najmä z vnútornej logiky tejto okolnosti vylučujúcej protiprávnosť, že osoba je oprávnená súhlasiť, aby do jej práva zasiahol niekto iný.[899]

[898] TURAY, L.; MIHÁLIK, S.; CÁDRA, R.; PETRIČKO, D. a kol. Trestný zákon. Komentár. 1. vydanie. Bratislava: C. H. Beck, 2025, s. 77.
[899] TURAY, L.; MIHÁLIK, S.; CÁDRA, R.; PETRIČKO, D. a kol. Trestný zákon. Komentár. 1. vydanie. Bratislava: C. H. Beck, 2025, s. 79.

12.4.3 Počítačové trestné činy v užšom slova zmysle

Právna úprava počítačových trestných činov bola v podmienkach Slovenskej republiky zákonodarcom pomerne dlhý čas opomínaná. Záväzok, ktorý Slovenská republika vyjadrila pristúpením k Budapeštianskemu dohovoru bol premietnutý do trestnoprávnych kódexov až o niekoľko rokov neskôr, a to v dôsledku transpozície smernice 2013/40/EÚ.[900]

PRÍKLAD

S účinnosťou od 1. januára 2016 došlo k prijatiu nových skutkových podstát počítačových trestných činov, a to:

a) neoprávnený prístup do počítačového systému (§ 247 TZ),
b) neoprávnený zásah do počítačového systému (§ 247a TZ),
c) neoprávnený zásah do počítačového údaja (§ 247b TZ),
d) neoprávnené zachytávanie počítačových údajov (§ 247c TZ) a
e) výroba a držba prístupového zariadenia, hesla do počítačového systému alebo iných údajov (§ 247d TZ).[901]

Prijatím skutkových podstát počítačových trestných činov došlo k vypusteniu skutkovej podstaty trestného činu poškodenia a zneužitia záznamu na nosiči informácií podľa ustanovenia § 247 Trestného zákona v znení účinnom do 31. decembra 2015. Išlo o akúsi univerzálnu skutkovú podstatu kumulujúcou v sebe viacero spôsobov konania, ktorá však dostatočne nereflektovala trend v postihu počítačovej kriminality nastolený na pôde Európskej únie a Rady Európy, a preto bolo nevyhnutné vytvoriť nové individuálne skutkové podstaty. Súčasne boli touto právnou úpravou zo skutkových podstát trestného činu porušovania tajomstva prepravovaných správ podľa ustanovenia § 196 a nasl. TZ vyňaté konania týkajúce sa prenosu informácií prostredníctvom elektronickej komunikačnej služby a prenosu počítačových údajov v rámci počítačového systému, ktoré sú obsiahnuté v skutkovej podstate trestného činu neoprávneného zachytávania počítačových údajov podľa ustanovenia § 247c TZ.

[900] Smernica 2013/40/EÚ bola transponovaná do Trestného zákona zákonom č. 398/2015 Z. z. o európskom ochrannom príkaze v trestných veciach.

[901] Pozoruhodným javom je, že zákonodarca si pri preklade Budapeštianskeho dohovoru zvolil pojem „nezákonný" (prístup, zásah do počítačového systému atď.), pri preklade smernice 2013/40/EÚ sa od tohto pojmu odchýlil a nahradil ho slovom „protiprávny" a pri koncipovaní skutkových podstát počítačových trestných činov použil pojem „neoprávnený".

Z hľadiska systematiky Trestného zákona sú počítačové trestné činy zaradené v štvrtej hlave osobitnej časti Trestného zákona s názvom trestné činy proti majetku. Druhovým (skupinovým) objektom počítačových trestných činov je ochrana integrity, dostupnosti a dôvernosti[902] počítačových systémov a počítačových údajov.

Subjekt počítačových trestných činov je všeobecný, s výnimkou trestného činu neoprávneného zachytávania počítačových údajov podľa ustanovenia § 247c ods. 2 TZ, ktorý môže spáchať iba osoba, ktorá je zamestnancom poskytovateľa elektronickej komunikačnej služby, a preto ide o subjekt špeciálny.

Neoprávnený prístup do počítačového systému (§ 247 TZ)[903]

Uvedené zákonné ustanovenie pozostáva z jednej základnej skutkovej podstaty a dvoch kvalifikovaných skutkových podstát. Z hľadiska závažnosti je trestný čin neoprávneného prístupu do počítačového systému vo všetkých odsekoch prečinom, a preto treba mať na pamäti aj možnosť aplikácie materiálneho korektívu v zmysle ustanovenia § 10 ods. 2 TZ, resp. pri mladistvých páchateľoch v zmysle ustanovenia § 95 ods. 2 TZ. V prípade trestnej zodpovednosti právnických osôb sú podmienky pre aplikáciu materiálneho korektívu uvedené v ustanovení § 4 ods. 3 ZoTZPO. Treba brať do úvahy najmä to, do akej miery páchateľ narušil súkromie užívateľa, čo bolo cieľom páchateľa, napríklad či len poukázať na nedostatočné zabezpečenie počítačového systému alebo získať prístup k citlivým údajom a podobne. Nie je celkom bezvýznamné, či ide o počítačový systém pracovný alebo súkromný, ale ani to, či je počítač na pracovisku voľne prístupný, resp. či páchateľ využil na prístup do počítačového systému počítačovú sieť. Určite bude potrebné skúmať aj rodinné vzťahy, napr. či neoprávnený vstup do počítačového systému bol medzi blízkymi osobami, napríklad manželmi, resp. súrodencami.[904]

[902] K tomu pozri kapitolu 1. Teoretické základy kybernetickej bezpečnosti.

[903] Ustanovenie § 247 TZ:
„(1) Kto prekoná bezpečnostné opatrenie, a tým získa neoprávnený prístup do počítačového systému alebo jeho časti, potrestá sa odňatím slobody až na dva roky.
(2) Odňatím slobody na šesť mesiacov až tri roky sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 a) závažnejším spôsobom konania, alebo b) a spôsobí ním značnú škodu.
(3) Odňatím slobody na jeden rok až päť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 a) a spôsobí ním škodu veľkého rozsahu, alebo b) ako člen nebezpečného zoskupenia."

[904] ZÁHORA, J.: Aktuálne trendy v postihu počítačovej kriminality v Slovenskej republike. In Justičná revue. 2016, č. 3, s. 323 – 340.

Objektom trestného činu neoprávneného prístupu do počítačového systému podľa ustanovenia § 247 TZ je ochrana počítačového systému ako celku, ako aj ochrana časti počítačového systému pred akýmkoľvek neoprávneným prístupom.

Objektívna stránka trestného činu neoprávneného prístupu do počítačového systému spočíva v tom, že páchateľ prekoná bezpečnostné opatrenie, čím získa neoprávnený prístup do počítačového systému alebo jeho časti. Trestným je už prístup do systému, nie je potrebné ďalšie poškodenie, zmena alebo prehliadanie údajov.

V tejto súvislosti sa môžeme stretnúť s pojmami ako tzv. *hacking* alebo *cracking.*[905] Tzv. *hacking* je činnosť odvodená od pojmu *hacker,* čo je v odbornej komunite pojem označujúci užívateľa, ktorý zo svojho počítača neoprávnene preniká do cudzích počítačových systémov. Hacker sa síce častokrát pohybuje na hrane zákona, avšak jeho motiváciou je poznanie. Cieľ hackera je preniknúť do systému a preskúmať jeho útroby. Akonáhle však tento cieľ dosiahne, je spokojný, pretože hackerská etika zakazuje dáta na „nabúranom" počítači akokoľvek meniť (až na výnimky, akými sú napríklad zahládzanie stôp, ktoré zostanú po tomto prieniku do systému.)[906] Tzv. *cracking* je všeobecne činnosť prelamovania niečoho, napríklad hesla, ktoré v zašifrovanej (napr. hashom) podobe uniklo z databázy. Crackeri vyhľadávajú heslá a snažia sa neoprávnene vniknúť do systémov, aby z nich odcudzili, pozmenili či zničili dáta, rovnako tak zavádzajú do systémov škodlivé kódy.[907]

Z hľadiska štruktúry objektívnej stránky ide o zloženú kumulatívnu skutkovú podstatu, pretože sú v nej kumulatívne vyjadrené dve konania. Na spáchanie trestného činu musí byť použité jednak prekonanie bezpečnostného opatrenia, prostredníctvom ktorého dôjde k neoprávnenému prístupu do počítačového systému alebo jeho časti, teda páchateľ musí svojim konaním naplniť oba znaky. Ak by v konaní páchateľa jeden z nich absentoval, skutok by nemohol byť kvalifikovaný podľa tohto ustanovenia.

Pojem počítačový systém nemá legálnu definíciu v Trestnom zákone ani v Trestnom poriadku. Čl. 1 písm. a) Budapeštianskeho dohovoru pod pojmom počítačový systém rozumie *„zariadenie alebo skupinu vzájomne prepojených alebo súvisiacich zariadení, z ktorých jedno zariadenie alebo viaceré zariadenia vykonávajú automatizované spracúvanie údajov na základe*

[905] Z pohľadu trestnej zodpovednosti je však irelevantné či sa konkrétny subjekt označuje za „dobrého" hackera alebo „zlého" crackera, prípadne hacktivistu a pod.
[906] LITTMAN, J.: Hacker: podivný život a zločiny počítačového génia Kevina Poulsena. Praha: Práh, 1988, s. 10. In: SMEJKAL, V.: Kybernetická kriminalita. 2. vyd. Plzeň : Aleš Čeněk, 2018. s. 181.
[907] Ibid, s. 181.

programu." Smernica 2013/40/EÚ sa odklonila od používania pojmu počítačový systém, ktorý nahradila pojmom informačný systém, ktorého definícia je upravená v čl. 2 písm. a) smernice 2013/40/EÚ a možno pod ňou rozumieť *„zariadenie alebo skupinu navzájom prepojených alebo súvisiacich zariadení, z ktorých jedno alebo viaceré automaticky spracúvajú počítačové údaje podľa programu, ako aj počítačové údaje, ktoré toto zariadenie alebo skupina zariadení ukladá, spracúva, opätovne získava alebo prenáša na účely svojho fungovania, používania, ochrany a údržby.*" Rozšírením definície preto došlo k ochrane počítačových údajov, ktoré sú uložené, spracovávané, sprístupňované alebo prenášané v dôsledku fungovania, používania, ochrany a údržby zariadenia, resp. skupiny zariadení určených na automatické spracovanie údajov prostredníctvom programu. Je zrejmé, že oba pojmy sú formulované čo najširšie tak, aby do seba pojali hardvérové aj softvérové vybavenie, rovnako aj dáta, teda v praxi pôjde nielen o mobil, laptop, server, ale aj webové sídlo, mobilnú aplikáciu, program atď.[908]

Pod bezpečnostným opatrením možno rozumieť každé ochranné opatrenie (heslo, prístupový kód, elektronický certifikát, biometrické údaje a pod.), ktoré zabraňuje neoprávnenému prístupu do počítačového systému. Prekonanie bezpečnostného opatrenia možno pripodobniť k spáchaniu trestného činu vlámaním vykonaným v kybernetickom priestore, kedy páchateľ vnikne do počítačového systému, resp. jeho časti prekonaním uzamknutia alebo inej zabezpečovacej prekážky použitím sily alebo ľsťou.

Pre použitie sily môžu byť príznačné viac či menej sofistikované prejavy zločinnej vôle páchateľa, napríklad manuálne prelamovanie hesla skúšaním rôznych kombinácií prihlasovacích údajov, využitie programov zameraných na dešifrovanie hesiel,[909] ale aj typ útoku *session hijacking*, kedy sa páchateľ dostáva k prihlasovacím údajom prostredníctvom súborov *cookies* uložených vo webovom prehliadači poškodeného.

Pod pojmom získanie neoprávneného prístupu do počítačového systému alebo jeho časti možno rozumieť akékoľvek konanie, ktoré páchateľovi umožní neoprávnenú dispozíciu nad počítačovým systémom, resp. jeho časťou a využitie jeho informačného obsahu. Trestnoprávny postih je však podmienený preniknutím do počítačového systému alebo do

[908] DRAŽOVÁ, P. *§ 247 TZ Neoprávnený prístup do počítačového systému.* In STRÉMY, T., KURILOVSKÁ, R. a kol.. Trestný zákon. Komentár. Wolters Kluwer, Bratislava, ISBN:, 978-80-7676-534-4, 2022, s. 576.

[909] Páchatelia na prelamovanie hesiel častokrát používajú slovníkový útok (*dictionary attack*) alebo útok hrubou silou (*brute force attack*). Slovníkový útok značí spôsob, kedy páchateľ na prekonanie zabezpečenia používa databázu najčastejšie sa opakujúcich hesiel, kým pri útoku hrubou silou je potrebné použiť špeciálny softvér, ktorý postupne skúša rôzne kombinácie znakov až do momentu, kým heslo neuhádne, čo je však spojené s určitou časovou náročnosťou.

ktorejkoľvek jeho časti bez náležitého oprávnenia, to znamená bez súhlasu vlastníka či iného držiteľa (administrátora) práv systému alebo jeho časti, alebo nie je povolené *ex lege*. Avšak musí ísť v zmysle § 247 ods.1 TZ o prístup neoprávnený, pričom nie je rozhodný dôvod ktorý viedol k neoprávnenému prístupu (náhoda, nález, plnenie si pracovných povinností). Súčasne naplnenie tohto znaku nevylučuje ani výnimočne nízka úroveň tohto bezpečnostného opatrenia alebo chyba v zabezpečení počítačového systému.[910] Hoci spôsobenie škody nie je zákonným znakom základnej skutkovej podstaty tohto trestného činu, spôsobenie značnej škody, resp. škody veľkého rozsahu je okolnosťou umožňujúcou použitie vyššej trestnej sadzby.

Subjektom môže byť ktorákoľvek trestne zodpovedná osoba, a to nielen fyzická osoba, ale s poukazom na ustanovenie § 3 ZoTZPO aj právnická osoba, a to vo všetkých ustanoveniach § 247 TZ. I keď sa uvedené ustanovenie nachádza v norme upravujúcej súhlas poškodeného podľa § 211 TP, kvôli nedôslednosti zákonodarcu však v tomto ustanovení figuruje ešte pôvodný názov trestného činu (poškodenia a zneužitia záznamu na nosiči informácií, ktorý v sebe kumuloval viaceré súčasné skutkové podstaty počítačových trestných činov), sme toho názoru, že ak sa má ponechať ustanovenie § 247 TZ medzi trestnými činmi, na ktoré sa vzťahuje súhlas poškodeného, je potrebné upraviť názov a doplniť aj ostatné ustanovenia podľa § 247a – 247d TZ, čo by viedlo k naplneniu zmyslu ustanovenia § 211 TP ako individuálneho posúdenia trestného činu zo strany poškodeného a rešpektovania jeho vôle.

Subjektívna stránka vyžaduje vo všetkých odsekoch § 247 TZ úmyselné zavinenie. Z hľadiska trestnoprávne relevantných vývojových štádií trestného činu Trestný zákon rozlišuje prípravu na zločin, pokus trestného činu a dokonaný trestný čin. Keďže trestný čin neoprávneného prístupu do počítačového systému je vo všetkých odsekoch prečinom, príprava naň nebude trestná, avšak pokus o trestný čin (teda aj pokus o prečin) definovaný v ustanovení § 14 ods. 1 TZ ako konanie, ktoré bezprostredne smeruje k dokonaniu trestného činu, ktorého sa páchateľ dopustil v úmysle spáchať trestný čin, ak nedošlo k dokonaniu trestného činu, je trestný podľa trestnej sadzby ustanovenej za dokonaný trestný čin.

[910] K tomu pozri napr. rozhodnutie NS ČR, sp. zn. 8 Tdo 450/2024.

Neoprávnený zásah do počítačového systému (§ 247a TZ)[911]

Uvedené zákonné ustanovenie pozostáva z jednej základnej skutkovej podstaty a dvoch kvalifikovaných skutkových podstát. Z hľadiska závažnosti je trestný čin neoprávneného zásahu do počítačového systému v prvom a druhom odseku prečinom, v treťom odseku zločinom. Pri prvom a druhom odseku preto treba mať na zreteli aj možnosť aplikácie materiálneho korektívu v zmysle ustanovenia § 10 ods. 2 TZ, resp. pri mladistvých páchateľoch v zmysle ustanovenia § 95 ods. 2 TZ. V prípade trestnej zodpovednosti právnických osôb sú podmienky pre aplikáciu materiálneho korektívu uvedené v ustanovení § 4 ods. 3 ZoTZPO. V zahraničnej literatúre sa v kontexte s týmto trestným činom môžeme stretnúť aj s pojmom počítačová sabotáž (*computer sabotage*).[912] Uvedené ustanovenie implementuje čl. 5 Budapeštianskeho dohovoru o trestnosti zasahovania do počítačového systému a čl. 4 Smernice EÚ 2013/40 o útokoch na počítačové systémy, ktorý upravuje protiprávny zásah do informačného systému.

Objektom trestného činu neoprávneného zásahu do počítačového systému podľa ustanovenia § 247a TZ je záujem na správnom fungovaní počítačového systému ako celku,

[911] Ustanovenie § 247a TZ:
„(1) 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.
(2) Odňatím slobody na jeden rok až päť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) a spôsobí ním značnú škodu,
b) a spôsobí ním vážnu poruchu v činnosti štátneho orgánu, orgánu územnej samosprávy, súdu alebo iného orgánu verejnej moci,
c) tak, že zneužije osobné údaje iného s cieľom získať dôveru tretej strany, alebo
d) závažnejším spôsobom konania.
(3) Odňatím slobody na dva roky až osem rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) a spôsobí ním škodu veľkého rozsahu,
b) a spôsobí ním vážnu poruchu v kritickej infraštruktúre, alebo
c) ako člen nebezpečného zoskupenia."

[912] Sabotáž alebo aj záškodníctvo či úmyselné poškodzovanie niečoho pochádza z francúzskeho slova *les sabots* (dreváky). Za týmto pojmom sa odohráva príbeh vôbec prvej známej sabotáže v histórii ľudstva. Joseph-Marie Jacquard v roku 1801 vynašiel programovateľný tkáčsky stav, ktorý zjednodušil výrobu textílií, ale zároveň tým pripravil o prácu mnohých robotníkov. Tí na znak vzbury pohádzali svoje dreváky do stroja, aby tak znefunkčnili jeho prevádzku. Počítačová sabotáž je útok vedený v úmysle obmedziť alebo znefunkčniť prevádzku počítača, prípadne akejkoľvek jeho časti, v širšom ponímaní aj akéhokoľvek prostriedku informačno-komunikačných technológií formou fyzického alebo logického útoku.

ako aj jeho časti, teda aj ochrana integrity počítačového systému ako celku a jeho časti pred akýmkoľvek neoprávneným zásahom.[913]

Objektívna stránka trestného činu neoprávneného zásahu do počítačového systému je daná alternatívne, a to dvomi spôsobmi konania. Prvý spôsob zahŕňa neoprávnené vkladanie, prenášanie, poškodenie, vymazanie, zhoršenie kvality, pozmenenie, potlačenie alebo zneprístupnenie počítačových údajov, v dôsledku ktorého páchateľ obmedzí alebo preruší fungovanie počítačového systému alebo jeho časti. Druhý spôsob konania môže spočívať v tom, že páchateľ urobí neoprávnený zásah do technického alebo programového vybavenia počítača a získané informácie neoprávnene zničí, poškodí, vymaže, pozmení alebo zníži ich kvalitu a následkom toho obmedzí alebo preruší fungovanie počítačového systému alebo jeho časti. Na trestnosť páchateľa však postačuje, ak koná niektorým z uvedených spôsobov, pričom v niektorých prípadoch môže ísť aj o kumuláciu týchto spôsobov konania.[914]

Pod pojmom obmedziť alebo prerušiť fungovanie počítačového systému možno rozumieť akékoľvek konanie, ktoré zabraňuje správnemu fungovaniu počítačového systému. Z hľadiska vzniku trestnej zodpovednosti je pritom irelevantné či ide o dočasné alebo trvalé obmedzenie, resp. prerušenie fungovania, rovnako je vo vzťahu k vzniku trestnej zodpovednosti bezpredmetné či ide o obmedzenie, resp. prerušenie fungovania celého počítačového systému alebo iba niektorej jeho časti. Tieto skutočnosti však samozrejme majú svoj význam, nakoľko ide o okolnosti, za ktorých bol čin spáchaný, na ktoré súd prihliada pri ukladaní trestu. Z pohľadu ukladania trestu bude tiež významnou skutočnosťou aj to či obmedzenie alebo prerušenie fungovania počítačového systému ovplyvnilo verejný záujem alebo poškodilo práva súkromnej osoby. Je zrejmé, že ak dôjde v dôsledku tohto činu napríklad k znefunkčneniu semaforov v celom okrese, tak dôjde k porušeniu významnejšieho záujmu chráneného Trestným zákonom ako v prípade, kedy by došlo napríklad k výpadku bezpečnostnej kamery, ktorá monitoruje vstup do súkromného objektu.[915]

[913] DRAŽOVÁ, P. *§ 247a TZ Neoprávnený zásah do počítačového systému.* In STRÉMY, T., KURILOVSKÁ, R. a kol.. Trestný zákon. Komentár. Wolters Kluwer, Bratislava, ISBN: 978-80-7676-534-4, 2022 s. 581.
[914] DRAŽOVÁ, P. *§ 247a TZ Neoprávnený zásah do počítačového systému.* In STRÉMY, T., KURILOVSKÁ, R. a kol.. Trestný zákon. Komentár. Wolters Kluwer, Bratislava, ISBN: 978-80-7676-534-4, 2022 s. 581-582.
[915] DRAŽOVÁ, P. *§ 247a TZ Neoprávnený zásah do počítačového systému.* In STRÉMY, T., KURILOVSKÁ, R. a kol.. Trestný zákon. Komentár. Wolters Kluwer, Bratislava, ISBN: 978-80-7676-534-4, 2022 s. 582.

Najčastejšie za obmedzením alebo prerušením fungovania počítačového systému stoja útoky odmietnutia služby DoS *(denial of service)* a DDoS *(distributed denial of service)*. Primárnym cieľom útokov odmietnutia služby je zahltiť alebo dočasne vyradiť z prevádzky počítačový systém vysokým počtom požiadaviek v jednom časovom okamihu, ktoré nie je možné naraz spracovať. V dôsledku tohto útoku dochádza k obmedzeniu, spomaleniu alebo zablokovaniu prístupu k danej službe (napríklad webovej stránky). Rozdiel medzi útokom DoS a DDoS tkvie v spôsobe realizácie vedeného útoku.

V súvislosti s postihovaním útokov odmietnutia služby smernica 2013/40/EÚ ponechala na úvahu členských štátov Európskej únie, aby určili, čo podľa ich vnútroštátneho práva a praxe predstavuje závažný následok, ako napríklad narušenie systémových služieb zásadného spoločenského významu alebo spôsobenie veľkých finančných nákladov či strata osobných údajov alebo citlivých informácií. Všetky tieto skutočnosti zákonodarca reflektoval, a to najmä s prihliadnutím na kvalifikované skutkové podstaty trestného činu neoprávneného zásahu do počítačového systému. Odlišný prístup je možné vidieť v prípade Budapeštianskeho dohovoru. Ten predpokladal následok vo forme spôsobenia vážneho prerušenia alebo obmedzenia počítačového systému *(serious hindering)*, čo sa však nepretransformovalo do znenia Trestného zákona, nakoľko zákonodarca koncipoval znenie základnej skutkovej podstaty tak, aby mohlo byť stíhané každé obmedzenie alebo prerušenie počítačového systému za predpokladu, že bolo urobené neoprávnene niektorým z konaní uvedených v základnej skutkovej podstate. To, samozrejme, nevylučuje aplikáciu materiálneho korektívu.

Pod pojmom neoprávnené vkladanie, prenášanie, poškodenie, vymazanie, zhoršenie kvality, pozmenenie, potlačenie alebo zneprístupnenie počítačových údajov možno rozumieť situáciu, kedy použitím špecifického druhu škodlivého kódu, napríklad ransomvéru (*ransomware*)[916] a jeho vložením do tej časti operačného systému, ktorý spúšťa počítač, túto funkciu zašifruje, v dôsledku čoho počítač nejde spustiť. Typickým neoprávneným zásahom

[916] R*ansomware* je pojem zložený z dvoch slov, a to *ransom* (výkupné) a *software* (počítačový program). Ide o typ škodlivého kódu, ktorý môžu útočníci využiť na uzamknutie zariadenia alebo zašifrovanie jeho obsahu s cieľom vymôcť od majiteľa daného zariadenia peniaze. Na oplátku autori škodlivého kódu sľubujú, samozrejme bez akýchkoľvek záruk, obnovenie prístupu k zablokovanému zariadeniu alebo dátam. Ransomvéry sa ďalej delia na poddruhy, a to v závislosti od toho, aký druh činnosti vykonávajú, napr. screen locker ransomware, PIN locker ransomware, disk coding ransomware, crypto-ransomware atď.

do programového vybavenia počítača je rozširovanie malvéru (*malware*),[917] teda škodlivého kódu, programu, ktorý vykonáva záškodnícku činnosť, a to za účelom monitorovania činnosti *(spyware, trojan, keylogger)*, zberu informácií *(adware)*, prevzatia kontroly nad systémom *(bot)*, poškodenia či zničenia systému, vrátane dát *(virus, worms, payloads)* a nie je ničím nezvyčajným, že útočníci používajú aj rôzne kombinácie týchto škodlivých programov.[918]

Pod neoprávnený zásah do technického vybavenia počítača možno subsumovať aj také konanie páchateľa, ktorý by si počínal napríklad tak, že odpojí počítač od zdroja elektriny, v dôsledku čoho dôjde k pozastaveniu určitých procesov, ktoré bežia, následkom čoho nastáva nielen okamžitá strata údajov, ale aj prerušenie fungovania počítačového systému.

Ako správne uvádza Záhora, vyvstáva otázka, prečo zákonodarca používa rozdielnu terminológiu zásah do počítača a nie do počítačového systému, aký používa v iných ustanoveniach. V odbornej literatúre je pojem počítač považovaný za užší pojem ako počítačový systém, keďže počítačový systém = počítač + periférne zariadenia.[919] Pokiaľ by páchateľ zasiahol napríklad do externej mechaniky (CD, DVD), respektíve do externého HDD alebo SSD disku a znemožnil by tým čítanie na týchto nosičoch uložených počítačových údajov, páchateľ by sa zrejme mohol úspešne obhajovať tým, že nešlo o počítač. Preto by bolo vhodné použiť namiesto slova počítač pojem počítačový systém, resp. jeho časť v rámci jednotnej terminológie používanej pri ostatných počítačových trestných činoch.[920] Hoci spôsobenie škody nie je zákonným znakom základnej skutkovej podstaty tohto trestného činu, spôsobenie značnej škody, resp. škody veľkého rozsahu je okolnosťou umožňujúcou použitie vyššej trestnej sadzby.

Za zmienku stojí aj kvalifikačný znak v § 247a ods. 2 písm. b) TZ, ktorý podmieňuje použitie vyššej trestnej sadzby, ak takýto zásah spôsobí vážnu poruchu v činnosti štátneho orgánu, orgánu územnej samosprávy, súdu alebo iného orgánu verejnej moci. Iným

---

[917] Malvér je v širokej verejnosti častokrát zamieňaný s pojmom vírus. Vírus je však program, ktorý modifikuje ostatné programy. Je možné ho pripodobniť ľudskému vírusu, ktorý tiež musí mať hostiteľa, prostredníctvom ktorého sa šíri na ďalších ľudí. Aj vírus počítačový musí mať pomyselného hostiteľa (program) odkiaľ sa kopíruje do ďalších programov, dokumentov atď. Vírusy sú preto iba malou množinou škodlivých, malicióznych programov.

[918] DRAŽOVÁ, P. *§ 247a TZ Neoprávnený zásah do počítačového systému.* In STRÉMY, T., KURILOVSKÁ, R. a kol.. Trestný zákon. Komentár. Wolters Kluwer, Bratislava, ISBN: 978-80-7676-534-4, 2022 s. 560.

[919] SMEJKAL, V.: Kybernetická kriminalita. 2. vyd. Plzeň : Aleš Čeněk, 2018. s. 29.

[920] ZÁHORA, J.: Aktuálne trendy v postihu počítačovej kriminality v Slovenskej republike. In Justičná revue. 2016, č. 3, s. 323 – 340.

kvalifikačným znakom podľa § 247a ods. 2 písm. c) TZ je, že páchateľ zneužije osobné údaje iného, napríklad prihlasovacie údaje poškodeného, s cieľom získať dôveru tretej strany, napr. rôznymi technikami sociálneho inžinierstva, phishingom a podobne, a spôsobom formulovaným v základnej skutkovej podstate znefunkční počítačový systém.

Subjektom môže byť ktorákoľvek trestne zodpovedná osoba, a to nielen fyzická osoba, ale s poukazom na ustanovenie § 3 ZoTZPO aj právnická osoba, a to vo všetkých ustanoveniach § 247a TZ.

Subjektívna stránka vyžaduje vo všetkých ustanoveniach § 247a TZ úmyselné zavinenie.

Je potrebné tiež upriamiť pozornosť na vzájomný vzťah ustanovení § 247b ods. 1 TZ a § 247a ods. 1 písm. a) TZ. Ak páchateľ neoprávnene poškodí, vymaže, pozmení, potlačí alebo zneprístupní počítačové údaje alebo zhorší ich kvalitu, je zrejmé, že naplní znaky skutkovej podstaty trestného činu neoprávneného zásahu do počítačového údaja podľa § 247b TZ. Avšak, ak niektorý z týchto spôsobov páchateľ vykoná, v dôsledku čoho dôjde k obmedzeniu alebo prerušeniu fungovania počítačového systému alebo jeho časti, naplní znaky skutkovej podstaty trestného činu neoprávneného zásahu do počítačového systému podľa § 247a ods. 1 písm. a) TZ. Z uvedeného možno preto dôvodiť, že tieto dve skutkové podstaty sú navzájom v pomere špeciality pretože porušenie objektu chráneného skutkovou podstatou trestného činu neoprávneného zásahu do počítačového údaja je iba akýmsi vedľajším produktom pri porušení objektu chráneného skutkovou podstatou trestného činu neoprávneného zásahu do počítačového systému, teda jednočinný súbeh týchto trestných činov je vylúčený.

Neoprávnený zásah do počítačového údaja (§ 247b TZ)[921]

Uvedené zákonné ustanovenie pozostáva z jednej základnej skutkovej podstaty a dvoch kvalifikovaných skutkových podstát. Z hľadiska závažnosti je trestný čin neoprávneného zásahu do počítačového údaja v prvom a druhom odseku prečinom, v treťom odseku zločinom. Pri prvom a druhom odseku preto treba mať na pamäti aj možnosť aplikácie materiálneho korektívu v zmysle ustanovenia § 10 ods. 2 TZ, resp. pri mladistvých páchateľoch v zmysle ustanovenia § 95 ods. 2 TZ. V prípade trestnej zodpovednosti právnických osôb sú podmienky pre aplikáciu materiálneho korektívu uvedené v ustanovení § 4 ods. 3 ZoTZPO. Uvedené ustanovenie je implementujúcou normou čl. 4 Budapeštianskeho dohovoru o trestnosti zasahovania do údajov a čl. 5 Smernice EÚ 2013/40 o útokoch na počítačové systémy, ktorý upravuje protiprávny zásah do údajov.

Objektom trestného činu neoprávneného zásahu do počítačového údaja podľa ustanovenia § 247b TZ je ochrana integrity, dostupnosti a dôvernosti uchovávaných počítačových údajov a programov v rámci počítačového systému.

Objektívna stránka trestného činu neoprávneného zásahu do počítačového údaja spočíva v tom, že páchateľ úmyselne poškodí, vymaže, pozmení, potlačí alebo zneprístupní počítačové údaje alebo zhorší ich kvalitu v rámci počítačového systému alebo jeho časti. Na trestnosť páchateľa stačí, ak koná niektorým z uvedených spôsobov, pričom v niektorých prípadoch však môže ísť aj o kumuláciu týchto spôsobov konania. Rovnako je pre trestnosť tohto činu irelevantné či páchateľ vykonal neoprávnený zásah do počítačového údaja v dôsledku prekonania určitého bezpečnostného zariadenia, a teda došlo aj k naplneniu znakov samostatnej skutkovej podstaty trestného činu neoprávneného prístupu do počítačového systému podľa ustanovenia § 247 TZ alebo ide o páchateľa, ktorý má k systému oprávnený prístup.

---

[921] Ustanovenie § 247b TZ:
„(1) 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.
(2) Odňatím slobody na jeden rok až päť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) a spôsobí ním značnú škodu,
b) a spôsobí ním vážnu poruchu v činnosti štátneho orgánu, orgánu územnej samosprávy, súdu alebo iného orgánu verejnej moci,
c) tak, že zneužije osobné údaje iného s cieľom získať dôveru tretej strany, alebo
d) závažnejším spôsobom konania.
(3) Odňatím slobody na dva roky až osem rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) a spôsobí ním škodu veľkého rozsahu,
b) a spôsobí ním vážnu poruchu v kritickej infraštruktúre, alebo
c) ako člen nebezpečného zoskupenia."

Pojem počítačový údaj nemá legálnu definíciu v Trestnom zákone ani v Trestnom poriadku, avšak v zmysle definície podľa § 130 ods. 2 TZ je považovaný za vec. Počítačový údaj je na účely Budapeštianskeho dohovoru definovaný v čl. 1 písm. c) ako záznam skutočností, informácií alebo pojmov vo forme, ktorá je vhodná na spracovanie v počítačovom systéme, vrátane programu schopného spôsobiť, že počítačový systém vykoná určitú činnosť. Smernica 2013/40/EÚ vymedzila pojem počítačové údaje v čl. 2 písm. b) ako zastúpenia skutočností, informácií alebo pojmov vo forme vhodnej na spracovanie v informačnom systéme vrátane programu, ktorý zabezpečí, aby informačný systém vykonal funkciu.

Pojmy poškodiť počítačové údaje (*damage*) a zhoršiť kvalitu počítačových údajov (*deterioration*) odkazujú na spôsoby konania, ktoré sa môžu navzájom prekrývať a týkajú sa najmä negatívnych zmien integrity počítačových údajov alebo programov, ktoré majú za následok zmenu ich obsahu, výpovednej hodnoty, teda zmenu informácie, ktorej sú nositeľom Typickým príkladom je napríklad komprimácia fotografií, ktorá má za následok zhoršenie ich kvality alebo tzv. *website defacement attack*, čo je útok na vzhľad webovej stránky, kedy páchateľ neoprávnene prenikne do servera, na ktorom beží poškodená webová stránka a zmení jej vzhľad do požadovanej podoby, pričom tento typ útoku je v reálnom svete možné pripodobniť maľbe graffiti na stenu. Možno tiež uviesť, že poškodením počítačových údajov neraz dochádza aj k zhoršeniu ich kvality alebo k ich zneprístupneniu oprávnenej osobe.[922]

Pojem vymazať počítačové údaje (*deletion*) je ekvivalentom k faktickému zničeniu hmotnej veci. Ide o také konanie, ktoré smeruje k nezvrátiteľnej deštrukcii údajov, a teda ich ďalšej neupotrebiteľnosti.

Pozmeniť počítačové údaje (*alteration*) znamená akúkoľvek modifikáciu dát, teda akýkoľvek iný zásah do ich pôvodného obsah spočívajúci napríklad v prepísaní dát inými dátami, ktoré sú nositeľmi inej informácie. Napríklad také vkladanie alebo kopírovanie vírusov či akýchkoľvek škodlivých kódov do počítačových dát spôsobuje ich modifikáciu.

Potlačiť počítačové údaje (*suppression*) znamená aj odňať niekomu právo na niečo, čiže v zásade ide o podobný význam ako v prípade z*neprístupnenia* počítačových údajov, ktoré odkazuje na akékoľvek konanie, ktoré je spôsobilé zabrániť alebo odňať prístup k údajom určitej oprávnenej osobe, ktorá má prístup, resp. má vo svojej dispozícii technický

[922] DRAŽOVÁ, P. *§ 247b TZ Neoprávnený zásah do počítačového údaja.* In STRÉMY, T., KURILOVSKÁ, R. a kol.. Trestný zákon. Komentár. Wolters Kluwer, Bratislava, ISBN: 978-80-7676-534-4, 2022 s. 588.

nosič, zariadenie, na ktorom sa údaje nachádzajú. Pod túto časť skutkovej podstaty predmetného trestného činu možno typicky subsumovať útoky prostredníctvom šírenia ransomvéru, ktorý údaje zašifruje a oprávnenej osobe tým *de facto* odníme prístup k nim spravidla motivovaný tvorbou informačnej nerovnováhy, alebo tvorbou malformácie.

Hoci spôsobenie škody nie je zákonným znakom základnej skutkovej podstaty tohto trestného činu, spôsobenie značnej škody, resp. škody veľkého rozsahu je okolnosťou umožňujúcou použitie vyššej trestnej sadzby.

Subjektom môže byť ktorákoľvek trestne zodpovedná osoba, a to nielen fyzická osoba, ale s poukazom na ustanovenie § 3 ZoTZPO aj právnická osoba, a to vo všetkých ustanoveniach § 247b TZ.

Subjektívna stránka vyžaduje vo všetkých ustanoveniach § 247b TZ úmyselné zavinenie.

Zákonodarca pri transpozícii tohto trestného činu do Trestného zákona pravdepodobne opomenul doplniť do návetia predmetnej skutkovej podstaty slovo „neoprávnene", zato celkom zbytočné sa javí uvedenie formy zavinenia, keďže platí interpretačné pravidlo uvedené v ustanovení § 17 TZ.[923] Preto sa domnievame, že jej správne vyjadrenie by malo znieť *„Kto neoprávnene poškodí…*", nakoľko obdobným spôsobom je to formulované aj v čl. 4 bod 1 Budapeštianskeho dohovoru – zasahovanie do údajov[924] a rovnako tak aj v čl. 5 smernice 2013/40/EÚ sa uvádza „bez oprávnenia". V opačnom prípade by sme sa mohli dostať do absurdnej situácie, kedy by bolo nutné stíhať aj skutky napĺňajúce znaky predmetnej skutkovej podstaty na tom základe, že v súčasnosti veľká časť populácie používa na komunikáciu šifrované mobilné aplikácie z dôvodu vyššieho stupňa zabezpečenia, pričom v rámci šifrovania jednoznačne dochádza k pozmeňovaniu prenášaných údajov. Takisto aj v situáciách, kedy používatelia využívajú na prehliadanie webových stránok rôzne anonymizačné nástroje,[925] čo je rovnako odôvodniteľné bezpečnostným hľadiskom, nepochybne dochádza k prepisovaniu lokalizačných údajov.

---

[923] Ustanovenie § 17 TZ: *„Pre trestnosť činu spáchaného fyzickou osobou treba úmyselné zavinenie, ak tento zákon výslovne neustanovuje, že stačí zavinenie z nedbanlivosti.*"

[924] Čl. 4 bod 1 Budapeštianskeho dohovoru: *„Každá strana prijme potrebné legislatívne a iné opatrenia, aby neoprávnené poškodenie, vymazanie, zhoršenie kvality, pozmenenie počítačových údajov alebo zamedzenie prístupu k nim boli trestným činom podľa jej vnútroštátneho právneho poriadku, ak boli spáchané úmyselne.*"

[925] Tým nemáme na mysli používanie anonymných okien v rámci webového prehliadača, ktorými je možné zamaskovať aktivitu v zariadení, z ktorého užívateľ pristupuje do siete. Navštívené webové lokality sa síce nezobrazia v histórii prehliadača, ale poskytovateľ pripojenia na internet (ISP) vidí presne kam, kedy a z akej adresy, prípadne z akého zariadenia sa užívateľ pripojil. Ide o používanie napríklad proxy serverov alebo VPN

Neoprávnené zachytávanie počítačových údajov (§ 247c TZ)[926]

Uvedené zákonné ustanovenie pozostáva z dvoch základných skutkových podstát uvedených v ustanoveniach § 247c ods. 1 a 2 TZ a dvoch kvalifikovaných skutkových podstát uvedených v ustanoveniach § 247c ods. 3 a 4 TZ. Z hľadiska závažnosti je trestný čin neoprávneného zachytávania počítačových údajov v prvom, druhom a treťom odseku prečinom, v štvrtom odseku zločinom. Pri prvom, druhom a treťom odseku preto treba mať na pamäti aj možnosť aplikácie materiálneho korektívu v zmysle ustanovenia § 10 ods. 2 TZ, resp. pri mladistvých páchateľoch v zmysle ustanovenia § 95 ods. 2 TZ. V prípade trestnej zodpovednosti právnických osôb sú podmienky pre aplikáciu materiálneho korektívu uvedené v ustanovení § 4 ods. 3 ZoTZPO. V kybernetickom priestore je tento trestný čin označovaný ako tzv. *sniffing*, pod ktorým možno rozumieť neoprávnené odpočúvanie, zachytávanie komunikácie na sieti, ktorého účelom je monitoring diania na sieti, zachytávanie hesiel, čítanie cudzích e-mailov, správ a podobne.[927]

Objektom trestného činu neoprávneného zachytávania počítačových údajov podľa ustanovenia § 247c TZ je ochrana tajomstva informácie (či už vo forme obrazu, zvuku, textu), ktorá je neverejne prenášaná z, do alebo v rámci počítačového systému, sekundárne aj ochrana súkromia pred neoprávneným odpočúvaním. Uvedené ustanovenie je implementujúcou normou čl. 2 Budapeštianskeho dohovoru o trestnosti nezákonného zachytávania údajov a čl. 6 Smernice EÚ 2013/40 o útokoch na počítačové systémy, ktorý

(*Virtual Private Network*) spojení či systému TOR (*The Onion Router*), prostredníctvom ktorých dochádza k zamaskovaniu aktivity aj pred poskytovateľom pripojenia na internet.

[926] Ustanovenie § 247c TZ:

„(1) 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 až na dva roky.

(2) Kto ako zamestnanec poskytovateľa elektronickej komunikačnej služby spácha čin uvedený v odseku 1 alebo inému úmyselne umožní spáchať taký čin, alebo pozmení alebo potlačí správu podanú prostredníctvom elektronickej komunikačnej služby, potrestá sa odňatím slobody na šesť mesiacov až tri roky.

(3) Odňatím slobody jeden rok až päť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 alebo 2

a) z osobitného motívu,

b) závažnejším spôsobom konania, alebo

c) spôsobí ním značnú škodu.

(4) Odňatím slobody na dva roky až osem rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 alebo 2

a) a spôsobí ním škodu veľkého rozsahu, alebo

b) ako člen nebezpečného zoskupenia."

[927] Tzv. *sniffing* je technika, pri ktorej dochádza k ukladaniu TCP paketov. Postupy môžu byť rôzne, napríklad Man-In-The-Middle je typ útoku, v rámci ktorého útočník vystupuje v komunikácii ako medzičlánok, packet sniffing je odchytávanie paketov obsahujúcich záujmovú komunikáciu a local sniffing využíva škodlivý softvér priamo na niektorom z komunikujúcich počítačov. K tomu pozri SMEJKAL, V.: Kybernetická kriminalita. 2. vyd. Plzeň : Aleš Čeněk, 2018. s. 344.

upravuje protiprávne zachytávanie údajov. Čl. 8 ods. 1 Dohovoru o ochrane ľudských práv a základných slobôd[928] ustanovuje právo každého na rešpektovanie svojho súkromného a rodinného života, obydlia a korešpondencie. Toto právo je zakotvené rovnako aj v čl. 22 Ústavy SR. Teda bez ohľadu na to, o aký spôsob prenosu informácii ide (telefón, e-mail, komunikačné aplikácie, fax), tieto sú postavené na roveň a je im poskytnutá rovnaká miera ochrany.

Objektívna stránka trestného činu neoprávneného zachytávania počítačových údajov podľa ustanovenia § 247c ods. 1 TZ spočíva v neoprávnenom zachytávaní počítačových údajov 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 podľa ustanovenia § 247c ods. 1 TZ alebo alternatívne v neoprávnenom zachytávaní počítačových údajov 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 alebo v umožnení inému spáchať taký čin alebo v pozmenení alebo potlačení správy podanej prostredníctvom elektronickej komunikačnej služby podľa ustanovenia § 247 ods. 2 TZ.

Pod pojmom neoprávnene treba rozumieť bez oprávnenia, pretože oprávnene v tomto prípade môžu konať iba orgány verejnej moci na základe písomného a odôvodneného príkazu súdu, a to buď v trestnom konaní (najmä podľa § 115 TP) alebo za splnenia zákonných podmienok ustanovených v zákone č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním).

Použitím analógie s ustanovením § 10 ods. 20 TP si pod pojmom zachytávanie počítačových údajov prostredníctvom technických prostriedkov si možno predstaviť akýkoľvek, najmä elektrotechnický, rádiotechnický, fototechnický, optický, mechanický, chemický a iný technický prostriedok alebo zariadenie alebo súbor týchto prostriedkov alebo zariadení používaných spravidla utajovaným spôsobom. Z uvedeného je teda zrejmé, že pod túto definíciu možno subsumovať široké množstvo zariadení od optických káblov, cez infračervené žiarenie, Bluetooth až po Wi-Fi. Do úvahy prichádza samozrejme aj

[928] Rada Európy, Európsky dohovor o ochrane ľudských práv a základných slobôd v znení protokolov č. 11 a 14, 4. november 1950, ETS 5. Dostupné na: LINK

odchytávanie prenášaných údajov prostredníctvom infikovania počítača malvérom, ktorý je schopný zmeniť vstupné zariadenie na výstupné, a tak napríklad vzdialene aktivovať na počítači nahrávanie zvuku cez slúchadlá bez vedomia používateľa.

Rozdiel medzi základnými skutkovými podstatami spočíva v subjekte trestného činu. V § 247c ods. 1 TZ je uvedený všeobecný subjekt a v § 247c ods. 2 TZ subjekt špeciálny, teda osoba, ktorá je zamestnancom poskytovateľa elektronickej komunikačnej služby. Pojem elektronická komunikačná služba odkazoval na v súčasnosti už neexistujúci zákon o elektronických komunikáciách, ktorý bol zrušený a nahradený ZEK. § 2 ods. 17 ZEK obsahuje legálnu definíciu pojmu služba.[929] Teda pôjde predovšetkým o zamestnancov poskytovateľov pripojenia na internet, ale aj poskytovateľov interpersonálnych komunikačných služieb. Keďže z povahy veci môže byť zamestnancom iba fyzická osoba, páchateľom skutkovej podstaty trestného činu podľa ustanovenia § 247c ods. 2 TZ môže byť iba trestne zodpovedná fyzická osoba, ktorá je zamestnancom poskytovateľa elektronickej komunikačnej služby, avšak páchateľom skutkovej podstaty trestného činu podľa ustanovenia § 247c ods. 1 TZ môže byť s poukazom na ustanovenie § 3 ZoTZPO aj právnická osoba. Tento trestný čin sa však nevzťahuje iba na obsah komunikácie, ale akékoľvek počítačové údaje vrátane prevádzkových či lokalizačných údajov (neoprávnený packet sniffing, neoprávnené packet analýzy, dekriptory) na rozdiel od trestného činu porušovania tajomstva prepravovaných správ podľa §196 - 198 TZ alebo trestného činu porušovania dôvernosti ústneho prejavu a iného prejavu osobnej povahy podľa § 377 TZ, ktoré sú vo vzťahu špeciality k tomuto trestnému činu.[930] Subjektívna stránka vyžaduje vo všetkých odsekoch § 247c TZ úmyselné zavinenie.

[929] Ustanovenie § 2 ods. 17 ZEK:
„Služba je služba obvykle poskytovaná za odplatu prostredníctvom sietí, ktorá zahŕňa službu prístupu k internetu, interpersonálnu komunikačnú službu alebo služby pozostávajúce úplne alebo prevažne z prenosu signálov, napríklad prenosové služby používané na poskytovanie služieb komunikácie stroj-stroj (M2M) a na rozhlasové a televízne vysielanie. Službou nie je poskytovanie obsahu alebo vykonávanie redakčnej kontroly obsahu prenášaného pomocou sietí a služieb."

[930] DRAŽOVÁ, P. *§ 247c TZ Neoprávnené zachytávanie počítačových údajov.* In STRÉMY, T., KURILOVSKÁ, R. a kol.. Trestný zákon. Komentár. Wolters Kluwer, Bratislava, ISBN: 978-80-7676-534-4, 2022 s. 593.

Výroba a držba prístupového zariadenia, hesla do počítačového systému alebo iných údajov (§ 247d TZ)[931]

Uvedené zákonné ustanovenie pozostáva z jednej základnej skutkovej podstaty a dvoch kvalifikovaných skutkových podstát. Z hľadiska závažnosti je trestný čin výroby a držby prístupového zariadenia, hesla do počítačového systému alebo iných údajov vo všetkých odsekoch prečinom. Z toho dôvodu je potrebné mať na pamäti aj možnosť aplikácie materiálneho korektívu v zmysle ustanovenia § 10 ods. 2 TZ, resp. pri mladistvých páchateľoch v zmysle ustanovenia § 95 ods. 2 TZ. V prípade trestnej zodpovednosti právnických osôb sú podmienky pre aplikáciu materiálneho korektívu uvedené v ustanovení § 4 ods. 3 ZoTZPO. Uvedené ustanovenie je implementujúcou normou čl. 6 Budapeštianskeho dohovoru o trestnosti zneužitia zariadení a čl. 7 Smernice EÚ 2013/40 o útokoch na počítačové systémy, ktorý upravuje nástroje na spáchanie trestných činov.

Objektom trestného činu výroby a držby prístupového zariadenia, hesla do počítačového systému alebo iných údajov podľa ustanovenia § 247d TZ je ochrana pred možným ohrozením vyplývajúcim z nekontrolovanej distribúcie prostriedkov slúžiacich na neoprávnené zásahy do počítačových systémov.[932]

Objektívna stránka trestného činu výroby a držby prístupového zariadenia, hesla do počítačového systému alebo iných údajov spočíva v tom, že páchateľ v úmysle spáchať niektorý z trestných činov podľa § 247 až 247c TZ vyrobí, dovezie, obstará, kúpi, predá, vymení, uvedie do obehu alebo akokoľvek sprístupní zariadenie, vrátane počítačového programu vytvorené na neoprávnený prístup do počítačového systému alebo jeho časti alebo

---

[931] Ustanovenie § 247d TZ:
„(1) 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.
(2) Odňatím slobody na šesť mesiacov až tri roky sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) závažnejším spôsobom konania, alebo
b) a spôsobí ním značnú škodu.
(3) Odňatím slobody na jeden rok až päť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) a spôsobí ním škodu veľkého rozsahu, alebo
b) ako člen nebezpečného zoskupenia."

[932] ZÁHORA, J.: Aktuálne trendy v postihu počítačovej kriminality v Slovenskej republike. In Justičná revue. 2016, č. 3, s. 323 – 340.

počítačové heslo, prístupový kód alebo podobné údaje umožňujúce prístup do počítačového systému alebo jeho časti.

Všetky počítačové trestné činy sú v každej základnej skutkovej podstate prečinmi a keďže z hľadiska vývojových štádií trestného činu je trestná iba príprava na zločin a pokus trestného činu, skutok, ktorý vykazuje znaky prípravy na prečin nemôže byť predmetom trestného stíhania. V niektorých prípadoch však Trestný zákon určité konania, ktoré sú svojou povahou len prípravou alebo pokusom koncipuje ako samostatné trestné činy, teda prípravu alebo pokus povyšuje na dokonaný trestný čin. Zo znenia skutkovej podstaty trestného činu výroby a držby prístupového zariadenia, hesla do počítačového systému alebo iných údajov, je preto zrejmé, že ide o také konanie, ktoré má charakter prípravy vo vzťahu k trestným činom podľa ustanovení § 247 až 247c TZ. Ide o prípravu výlučne na páchanie kybernetickej kriminality v užšom slova zmysle (tzv. *cyber dependent* kriminalita vrátane jej najsofistikovanejších foriem ako Crime as a Service). Toto ustanovenie nepokrýva prípravu na rôzne formy podvodov vo forme *scamov, deep fake* obsahu a podobne, vrátane výroby platobných prostriedkov a s nimi súvisiacich identifikačných prostriedkov.[933]

Tohto trestného činu sa preto dopúšťa iba ten, kto vyrobí, dovezie, obstará, kúpi, predá, vymení, uvedie do obehu alebo akokoľvek sprístupní zariadenie vrátane počítačového programu vytvorené na oprávnený prístup do počítačového systému alebo jeho časti, alebo počítačové heslo, prístupový kód alebo podobné údaje umožňujúce prístup do počítačového systému alebo jeho časti. Je však potrebné dodať aj to, že v praxi bude v rámci dokazovania v trestnom konaní veľmi obtiažne preukázanie úmyslu vo vzťahu k spáchaniu niektorého z uvedených trestných činov.

Argumentom *a contrario* možno dospieť k výkladu, že ak by napríklad zamestnanec vytvoril malvér za účelom vykonania penetračného testovania odolnosti bezpečnostného systému vo firme, v ktorej pôsobí, nebude trestne zodpovedný, pretože chýba fakultatívny znak subjektívnej stránky – cieľ vyjadrený zákonnou formuláciou „v úmysle spáchať trestný čin neoprávneného prístupu do počítačového systému podľa § 247 TZ, ...“ Teda na otázku, v akom okamihu sa softvér stáva malvérom, možno odpovedať tak, že v momente, kedy osoba pojme úmysel použiť ho ako prostriedok na spáchanie niektorého z vyššie uvedených trestných činov. Všimnime si, že zákonodarca v rozpore s čl. 6 Budapeštianskeho dohovoru

[933] K tomu porovnaj výklad k § 219 ods. 4 TZ.

opomenul kriminalizovať aj držbu uvedených počítačových programov, hesiel, prístupových kódov s úmyslom použiť ich na spáchanie niektorého z predmetných trestných činov. Odlišný prístup bol zvolený v čl. 7 smernice 2013/40/EÚ, ktorý explicitne držbu neustanovuje ako jednu z foriem objektívnej stránky, hoci by sa dalo uvažovať o tom, že ju do výpočtu pojala v rámci dikcie „obstarávanie na použitie". Napriek tomu sa však domnievame, že s ohľadom na princíp *nullum crimen sine lege scripta* by bolo vhodné do znenia trestného činu v zmysle ustanovenia § 247d TZ doplniť trestnosť aj za prechovávanie (*possession*) takýchto zariadení, resp. programov.[934]

Ďalšia otázka vyvstávajúca v súvislosti s aplikáciou tejto skutkovej podstaty v aplikačnej praxi sa týka charakteru zariadení, ktorých výroba, dovoz, kúpa, obstaranie, predaj, výmena, uvedenie do obehu či akékoľvek sprístupnenie sa má postihovať. Ak by sme prijali záver, že má ísť výlučne o zariadenia určené na páchanie trestnej činnosti, obrali by sme sa tým o možnosť postihovať výrobu, dovoz, kúpu, obstaranie, predaj, výmenu, uvedenie do obehu či akékoľvek sprístupnenie zariadení, ktoré umožňujú dvojaký účel – legálny aj protiprávny a navyše by sa toto ustanovenie stalo prakticky neaplikovateľným, resp. aplikovateľným iba v ojedinelých prípadoch. Na druhej strane, výklad, že by mohlo ísť aj o zariadenia, ktoré sú verejne dostupné a legálne distribuované by sa mohol zdať príliš extenzívny.[935] Na základe vyššie uvedeného sa domnievame, že by preto malo ísť o zariadenia, ktoré sú na základe objektívnych znakov uspôsobené predovšetkým za účelom spáchania niektorého z uvedených trestných činov, čo je však otázka, ktorú bude v rámci trestného konania potrebné ustáliť znaleckým skúmaním.

Subjektom môže byť ktorákoľvek trestne zodpovedná osoba, a to nielen fyzická osoba, ale s poukazom na ustanovenie § 3 ZoTZPO aj právnická osoba, a to vo všetkých ustanoveniach § 247d TZ.

Subjektívna stránka vyžaduje vo všetkých odsekoch § 247d TZ úmyselné zavinenie, pričom k subjektívnej stránke pristupuje ako jej fakultatívny znak motív v podobe úmyslu spáchať trestný čin neoprávneného prístupu do počítačového systému podľa § 247a TZ, neoprávneného zásahu do počítačového systému podľa § 247a TZ, neoprávneného zásahu do

[934] ZÁHORA, J.: Aktuálne trendy v postihu počítačovej kriminality v Slovenskej republike. In Justičná revue. 2016, č. 3, s. 323 – 340.
[935] K tomu pozri čl. 6 bod 73 Dôvodovej správy k Budapeštianskemu dohovoru. Dostupné na: LINK

počítačového údaja podľa § 247b TZ alebo neoprávneného zachytávania počítačových údajov podľa § 247c TZ.

12.4.4 Súvisiace počítačové trestné činy

12.4.4.1Nátlakové a podvodné počítačové trestné činy

Do tejto skupiny trestných činov sme zaradili trestné činy proti majetku a trestné činy proti slobodám, najmä v rozhodovaní o majetkových a ekonomických otázkach.

PRÍKLAD
Uvedené trestné činy spája spoločný objekt, ktorým je ochrana pred nátlakovými a podvodnými praktikami, ktoré sú trestné aj v materiálnom svete, avšak ich virtuálny ekvivalent predstavuje rýchlejšie, priame konanie, ktoré je dostupné širokému okruhu osôb na diaľku, a to vrátane cezhraničného prvku. Prístupnosť, jednoduchosť až priamočiarosť uvedených postupov má za následok širokoplošné páchanie tejto trestnej činnosti tzv. „kampaňovým" spôsobom čo rezultuje do veľkého počtu obetí, resp. poškodených, často vo viacerých krajinách súčasne. Uvedené nátlakové a podvodné počítačové trestné činy sú spravidla determinované získaním majetkového prospechu.

Vydieranie (§189TZ)[936] a Nebezpečné vyhrážanie (§360 TZ)[937]

Objektom trestného činu je ochrana osobnej slobody človeka v zmysle jeho slobodného rozhodovania.

Objektívna stránka vyžaduje konanie páchateľa, ktorý iného násilím, hrozbou násilia alebo hrozbou inej ťažkej ujmy núti, aby niečo konal, opomenul (§ 122 ods. 1 TZ) alebo trpel. Čin je dokonaný násilným konaním, alebo hrozbou násilného konania a nevyžaduje sa, aby páchateľ dosiahol to, čo sledoval.[938] Cieľ páchateľa však musí byť adresovaný poškodenému a ten ho musí vnímať. Vo vzťahu k počítačovej kriminalite pôjde najmä o prípady vydierania elektronickými prostriedkami (maily, textové aplikácie, SMS) v prípade zašifrovania dôležitých dát a prístupov prostredníctvom ransomvéru, ktorých odšifrovanie je podmienené úhradou výkupného prostredníctvom virtuálnych mien.[939] Ransomvér je typ škodlivého softvéru, ktorý zločinci vyvíjajú a/alebo používajú na zamedzenie prístupu k údajom, systémom alebo sieťam a požadujú zaň výkupné. Medzi bežné metódy útoku patrí šifrovanie údajov, exfiltrácia údajov a narušenie prevádzky obete. Útoky často zahŕňajú viac ako jednu

[936] Ustanovenie § 189 TZ:
„(1) Kto iného násilím, hrozbou násilia alebo hrozbou inej ťažkej ujmy núti, aby niečo konal, opomenul alebo trpel, potrestá sa odňatím slobody na dva roky až šesť rokov.
(2) Odňatím slobody na štyri roky až desať rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) závažnejším spôsobom konania,
b) na chránenej osobe,
c) z osobitného motívu,
d) a spôsobí ním väčšiu škodu, alebo
e) spoločným konaním najmenej dvoch osôb.
(3) Odňatím slobody na desať rokov až dvadsať rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) a spôsobí ním ťažkú ujmu na zdraví alebo smrť, alebo
b) a spôsobí ním značnú škodu.
(4) Odňatím slobody na dvadsať rokov až dvadsaťpäť rokov alebo trestom odňatia slobody na doživotie sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) a spôsobí ním ťažkú ujmu na zdraví viacerým osobám alebo smrť viacerých osôb,
b) a spôsobí ním škodu veľkého rozsahu, alebo
c) ako člen nebezpečného zoskupenia."
[937] Ustanovenie § 360 TZ:
„(1) Kto sa inému vyhráža smrťou, ťažkou ujmou na zdraví alebo inou ťažkou ujmou takým spôsobom, že to môže vzbudiť dôvodnú obavu, potrestá sa odňatím slobody až na jeden rok.
(2) Odňatím slobody na šesť mesiacov až tri roky sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) závažnejším spôsobom konania,
b) na chránenej osobe,
c) preto, aby inému zmaril alebo sťažil uplatnenie jeho základných práv a slobôd,
d) z osobitného motívu, alebo
e) verejne."
[938] K tomu pozri napr. R 60/2003.
[939] ČENTÉŠ, J.; RAMPÁŠEK, M. Ransomvér a úhrada výkupného v kontexte trestného práva. Časopis pro právní vědu a praxi. roč. 33 (2025), č. 3, s. 555 – 578. ISSN: 1210-9126 LINK

metódu a môžu zahŕňať hrozbu zverejnenia údajov obete.[940] Pribúda čoraz viac prípadov, kde za ransomvérovým útokom je primárny dôvod neautorizovaný prenos dát mimo napadnutú entitu. V týchto prípadoch je požiadavka na výkupné často úplne nepodstatná. Takéto využívanie je typické pre štáty resp. skupinami sponzorovaným štátmi, proxy subjektmi konajúcimi v mene štátu (napr. zločineckými skupinami zameranými na špionáž, násilie atď.)[941] [942]

Objektívnu stránku trestného činu vydierania taktiež môžu napĺňať i zakázané praktiky podľa čl. 5 ods. 1 písm. a) a b) aktu o umelej inteligencii[943] - využívanie podprahových techník mimo vedomia osoby alebo účelovo manipulatívne alebo klamlivé techniky s cieľom podstatne narušiť správanie osoby alebo skupiny osôb tým, že sa citeľne oslabí ich schopnosť prijať informované rozhodnutie a využívanie zraniteľnosti osôb z dôvodu ich veku, zdravotného postihnutia alebo osobitnej sociálnej alebo ekonomickej situácie.

Útočníci sa zameriavajú na veľké podnikateľské subjekty alebo vysokopostavené subjekty, o ktorých si myslia, že je pravdepodobnejšie, že zaplatia výkupné, aby obnovili predmet činnosti *(tzv. business continuity*).[944]

Taktiež sú predmetom vydierania prejavy osobnej a intímnej povahy, ako fotky, textové správy, videá, ku ktorým sa páchateľ dostal neoprávnene iným trestným činom a ich nezverejnenie podmieňuje určitým spôsobom, alebo zaplatením určitej sumy, alebo iným konaním, ktoré má rovnako prvky kyberšikany. Vždy pritom však musí ísť o nedovolené konanie.

Taktiež sú týmto trestným činom naplnené rôzne iné formy kyberšikany ako zastrašovania, ponižovania prostredníctvom e-mailov, chatov, sociálnych sietí, portálov,

---

[940] Financial Action Task Force (FATF) Report: Countering Ransomware Financing. Marec 2023 dostupné na: LINK

[941] CONOLLY, L. Y.; WALL, D. S.; LANG, M.; ODDSON, B. An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability, Journal of Cybersecurity, Volume 6, Issue 1, 2020, dostupné na: LINK In: ČENTÉŠ, J.; RAMPÁŠEK, M. Ransomvér a úhrada výkupného v kontexte trestného práva. Časopis pro právní vědu a praxi. roč. 33 (2025), č. 3, s. 555 – 578. ISSN: 1210-9126. Dostupné na: LINK

[942] Zo štatistík vyplýva, že v prvom polroku 2024 bolo v činnosti 73 ransomvérových skupín v porovnaní so 46 skupinami v prvom polroku 2023, čo predstavuje 56-percentný nárast počtu ransomvérových skupín Searchlight Cyber: Ransomware in H1 2024: Trends from the Dark web. s. 4 a 7. Dostupné na: LINK In: In: ČENTÉŠ, J.; RAMPÁŠEK, M. Ransomvér a úhrada výkupného v kontexte trestného práva. Časopis pro právní vědu a praxi. roč. 33 (2025), č. 3, s. 555 – 578. ISSN: 1210-9126. Dostupné na: LINK

[943] K tomu pozri bližšie výklad k trestnému činu úžery.

[944] ČENTÉŠ, J.; RAMPÁŠEK, M. Ransomvér a úhrada výkupného v kontexte trestného práva. Časopis pro právní vědu a praxi. roč. 33 (2025), č. 3, s. 556. ISSN: 1210-9126. Dostupné na: LINK

blogov, pokiaľ osoba žiada nejaké protiplnenie výmenou za to, aby prestala. Pokiaľ páchateľ svojim konaním určitú konkrétnu osobu zastrašuje smrťou, ťažkou ujmou na zdraví alebo inou ťažkou ujmou takým spôsobom, že to môže vzbudiť dôvodnú obavu, a v jeho konaní absentuje protiplnenie pôjde o trestný čin nebezpečného vyhrážania podľa § 360 TZ.[945] Tento typický rys nebezpečného vyhrážania podľa § 360 TZ vo forme kyberšikany zaraďuje okruh takto spáchaných skutkov viac k súvisiacim počítačovým trestným činom a preto je tento trestný čin i súčasťou počítačových trestných činov súvisiacich s obsahom,[946] kedy je primárnou motiváciou šírenie nenávisti a vyhrážania vo verejnom priestore, v diskusiách. Šírenie nenávisti a vyhrážanie sa smrťou, ťažkou ujmou, alebo inou ťažkou ujmou smeruje spravidla voči osobám, ktoré sú buď verejné známe, alebo páchateľ sa snaží zastrašovať osoby pre ich prezentovaný názor a osobne tieto subjekty ani poznať nemusí. Rozlišovanie týchto rôznych aspektov nebezpečného vyhrážania má význam vo vzťahu k mimo trestným aspektom a rizikám, ktoré súvisia s poskytovaním služieb digitálnych platforiem, majúcich svoj pôvod najmä v európskych predpisoch. Subjektívna stránka vyžaduje úmyselné zavinenie (§ 15 TZ). Subjekt je všeobecný, teda môže ním byť ktorákoľvek fyzická osoba. Trestný čin vydierania podľa § 189 TZ je vo vzťahu špeciality aj k trestným činom hrubého nátlaku podľa § 190 a § 191 TZ, nátlaku podľa § 192 TZ a teroru podľa § 313 TZ. Rovnako je vylúčený súbeh trestného činu vydierania a trestného činu podvodu.[947]

[945] K tomu pozri výklad k § 360 TZ.
[946] K tomu pozri výklad k § 360 TZ.
[947] K tomu pozri napr. R 19/2015.

Hrubý nátlak (§ 190)[948]

Objektom trestného činu je slobodného rozhodovanie osoby. Objektívna stránka spočíva v konaní páchateľa, ktorý iného násilím, hrozbou násilia alebo hrozbou inej ťažkej ujmy núti (prostriedok nátlaku na vôľu poškodeného), poskytnúť plnenie majetkovej alebo nemajetkovej povahy pre seba alebo pre tretiu osobu za služby vlastné alebo služby tretej osoby, ktoré mu za takéto plnenie proti jeho vôli vnucuje, a to aj vtedy, ak také služby predstiera. Vo vzťahu ku kybernetickej kriminalite ide o ustanovenie, ktoré postihuje konanie spočívajúce napr. v konaní páchateľa, ktorý podmieňuje odšifrovanie obsahu resp. dát využívaním vlastných IT služieb, resp. postup „etického" hackera alebo penetračného testera, ktorý takýmto spôsobom „nájde" kritickú zraniteľnosť v systéme a na jeho odstránenie ponúkne svoje služby.

Čin je dokonaný použitím násilia alebo hrozieb. Nevyžaduje sa, aby páchateľ svoj zámer dosiahol. Pri hrubom nátlaku (na rozdiel od lúpeže) stačí hrozba násilím, ktorá nemusí byť bezprostredná (napr. listom, telefonicky a pod.). Hrozba nemusí smerovať priamo proti napadnutému, môže sa týkať jeho detí, blízkej osoby, ale aj majetku.[949] Hrozba inej ťažkej ujmy môže spočívať v hrozbe spôsobenia majetkovej ujmy, vážnej ujmy na cti a dobrej povesti, môže smerovať k rozvratu manželstva, k začatiu trestného stíhania, a to bez ohľadu na to, či poškodený skutočne spáchal trestný čin a pod.[950] Službami (vnucovanými) možno rozumieť napríklad poskytovanie ochrany za odplatu.

Hmotným predmetom útoku je človek.

---

[948] Ustanovenie § 190 TZ:
„(1) Kto iného násilím, hrozbou násilia alebo hrozbou inej ťažkej ujmy núti poskytnúť plnenie majetkovej alebo nemajetkovej povahy pre seba alebo pre tretiu osobu za služby vlastné alebo služby tretej osoby, ktoré mu za takéto plnenie proti jeho vôli vnucuje, a to aj vtedy, ak také služby predstiera, potrestá sa odňatím slobody na štyri roky až desať rokov.
(2) Odňatím slobody na sedem rokov až pätnásť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) závažnejším spôsobom konania,
b) na chránenej osobe,
c) z osobitného motívu,
d) na žene vo výkone väzby alebo vo výkone trestu odňatia slobody, alebo
e) spoločným konaním najmenej dvoch osôb.
(3) Odňatím slobody na pätnásť rokov až dvadsať rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 a
a) spôsobí ním ťažkú ujmu na zdraví, alebo
b) bezprostredne ním ohrozí život dieťaťa.
(4) Odňatím slobody na dvadsať rokov až dvadsaťpäť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) a spôsobí ním smrť, alebo
b) za krízovej situácie."
[949] K tomu pozri napr. R 1/1980.
[950] K tomu pozri napr. R 27/1982.

Subjektívna stránka vyžaduje úmyselné zavinenie (§ 15 TZ).

Subjekt (páchateľ) je všeobecný, teda môže ním byť ktorákoľvek trestne zodpovedná fyzická osoba.

Trestný čin hrubého nátlaku podľa § 190 TZ je vo vzťahu špeciality napríklad k trestným činom vydierania podľa § 189 TZ, ale aj lúpeže podľa § 190 TZ a brania rukojemníka podľa § 185 TZ. Skutková podstata trestného činu hrubého nátlaku podľa § 190 TZ je privilegovaná skutková podstata k trestnému činu vydierania podľa § 189 TZ.

Nebezpečné prenasledovanie (§360a TZ)[951] a Nebezpečné elektronické obťažovanie (§360b)[952]

Objektom tohto trestného činu je ochrana súkromia a medziľudských vzťahov a riadneho občianskeho spolunažívania.

Objektívna stránka spočíva v zameraní sa na konkrétnu osobu (*stalking)*, ktorú páchateľ prenasleduje, vyhráža sa, obťažuje ju alebo jej blízke osoby, a tým vo svojej obeti

[951] Ustanovenie § 360a TZ:
„(1) Kto iného prenasleduje takým spôsobom, že to môže vzbudiť dôvodnú obavu o jeho život alebo zdravie, život alebo zdravie jemu blízkej osoby alebo podstatným spôsobom zhoršiť kvalitu jeho života, tým, že
a) sa vyhráža ublížením na zdraví alebo inou ujmou jemu alebo jemu blízkej osobe,
b) vyhľadáva jeho osobnú blízkosť alebo ho sleduje
c) ho kontaktuje prostredníctvom tretej osoby alebo elektronickej komunikačnej služby, písomne alebo inak proti jeho vôli,
d) zneužije jeho osobné údaje na účel získania osobného alebo iného kontaktu, alebo
e) ho inak obmedzuje v jeho obvyklom spôsobe života,
potrestá sa odňatím slobody až na dva roky.
(2) Odňatím slobody na šesť mesiacov až tri roky sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) na chránenej osobe,
b) závažnejším spôsobom konania,
c) z osobitného motívu, alebo
d) verejne."
[952] Ustanovenie §360b TZ:
„(1) Kto úmyselne prostredníctvom elektronickej komunikačnej služby, počítačového systému alebo počítačovej siete podstatným spôsobom zhorší kvalitu života iného tým, že
a) ho dlhodobo ponižuje, zastrašuje, neoprávnene koná v jeho mene alebo dlhodobo inak obťažuje, alebo
b) neoprávnene zverejní alebo sprístupní tretej osobe obrazový, zvukový alebo obrazovo-zvukový záznam jeho prejavu osobnej povahy získaný s jeho súhlasom, spôsobilý značnou mierou ohroziť jeho vážnosť alebo privodiť mu inú vážnu ujmu na právach,
potrestá sa odňatím slobody až na tri roky.
(2) Odňatím slobody na jeden rok až štyri roky sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) na chránenej osobe, alebo
b) z osobitného motívu.
(3) Odňatím slobody na dva roky až šesť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) a spôsobí ním značnú škodu,
b) s úmyslom získať pre seba alebo iného značný prospech, alebo
c) hoci bol za taký čin v predchádzajúcich dvadsiatich štyroch mesiacoch odsúdený."

vyvoláva dôvodnú obavu o zdravie alebo zdravie jemu blízkej osoby alebo podstatným spôsobom zhoršiť kvalitu jeho života, tým, že:

1. sa vyhráža ublížením na zdraví alebo inou ujmou jemu alebo jemu blízkej osobe,
2. vyhľadáva jeho osobnú blízkosť alebo ho sleduje,
3. ho kontaktuje prostredníctvom tretej osoby alebo elektronickej komunikačnej služby, písomne alebo inak proti jeho vôli,
4. zneužije jeho osobné údaje na účel získania osobného alebo iného kontaktu, alebo
5. ho inak obmedzuje v jeho obvyklom spôsobe života,

Príkladom je neustále vypisovanie na sociálnej sieti, kde sa páchateľ vyhráža obeti, že jej ublíži alebo jej blízkej osobe, či už fyzicky alebo psychicky, písanie častých správ či emailov, vyhľadávanie osobnej blízkosti, vyhrážaním sa, šírením malformácií a pod.

Prenasledovaním sa rozumie súhrn viacerých čiastkových konaní (aj rôznorodých), ktoré napĺňajú definíciu podľa písmen a) až e). Kvalita života predstavuje obvyklý súhrn vzťahov, spôsobov a trávenia času obete pred začatím páchania tohto trestného činu samostatne ale i v spojení s inými osobami v rodine, zamestnaní, škole a pod. Vyhrážanie sa ublížením na zdraví alebo inou ujmou spočíva v konaní, kedy páchateľ verbálne, alebo neverbálne útočí na obeť, pričom z jej správania, obsahu, zo spôsobu vyslovenia, ako aj z ďalších súvisiacich okolností vyplýva skutočnosť, že je myslená vážne. Vyhľadávanie osobnej blízkosti alebo jeho sledovanie predpokladá úmyselné konanie páchateľa v jeho prítomnosti na miestach, ktoré obvykle navštevuje obeť (obydlie, škola, pracovisko resp. pracovné miesto ak sa jedná o väčšieho zamestnávateľa, miesta voľnočasových aktivít/krúžkov, obchody, kaviarne, reštaurácie a pod.). Nesmie ísť o náhodne stretnutie. Posúdenie trestnosti tohto konania je v praxi obtiažne ak sa jedná o osoby, ktoré sa na určitých miestach zdržiavajú spoločne z iných dôvodov (kolegovia, spolužiaci a pod.). Kontaktovanie prostredníctvom tretej osoby alebo komunikačnej služby, písomne alebo inak proti jeho vôli sa chápe ako spôsob obťažovania, ktorý je pre poškodeného nepríjemný, a proti jeho vôli, pričom poškodený by mal jednoznačne prejaviť nesúhlas alebo odpor proti tomuto spôsobu kontaktovania. Zneužitím osobných údajov na účel získania osobného alebo iného kontaktu sa myslí konanie páchateľa, ktorý použije osobné údaje poškodeného bez jeho súhlasu, pričom jeho cieľom je osobný kontakt, telefonický, textový (SMS, chat) alebo mailový kontakt s poškodeným. Iné obmedzovanie v obvyklom spôsobe života predstavuje obmedzovanie obete, ktoré je spôsobilé vyvolať dôvodnú obavu u poškodeného najmä v jeho

osobnom alebo pracovnom živote (napr. drobné poškodenia alebo „straty" vecí, zanechávanie dôkazov o svojej prítomnosti, čakaní a pod.).

Subjekt tohto trestného činu je všeobecný.

Pokiaľ intenzita útokov a vyhrážok u obete nespôsobí dôvodnú obavu o jej alebo jej blízkej osobe život, zdravie obete, pôjde spravidla o trestný čin nebezpečného elektronického obťažovania podľa § 360b TZ, ktorý sa označuje pojmom tzv. kyberšikana. Pojem kyberšikany je upravený i v smernici Ministerstva školstva, vedy, výskumu a športu č. 36/2018. V zmysle spomenutej smernice sa za kyberšikanovanie považuje priama forma šikanovania, pri ktorej ide o zneužitie informačno-komunikačných technológií (najmä telefónu, tabletu, internetu a sociálnych sietí) na úmyselné ohrozenie, ublíženie alebo zastrašovanie, pričom sa často vyskytuje v spojení s inými formami šikanovania. Pri šikanovaní ide o úmyselnú snahu získať prevahu nad jednotlivcom alebo viacerými jedincami prostredníctvom ubližovania, vyhrážania, výsmechu alebo zastrašovania. V zásade ide z psychologického a sociologického hľadiska o zneužívanie dominancie agresora, s prejavmi vyvolávania strachu, stresu alebo bolesti, s použitím prostriedkov elektronickej komunikácie.[953]

Objektom trestného činu je osobný život obete, jej právo na súkromie a prejavy osobnej povahy.

Objektívna stránka spočíva v konaní páchateľa, ktorý prostredníctvom elektronickej komunikačnej služby, počítačového systému alebo počítačovej siete podstatným spôsobom zhorší kvalitu života iného tým, že

- obeť dlhodobo ponižuje, zastrašuje, neoprávnene koná v jeho mene alebo inak obťažuje, alebo
- neoprávnene zverejní alebo sprístupní tretej osobe obrazový, zvukový alebo obrazovo-zvukový záznam obete s prejavom osobnej povahy získaný s jej súhlasom, spôsobilý značnou mierou ohroziť jeho vážnosť alebo privodiť mu inú vážnu ujmu na právach. Následkom uvedeného konania je podstatné zhoršenie kvality života spôsobom uvedeným v písmen a) a b).

Objektívna stránka vymedzená v písmene a) je pojem akékoľvek obťažovanie prostredníctvom elektronickej služby, alebo počítačového systému, ktoré je obeti nepríjemné a s ktorým nesúhlasí, pričom musí byť dostatočne intenzívne, aby podstatne

[953] STRÉMY, T.; KURILOVSKÁ, L.; REMETA, R. a kol. Trestný zákon - praktický komentár. Wolters Kluwer, Bratislava, ISBN: 978-80-286-0378-6, 2025 s. 1201.

zhoršilo kvalitu života (neustále prevolávanie aj v nočných hodinách, písanie správ, mailov, chatov, zadávanie osobných alebo kontaktných údajov na rôzne platformy bez súhlasu obete, zverejňovanie správ a informácií o živote obete alebo jej blízkej osoby apod.

Právna úprava vymedzená v písmene b) spočíva v zverejnení alebo sprístupnení záznamu osobnej povahy, ktorý je spôsobilý na ohrozenie vážnosti, či spôsobenia inej vážnej ujmy na právach, napr. záznam intímnej povahy obete, pričom môže ísť aj o verejný prejav, ktorý je realizovaný so súhlasom poškodeného a tento je následne zneužitý a neoprávnene zverejnený alebo sprístupnený tretej osobe.

Subjekt je v prípade tohto trestného činu všeobecný, čiže páchateľom trestného činu môže byť ktorákoľvek trestnej zodpovedná fyzická osoba.

Subjektívna stránka predpokladá zavinenie úmyselné, ktoré je zvýraznené príslušnou zákonnou formuláciou.

Trestný čin nebezpečného elektronického obťažovania podľa §360b ods.1 písm. b) TZ sa líši od trestného činu porušenia dôvernosti ústneho prejavu a iného prejavu osobnej povahy podľa § 377 TZ[954] v tom, že v tomto prípade sa neoprávnene zverejní prejav osobnej povahy získaný so súhlasom obete tohto trestného činu, zatiaľ čo pri trestnom čine porušenia dôvernosti ústneho prejavu a iného prejavu osobnej povahy podľa § 377 TZ bol záznam osobného neverejného prejavu získaný proti vôli osoby a bez jej súhlasu.

Podvod (§221 TZ)[955]

Z pohľadu kategórie súvisiacich počítačových trestných činov ide najmä o rôzne druhy podvodov spočívajúcich v *scamming kampaniach* (podvodné získanie finančných

[954] Pozri výklad k § 377 TZ.

[955] Ustanovenie § 221 TZ:
„(1) Kto na škodu cudzieho majetku seba alebo iného obohatí tým, že uvedie niekoho do omylu alebo využije niečí omyl, a spôsobí tak na cudzom majetku malú škodu, potrestá sa odňatím slobody až na dva roky
(2) Odňatím slobody až na štyri roky sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 a spôsobí ním väčšiu škodu.
(3) Odňatím slobody na dva roky až osem rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) a spôsobí ním značnú škodu,
b) z osobitného motívu,
c) závažnejším spôsobom konania, alebo
d) na chránenej osobe.
(4) Odňatím slobody na tri roky až desať rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) a spôsobí ním škodu veľkého rozsahu,
b) ako člen nebezpečného zoskupenia, alebo
c) za krízovej situácie."

prostriedkov, osobných údajov prostredníctvom rôznych legiend ako sú ponuky na sobáš, vypršaných Microsoft licencií, predstieraných zástupcov štátnych orgánov ako sú Polícia SR alebo Národna banka Slovenska, Slovenská pošta atď.), phishingových správ, ktoré predstierajú legitímnu službu, najčastejšie bankovú, e-shop či poštovú, s cieľom vylákať prístupové údaje k účtu, alebo platobnej karte alebo *deepfake* podvodov, ktoré najčastejšie realizované s použitím umelej inteligencie v spojení s presvedčivou grafickou úpravou mailu a ktoré predstierajú priamy pokyn nadriadeného o zaslanie určitej vysokej finančnej čiastky (tzv. CEO podvody) alebo ide o predstieranie kontaktovania príbuzným (legenda vnuk, lekár atď.). Taktiež sem spadá i nasadenie sledovacích aplikácií a programov „vírusového typu", ktoré zachytávajú stlačené klávesy a tým získavajú prístup k heslám do systémov, aplikácií *(tzv. key loggerov)* za účelom predstierania autorizovaného vstupu a zadania platieb.

Objektívnu stránku podvodu taktiež môžu naplniť i zakázané praktiky podľa čl. 5 ods.1 písm. a) a b) aktu o umelej inteligencii[956] - využívanie podprahových techník mimo vedomia osoby alebo účelovo manipulatívne alebo klamlivé techniky s cieľom podstatne narušiť správanie osoby alebo skupiny osôb tým, že sa citeľne oslabí ich schopnosť prijať informované rozhodnutie a využívanie zraniteľnosti osôb z dôvodu ich veku, zdravotného postihnutia alebo osobitnej sociálnej alebo ekonomickej situácie.

Objektom tohto trestného činu je ochrana vlastníctva a zásady právnej istoty, že zmluvy a záväzky sa majú plniť *(pacta sunt servanda).*

Objektívna stránka tohto trestného činu spočíva v spôsobení škody a vo využití omylu alebo uvedenia do omylu osoby, pričom môže ísť aj o tretiu osobu, odlišnú od poškodeného. Pre naplnenie trestnosti trestného činu podvodu vo vzťahu k právnickej osobe sa vyžaduje, aby bolo preukázané, že právnická osoba prostredníctvom osôb podľa § 4 ods. 1, ods. 2 ZoTZPO konala v čase uzatvorenia záväzku s tým, že záväzok v dohodnutej dobe nesplní, alebo ho nebude môcť splniť a že veriteľa uvádza do omylu, aby sa obohatil na jeho škodu. Cudzím majetkom sa rozumejú veci, pohľadávky, ako aj iné majetkové práva a hodnoty, ktoré vlastnícky nepatria páchateľovi, alebo nepatria výlučne len jemu.

Pojem uvedenia niekoho do omylu znamená aktívne vedomé predstieranie faktov alebo skutočnosti, ktoré sú rozporné s realitou. Môže tak konať nielen vo vzťahu priamo k

[956] K tomu pozri výklad k trestnému činu úžery.

poškodenému, ale aj k iným osobám. Pojem omyl je nezhoda predstavy človeka so skutočným stavom.

Miestom spáchania trestného činu podvodu je nielen miesto, kde dochádza k napĺňaniu tej časti objektívnej stránky skutkovej podstaty tohto trestného činu, ktorou páchateľ uvádza niekoho do omylu alebo niečí omyl využíva, ale aj miesto, kde v dôsledku uvedeného konania vznikla škoda a tiež miesto, kde sa páchateľ obohatil. Ak ide o pokračovací trestný čin podvodu, ktorého objektívna stránka sa napĺňala vykonaním viacerých čiastkových útokov postupne na viacerých miestach, je miestom spáchania činu každé toto miesto.[957]

Pojem obohatenie možno definovať ako neoprávnené rozšírenie majetku alebo ušetrenie nákladov, ktoré by za iných okolností museli byť vynaložené.

Pojem využitia niečieho omylu je možné definovať tak, že páchateľ svojím konaním omyl nevyvolal, uvedený omyl využije vo svoj prospech. Vzhľadom na úmyselné zavinenie, páchateľ si musí byť vedomý existencie omylu. Právnickú osobu možno uviesť do omylu len uvedením do omylu fyzickej osoby, ktorá je oprávnená tvoriť vôľu právnickej osoby a prejavovať ju navonok, teda rozhoduje a koná v jej mene (môže ísť aj o osobu, ktorá je členom štatutárneho alebo iného orgánu právnickej osoby). Rovnako platí, že využiť omyl právnickej osoby možno len využitím omylu vyššie charakterizovanej fyzickej osoby.[958] Spôsobiť škodu na cudzom majetku možno pri trestnom čine podvodu podľa § 221 TZ aj uvedením niekoho do omylu alebo využitím niečieho omylu, ak taká (mýliaca sa) fyzická osoba nie je poškodeným ani nereprezentuje poškodenú právnickú osobu.[959] Prijatie peňažnej čiastky z majetku iného v úmysle ponechať si ju, aj keď páchateľ vie, že mu táto čiastka nepatrí a že mu bola zaslaná omylom, je konaním, ktoré napĺňa znaky trestného činu podvodu, t. j. obohatením sa ku škode iného využitím omylu iného. Naproti tomu zatajenie veci z majetku iného tým, že si páchateľ privlastní vec, ktorá sa dostala do jeho moci omylom, predpokladá, že v dobe, kedy sa vec dostáva do jeho moci, páchateľ o tomto omyle nevie a až potom dodatočne si uvedomí, že mu vec nepatrí.[960]

Vo vzťahu k trestnému činu podvodu aplikačná prax rozvinula tzv. teóriu primeranej miery opatrnosti poškodeného, v rámci ktorej je, pri naplnení znakov skutkovej podstaty

[957] K tomu pozri napr. R 101/2001.
[958] K tomu pozri napr. NS SR sp. zn. 2 Tdo 38/2014.
[959] K tomu pozri napr. NS SR sp. zn. 2 Tdo 38/2014.
[960] K tomu pozri napr. R 17/1980.

podvodu potrebné skúmať, či vôbec konanie páchateľa je spôsobilé zapríčiniť následok predpokladaný Trestným zákonom, ak by poškodený sám vyvinul aspoň základnú opatrnosť a preveril si elementárne skutočnosti páchateľovho podvodného konania, z ktorého by mal získať podozrenie, že nejde o legitímny záujem osoby konať naznačeným spôsobom[961] Primeranú mieru opatrnosti je možné aplikovať i vo vzťahu k ostatným formám podvodu, pričom najčastejšie sa tento dôvod aplikuje práve pri rôznych scammimgových kapaniach, kedy orgány činné v trestnom konaní tento argument dovodzujú z konania, ktoré ak by bolo racionálne, nikdy by ku škode nedošlo.

Subjekt tohto trestného činu je všeobecný. Môže ním byť ktorákoľvek trestne zodpovedná fyzická alebo právnická osoba. Pravidlo *ultima ratio* možno uplatniť jedine prostredníctvom materiálneho korektívu v rozsahu § 10 ods. 2 TZ, teda v zmysle platnej a účinnej zákonnej úpravy, len pri prečinoch.[962]

Subjektívna stránka tohto trestného činu vyžaduje úmyselné zavinenie.

Kapitálový podvod (§ 224 TZ)[963]

V praxi ide najmä o rôzne formy tzv. investičných podvodov, pyramídových hier, Ponziho schém[964] budiacich dojem multi - level marketingových (MLM) aktivít,[965] ktoré sú v zásade legálnou pyramídovou obchodnou stratégiou. Taktiež ide o rôzne formy

[961] K tomu pozri napr. R NS SR I2 Tdo V 21/2013.
[962] K tomu pozri napr. R 96/2014, NSSR 3 Tdo 43/2017.
[963] Ustanovenie §224 TZ:
„(1) Kto v súvislosti s ponukou, predajom alebo rozširovaním cenných papierov alebo iných listín, ktoré sľubujú účasť na majetkových výnosoch podniku, alebo kto v súvislosti s ponukou zvýšiť výnosy takého investovania v prospektoch alebo v iných propagačných materiáloch alebo prehľadoch týkajúcich sa majetkových pomerov alebo výnosov podniku vo vzťahu k väčšiemu počtu osôb uvádza nepravdivé údaje alebo nereálne údaje o výnosoch investovania alebo o majetkových pomeroch podniku, do ktorého sa má investovať, alebo kto nevýhody takého investovania zamlčí, potrestá sa odňatím slobody na šesť mesiacov až tri roky.
(2) Odňatím slobody na dva roky až osem rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) a spôsobí ním väčšiu škodu,
b) z osobitného motívu, alebo
c) závažnejším spôsobom konania.
(3) Odňatím slobody na tri roky až osem rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 a spôsobí ním značnú škodu.
(4) Odňatím slobody na tri roky až desať rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) a spôsobí ním škodu veľkého rozsahu,
b) ako člen nebezpečného zoskupenia, alebo
c) za krízovej situácie."
[964] Pomenovaných po Carlovi Ponzim, ktorý v rokoch 1919-1920 získal od investorov (ako prevádzkovateľ) značné finančné sumy (cca 15. mil. USD) s cieľom ich zhodnotenia finančnými špekulatívnymi operáciami. Namiesto toho vyplácal výnosy z vkladov neskorších investorov a špekulácie na trhu nevykonával.
[965] Napr. predaj výrobkov určitej kozmetickej značky alebo rôzne investičné či marketingové platformy.

kontaktovania (emailom, telefonicky) za účelom vylákania peňažných prostriedkov ako údajnej veľmi výhodnej investície napr. do virtuálnych mien, výstavby letovísk v Karibiku, NFT tokenov. V ods. 1 je definovaná základná skutková podstata trestného činu kapitálového podvodu podľa § 224 TZ. Taktiež vo vzťahu ku kapitálovému podvodu možno uplatniť výklad o zakázaných praktikách podľa čl. 5 ods.1 písm. a), b) aktu o umelej inteligencii.[966]

Objektom tohto trestného činu je záujem na zodpovednom investovaní do produktov s reálnym výnosom za dodržania akceptovateľného investičného rizika.

Objektívna stránka spočíva v propagácií alebo sľube účasti na výnosoch podniku/obchodnej príležitosti v súvislosti s nakladaním s investičnými produktmi, alebo uvádzanie nepravdivých alebo nereálnych (nadhodnotených) údajov o výnosoch investovania alebo o majetkových pomeroch podniku do ktorého sa má investovať, alebo zamlčanie investičných rizík.

Pre naplnenie trestnosti trestného činu podvodu vo vzťahu k právnickej osobe sa vyžaduje, aby bolo preukázané, že právnická osoba prostredníctvom osôb podľa § 4 ods. 1 ods. 2 ZoTZPO uvádzala nepravdivé alebo nereálne výnosy, alebo zamlčala podstatné riziká investičnej príležitostí.

Subjekt tohto trestného činu je všeobecný. Môže ním byť ktorákoľvek trestne zodpovedná fyzická alebo právnická osoba.

Subjektívna stránka tohto trestného činu vyžaduje úmyselné zavinenie.

[966] K tomu pozri výklad k trestnému činu úžery.

Úžera (§ 235 TZ)[967]

Objektom trestného činu úžery podľa §235 ods. 1, písm. a) a ods. 2 TZ je ochrana možnosti správneho rozhodovania v majetkových záležitostiach i samotný majetok. Dôvodom je neekvivalentný pomer vzájomného plnenia z týchto záväzkov a porušenie etických princípov zo strany páchateľa, ktorý v záujme vlastného obohatenia ťaží z manipulatívnej techniky a neinformovaného rozhodnutia iného. Uvedená existencia samotného nepomeru plnení v neprospech poškodeného tak ako to vyžaduje Trestný zákon v zmysle ustanovenia § 235 ods. 1 TZ je možné podľa nášho názoru subsumovať pod spôsobenie závažnej ujmy podľa čl. 5 ods.1 písm. a), písm. b) aktu o umelej inteligencii, súčasne v prípade skutkovej podstaty trestného činu úžery podľa § 235 ods. 1 TZ ako i zakázanej manipulatívnej praktiky podľa čl. 5 ods. 1 písm. a), písm. b) aktu o umelej inteligencii - využívanie podprahových techník mimo vedomia osoby alebo účelovo manipulatívne alebo klamlivé techniky s cieľom podstatne narušiť správanie osoby alebo skupiny osôb tým, že sa citeľne oslabí ich schopnosť prijať informované rozhodnutie a využívanie zraniteľnosti osôb z dôvodu ich veku, zdravotného postihnutia alebo osobitnej sociálnej alebo ekonomickej situácie.[968] Navyše možno v oboch prípadoch hovoriť o ohrozovanom trestnom čine, ktorý na posúdenie trestnosti nevyžaduje spôsobenie následku.

---

[967] Ustanovenie §235 TZ:
„(1) Kto zneužívajúc niečiu tieseň, neskúsenosť alebo rozumovú slabosť alebo niečie rozrušenie, dá sebe alebo inému poskytnúť alebo sľúbiť plnenie, ktorého hodnota je k hodnote vzájomného plnenia v hrubom nepomere, alebo kto takú pohľadávku uplatní alebo v úmysle uplatniť ju, na seba prevedie, potrestá sa odňatím slobody až na šesť mesiacov až tri roky.
(2) Rovnako ako v odseku 1 sa potrestá, kto poskytne plnenie bez povolenia, v rozpore s vydaným povolením alebo poruší zákonom chránené práva spotrebiteľa a dá sebe alebo inému poskytnúť alebo sľúbiť plnenie, ktorého hodnota je k hodnote vzájomného plnenia v hrubom nepomere alebo kto takú pohľadávku uplatní alebo v úmysle uplatniť ju, na sebe prevedie.
(3) Odňatím slobody na jeden rok až päť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 alebo odseku 2
a) a spôsobí ním väčšiu škodu,
b) na chránenej osobe, alebo
c) z osobitného motívu.
(4) Odňatím slobody na dva roky až osem rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 alebo odseku 2
a) a spôsobí ním značnú škodu, alebo
b) závažnejším spôsobom konania.
(5) Odňatím slobody na tri roky až desať rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 alebo odseku 2
a) a spôsobí ním škodu veľkého rozsahu, alebo
b) ako člen nebezpečného zoskupenia."

[968] DRAŽOVÁ, P.; KORDÍK, M. Trestnoprávny presah vybraných zakázaných praktík podľa Aktu o umelej inteligencii, Bratislavské právnické fórum 2025 / MIHÁLIKOVÁ, M.; ŤAŽKÁ, V. (zost.). Bratislava: Právnická

Prvým druhom zakázaných praktík systémov s umelou inteligenciou je využívanie manipulatívnych praktík podľa čl. 5 ods.1 písm. a) aktu o umelej inteligencii s nasledovnými znakmi:

- ide o podprahovú techniku mimo vedomia osoby,
- (kumulatívne) s motívom prijať neracionálne pudové rozhodnutie, ktoré *a contrario* nie je založené na informovanom rozhodnutí,
- príčinná súvislosť medzi podprahovou technikou mimo vedomia osoby a prijatím neinformovaného rozhodnutia,
- odôvodnený predpoklad spôsobenia značnej ujmy prijatím neinformovaného rozhodnutia.

Pre naplnenie znakov zakázanej praktiky musia byť súčasne splnené všetky štyri podmienky a musí existovať hodnoverná príčinná súvislosť medzi použitými technikami, podstatným narušením správania osoby a značnou ujmou, ktorú uvedené správanie spôsobilo alebo je odôvodnené predpokladať, že spôsobí. Pod značnou ujmou sa rozumie fyzická, psychická, finančná a ekonomická ujma.

Druhou skupinou zakázaných praktík systémov s umelou inteligenciou je využívanie manipulatívnych praktík podľa čl. 5 ods.1, písm. b) aktu o umelej inteligencii s nasledovnými znakmi:

- využitie zraniteľnosti osoby z dôvodu jej veku, zdravotného stavu, ekonomickej alebo sociálnej situácie s cieľom ovplyvniť jej správanie,
- odôvodnený predpoklad spôsobenia značnej ujmy osobe ovplyvnením jej správania.

Na rozdiel od prvej skupiny zakázaných praktík nemusí ísť o podprahové techniky, ktorými sa má ovplyvniť rozhodovanie, ale zneužíva sa zraniteľnosť osoby na ovplyvnenie jej rozhodovania. Zmyslom zákazu uvedených praktík je ochrana pred oslabovaním a narúšaním samostatnosti rozhodovania a slobodnej voľbe osôb tak, že si poškodení neuvedomujú, že sú zavádzaní alebo hoci s vedomím vlastného zavádzania, nie sú schopní ovládať svoje rozhodnutie alebo takejto technike odolávať. Z uvedeného vyplýva, že tieto techniky zneužívajú vek, zdravotný stav, ekonomickú situáciu, sociálne postavenie a osobnosť poškodeného na dosiahnutie želaného rozhodnutia.

fakulta Univerzity Komenského v Bratislave, 2025. ISBN 978-80-7160-772-4, s. 641-642. Dostupné dňa 06.02.2026 na: LINK

Zákaz takýchto praktík mieri najmä na praktiky, ktoré poškodzujú spotrebiteľov. Netýka sa zákonných postupov v súvislosti s liečbou, duševných chorôb, fyzickej rehabilitácie, ak sú v súlade s platnými lekárskymi predpismi akým je súhlas pacienta alebo ich právnych zástupcov alebo reklama, ktorá je v súlade s platným právom Vo vzťahu k ostatným pojmom, je možné aplikovať výklad vyššie.

Objektívna stránka trestného činu úžery podľa § 235 ods. 1 písm. a) TZ, pod ktorú možno subsumovať uvedenú praktiku spočíva v zneužití niečej tiesne, neskúsenosti, rozumovej slabosti alebo niečieho rozrušenia k tomu, aby páchateľovi alebo inému bolo poskytnuté alebo sľúbené plnenie, ktorého hodnota je v hrubom nepomere.

Tiesňou sa rozumie mimoriadne ťaživá situácia poškodeného (alebo inej osoby, ktorej tieseň pociťuje poškodený ako tieseň vlastnú, vyvolaná určitou i prechodnou naliehavou potrebou, ktorej uspokojenie nie je v možnostiach poškodeného. Spravidla pôjde o hospodárske ťažkosti, splatnosť dlhu, ktorého nesplatenie môže vážne ohroziť spoločenské postavenie poškodeného. Môže ísť taktiež aj o iné ťažkosti, napríklad záujem získať byt na vyriešenie ťaživej rodinnej situácie alebo ťažkosti vyvolané osobnými a spoločenským pomermi poškodeného.

Neskúsenosť spočíva napríklad v nedostatočnej znalosti cien, nákupných možností spravidla v spojení s dôverčivosťou voči páchateľovi. Ide teda predovšetkým o neskúsenosť pri vybavovaní majetkových záležitostí. Neskúsenosť môže byť sprievodným javom nízkeho veku hlavne u neplnoletých.

Rozumová slabosť je neschopnosť poškodeného rozpoznať hodnotu svojho plnenia rozpoznať hodnotu svojho plnenia alebo sľubu k hodnote vzájomného plnenia páchateľa.

Rozrušenie je stav prudkého pohnutia mysle vyvolaný určitou bezprostredne predchádzajúcou udalosťou, ktorá obzvlášť intenzívne zasiahla citovú zložku duševného života poškodeného.

Pokiaľ ide o charakter plnenia, musí mať majetkovú (i keď nie peňažnú) hodnotu, podľa terminológie čl. 5 aktu o umelej inteligencii by práve trestný čin úžery pokrýval závažnú majetkovú ujmu.

Hrubý nepomer je nutné posudzovať z hľadiska súčasných objektívnych výmenných hodnôt oboch plnení. Hodnota vzájomného plnenia sa stanoví podľa rovnakých zásad, ako sa určuje výška škody.

K trestnej zodpovednosti sa vyžaduje, aby medzi zneužitím tiesne, neskúsenosťou, rozumovou slabosťou alebo rozrušením a hrubým nepomerom vzájomného plnenia bola príčinná súvislosť. Pritom jednotlivé uvedené skutočnosti nemusia byť jedinou a rozhodujúcou príčinu pre poskytnutie alebo pre sľub takého plnenia, ale stačí, aby tieto okolnosti k tomu spolupôsobili.

Rozdiel trestného činu úžery oproti trestnému činu podvodu podľa § 221 TZ je v tom, že úžerník neuvádza iného do omylu. Ak využíva niečí omyl je to omyl, ktorý má svoje zvláštne príčiny. Predstava poškodeného o podstate jeho konania pri úžere je správna, ale hodnotenie vzájomných plnení je nesprávne. Poškodený teda poskytuje alebo sľubuje plnenie v určitej tiesni, i keď vie, že hodnota je plnenia je k hodnote vzájomného protiplnenia v hrubom nepomere, alebo v dôsledku neskúsenosti, rozumovej slabosti alebo rozrušenia nie schopný zhodnotiť vzájomný pomer oboch plnení. Pri trestnom čine podvodu koná poškodený pod vplyvom svojho omylu alebo omylu inej osoby vyvolaného alebo využitého páchateľom, bez toho aby konal pod vplyvom tiesne alebo neschopnosti posúdiť dôsledky svojho konania

Zo subjektívnej stránky sa vyžaduje úmyselné zavinenie. Pre prípustnosť trestného stíhania voči osobe, ku ktorej má poškodený právo odoprieť výpoveď podľa § 130 TP, je nutný súhlas poškodeného podľa § 211 TP. Páchateľom tohto trestného činu môže byť ktorákoľvek trestne zodpovedná osoba, fyzická i právnická.

V § 235 ods. 2 TZ je definovaná druhá relevantná základná skutková podstata trestného činu úžery, ktorá je taktiež naplniteľná uvedenou zakázanou praktikou. Toto ustanovenie primárne chráni plnenia a služby, ktoré sú buď úplne, alebo sčasti regulované zákonom alebo spadajú do ochrany spotrebiteľa, v rámci, ktorých môže dôjsť k zneužitiu dominantného postavenia a podmieňovať plnenie prijatím iných služieb alebo hodnôt, ktoré následne môžu byť v hrubom nepomere.

Falšovanie predmetov kultúrnej hodnoty prostredníctvom počítačového systému (249a ods.1, ods. 2 písm. c) TZ)[969]

Objektom trestného činu je záujem na ochrane a riadnom obehu pravých predmetov kultúrnej hodnoty, ktoré sú základom kultúrneho dedičstva ako nadindividuálneho záujmu, ale taktiež slúžia v ekonomickom styku ako uchovávateľ ekonomickej hodnoty a investícia a sekundárne ako súčasť princípu právnej istoty. Z pohľadu kybernetickej kriminality táto skutková podstata chráni autentické a ekonomicky oceniteľné umelecké diela NFT tokenov[970] (jedinečné umelecké elektronické dielo vytvorené na blockchain).[971]

Predmet kultúrnej hodnoty je pôvodný hmotný alebo duchovný doklad, ktorý má schopnosť priamo alebo sprostredkovane vypovedať o vývoji spoločnosti a má trvalý vedecký, historický, kultúrny alebo umelecký význam.

Falšovaným predmetom kultúrnej hodnoty sa rozumejú akékoľvek neoprávnene vyhotovované napodobeniny kultúrnych predmetov bez ohľadu na kvalitu alebo spôsob napodobnenia. Falšovanie je proces neoprávneného vyhotovovania predmetu kultúrnej hodnoty.

Neoprávnene vyrobenými predmetmi kultúrnej hodnoty sú tie, ktoré spĺňajú technické špecifikácie pravých predmetov kultúrneho dedičstva, ktoré však boli vyrobené neoprávnenou osobou alebo osobou, ktorá je inak oprávnená, no vyrobila ich mimo rámca/nad rámec svojho oprávnenia.

---

[969] Ustanovenie §249a TZ:
„(1) Kto neoprávnene vyrobí, napodobní alebo pozmení predmet kultúrnej hodnoty tak, aby bol považovaný za pravý, alebo kto taký predmet sebe alebo inému zadováži alebo prechováva, potrestá sa odňatím slobody až na dva roky.
(2) Odňatím slobody na šesť mesiacov až tri roky sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) z osobitného motívu,
b) vo väčšom rozsahu, alebo
c) prostredníctvom počítačového systému.
(3) Odňatím slobody na jeden rok až päť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) závažnejším spôsobom konania, alebo
b) v značnom rozsahu.
(4) Odňatím slobody na dva roky až osem rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) vo veľkom rozsahu,
b) ako člen nebezpečného zoskupenia, alebo
c) ak ide o predmet kultúrnej hodnoty požívajúci ochranu podľa osobitného predpisu."

[970] *Non-fungible* (nezameniteľný) token napr. kolekcie obrázkov CryptoPunks alebo Bored Ape Yacht Club; dielo "Everydays: The First 5000 Days" od umelca Beeple; digitálne cyklistické rámy zn. Colnago alebo napr. predmet sporu medzi Meta Birkins NFT a spoločnosťou Hermés o predaj NFT tokenov ikonických dámskych kabeliek Birkin.

[971] Zväčša na blockchain Ethereum.

Zadovážením sa rozumie nadobudnutie falšovaných, pozmenených alebo neoprávnene vyrobených predmetov kultúrnej hodnoty, bez ohľadu na spôsob nadobudnutia – kúpa, darovanie, výmena, či už pre seba alebo inú osobu.

Znakom podmieňujúcim použitie kvalifikovanej sadzby je, že sa ho páchateľ dopustil prostredníctvom počítačového systému. V tomto prípade sa použije tento kvalifikačný znak ak sa predmet kultúrnej hodnoty získa s prispením počítačového systému, napr. vyrobenie alebo navrhnutie napodobeniny, alebo priamo vytvorenie NFT diela, ako digitálneho umeleckého diela, ktoré požíva ochranu.

Subjekt tohto trestného činu je všeobecný, a preto ním môže ním byť ktorákoľvek trestne zodpovedná fyzická alebo právnická osoba.

Subjektívna stránka tohto trestného činu vyžaduje úmyselné zavinenie.

12.4.4.2 Počítačové trestné činy zachytávajúce obsah a počítačové trestné činy sledujúce súkromie osoby

Ide o skupinu rôznych trestných činov z rôznych hláv osobitnej časti Trestného zákona, ktoré majú spoločný objekt v ochrane privilegovaných informácií alebo súkromia osôb, v ktorých prípade hovoríme *o tzv. stalkingu* prostredníctvom rôznych aplikácií, softvérov či *keyloggerov,* ktorými sa získa prístup k takýmto informáciám, avšak nie za účelom podvodného konania,[972] ale za účelom ich ďalšieho využitia či držby, nakoľko majú hospodársky význam pre súkromný sektor (napr. získanie konkurenčnej výhody) alebo pre verejný sektor (napr. získanie utajovaných informácií obranného, zahranično-politického významu). Vo vzťahu k zásahom do súkromia osôb ide najmä o sledovanie prejavov osobnej a intimnej povahy obete, prístupu k jej fotkám, videám, osobným údajom o jej živote, rodinných príslušníkoch a podobne.

PRÍKLAD

Najznámejšími hackerskými skupinami, s afinitou k štátom sú napr. skupiny: [973]

- APT38 (Lazarus) s prepojením na Severnú Kóreu;
- APT28 (Fancy Bear), APT29 (Cozy Bear), Sandworm, Turla, Sandworm, NoName 057 napojené na Ruskú federáciu a ich spravodajské služby FSB a GRU;

[972] K tomu pozri a porovnaj výklad k trestnému činu podvodu podľa § 221 TZ.
[973] Dostupné dňa 27.11.2025 na: LINK

- ShadowBrokers s afinitou na USA a ich Národnú bezpečnostnú agentúru (NSA);
- APT31 s napojením na Čínu;

Ohrozenie obchodného, bankového, poštového, telekomunikačného a daňového tajomstva (§264 TZ).[974]

Objekt tohto trestného činu je ochrana obchodného, bankového, daňového, telekomunikačného a poštového tajomstva pred *priemyslenou špionážou*.

Objektívna stránka spočíva alternatívne buď vo vyzvedaní obchodného, bankového, poštového, telekomunikačného alebo daňového tajomstva v úmysle vyzradiť ho nepovolanej osobe, alebo v samotnom vyzradení takého tajomstva. V zásade ide o ustanovenie, ktoré sankcionuje priemyselnú špionáž a získavanie citlivých privilegovaných informácií, ktoré sa spravidla uskutočňujú prostredníctvom ransomwere, softwarov zachytávajúcich obsah ako sú trojské kone, *man in the middle* technológie, či iné programy zameraná na zaisťovanie a zachytávanie údajov. Uvedené systémy môžu byť nainštalovane v danej entite i celé roky a zbierať citlivé údaje.

Vyzvedaním sa rozumie vedomé konanie smerujúce k získaniu informácie, ktorá tvorí predmet obchodného *(tzv. priemyselná špionáž),* bankového, poštového, telekomunikačného alebo daňového tajomstva.

Za vyzradenie sa považuje situácia, keď je takejto osobe neoprávnene sprístupnená informácia, ktorá má povahu uvedeného tajomstva.

Obchodné tajomstvo podľa § 17 ods. 1 OBZ tvoria všetky skutočnosti obchodnej, výrobnej alebo technickej povahy súvisiace s podnikom, ktoré majú skutočnú alebo aspoň potenciálnu materiálnu alebo nemateriálnu hodnotu, nie sú v príslušných obchodných

[974] Ustanovenie §264 TZ znie:
(1) Kto vyzvedá obchodné tajomstvo, bankové tajomstvo, poštové tajomstvo, telekomunikačné tajomstvo alebo daňové tajomstvo v úmysle vyzradiť ho nepovolanej osobe alebo kto také tajomstvo nepovolanej osobe úmyselne vyzradí, potrestá sa odňatím slobody na šesť mesiacov až tri roky.
(2) Odňatím slobody na jeden rok až päť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a. a spôsobí ním väčšiu škodu,
b. z osobitného motívu, alebo
c. závažnejším spôsobom konania.
(3) Odňatím slobody na dva roky až osem rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a. a spôsobí ním škodu veľkého rozsahu,
b. ako člen nebezpečného zoskupenia, alebo
c. za krízovej situácie.

kruhoch bežne dostupné, majú byť podľa vôle majiteľa obchodného tajomstva utajené a majiteľ obchodného tajomstva zodpovedajúcim spôsobom ich utajenie zabezpečuje.

Bankové tajomstvo tvoria podľa § 91 ods. 1 zákona č. 483/2001 Z. z. o bankách všetky informácie a doklady o záležitostiach týkajúcich sa klienta banky alebo klienta pobočky zahraničnej banky, ktoré nie sú verejne prístupné, najmä informácie o obchodoch, stavoch na účtoch a stavoch vkladov. Tieto informácie banka a pobočka zahraničnej banky sú povinné utajovať a chrániť pred vyzradením, zneužitím, poškodením, zničením, stratou alebo odcudzením.

Poštové tajomstvo podľa § 10 ods. 1 zákona č. 324/2011 Z. z. o poštových službách tvorí informácia a údaj o poštových zásielkach a o poštových službách k nim poskytnutých alebo poskytovaných okrem informácií štatistického charakteru, z ktorých nevyplýva, kto bol odosielateľom alebo adresátom, obsah korešpondencie alebo obsah ostatných poštových zásielok.

Telekomunikačné tajomstvo je podľa § 117 ods. 1 zákona č. 452/2021 Z. z. o elektronických komunikáciách tvorené obsahom prenášaných správ, údajmi komunikujúcich strán, ktorými sú telefónne číslo, obchodné meno a sídlo právnickej osoby, alebo obchodné meno a miesto podnikania fyzickej osoby – podnikateľa alebo osobné údaje fyzickej osoby, ktorými sú meno, priezvisko, titul a adresa trvalého pobytu ak sú spojené s údajmi podľa písmena a), c) alebo písmena d); predmetom telekomunikačného tajomstva nie sú údaje, ktoré sú zverejnené v telefónnom zozname, prevádzkové údaje, lokalizačné údaje.

Daňové tajomstvo je podľa § 11 ods. 1 zákona č. 563/2009 Z. z. o správe daní (daňový poriadok) informácia o daňovom subjekte, ktorá sa získa pri správe daní. Za daňové tajomstvo sa nepovažuje informácia, ktorá bola alebo je verejne prístupná, a informácia o tom, či prebieha alebo prebiehala daňová kontrola alebo daňové exekučné konanie.

Subjekt je všeobecný, a teda páchateľom môže byť ktorákoľvek trestne zodpovedná fyzická osoba.

Subjektívna stránka predpokladá pri oboch základných skutkových podstatách úmyselné zavinenie. V prípade vyzvedania obchodného, bankového, poštového, telekomunikačného alebo daňového tajomstva pristupuje aj obligatórny znak tejto skutkovej podstaty, ktorým je motív v podobe úmyslu vyzradiť informácie, ktoré sú predmetom tajomstva, nepovolanej osobe.

Trestnosť tohto trestného činu zaniká podľa § 85 TZ účinnou ľútosťou, ak páchateľ dobrovoľne škodlivý následok trestného činu zamedzil alebo napravil, alebo urobil o trestnom čine oznámenie v čase, keď sa škodlivému následku trestného činu mohlo ešte zabrániť.

Vyzvedačstvo (§318 TZ)[975], Ohrozenie utajovanej skutočnosti (§319 a §320 TZ)[976] a Ohrozenie dôvernej skutočnosti a vyhradenej skutočnosti (§353 TZ)[977]

Objektom trestného činu vyzvedačstva je ochrana utajovaných skutočností Prísne tajné a Tajné v záujme SR, iného štátu, medzinárodnej organizácie, nadnárodnej organizácie alebo združenia štátov pred cudzou mocou alebo cudzími činiteľmi. **V tomto sa odlišuje**

[975] Ustanovenie §318 TZ znie
(1) Kto vyzvedá skutočnosť utajovanú na ochranu záujmov Slovenskej republiky alebo na ochranu záujmov iného štátu, medzinárodnej organizácie, nadnárodnej organizácie alebo združenia štátov, na ochranu záujmov ktorých sa Slovenská republika zaviazala, označenú podľa zákona stupňom utajenia Prísne tajné alebo Tajné, s cieľom vyzradiť ju cudzej moci alebo cudziemu činiteľovi, alebo kto s takým cieľom zbiera údaje obsahujúce takú utajovanú skutočnosť, alebo kto takú utajovanú skutočnosť cudzej moci úmyselne vyzradí, potrestá sa odňatím slobody na štyri roky až desať rokov.
(2) Odňatím slobody na osem rokov až pätnásť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) ako člen organizácie, ktorej cieľom je vyzvedať utajované skutočnosti, alebo
b) hoci mu bolo uchovávanie utajovanej skutočnosti osobitne uložené.
(3) Odňatím slobody na pätnásť rokov až dvadsaťpäť rokov alebo trestom odňatia slobody na doživotie sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 za krízovej situácie.
[976] Ustanovenie §319 TZ znie:
(1)Kto vyzvedá skutočnosť utajovanú na ochranu záujmov Slovenskej republiky alebo na ochranu záujmov iného štátu, medzinárodnej organizácie, nadnárodnej organizácie alebo združenia štátov, na ochranu záujmov ktorých sa Slovenská republika zaviazala, označenú podľa zákona stupňom utajenia Prísne tajné alebo Tajné, s cieľom vyzradiť ju nepovolanej osobe, alebo kto s takým cieľom zbiera údaje obsahujúce utajovanú skutočnosť, alebo kto takú utajovanú skutočnosť nepovolanej osobe úmyselne vyzradí, potrestá sa odňatím slobody na šesť mesiacov až tri roky.
(2) Kto utajovanú skutočnosť uvedenú v odseku 1 vyzvedá s úmyslom vyzradiť ju do cudziny alebo kto takú utajovanú skutočnosť úmyselne do cudziny vyzradí, potrestá sa odňatím slobody na jeden rok až päť rokov.
(3) Odňatím slobody na tri roky až osem rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 alebo 2
a) hoci mu bolo uchovávanie utajovanej skutočnosti osobitne uložené, alebo
b) za krízovej situácie.
Ustanovenie §320 TZ znie:
Kto z nedbanlivosti spôsobí vyzradenie skutočnosti utajovanej na ochranu záujmov Slovenskej republiky alebo na ochranu záujmov iného štátu, medzinárodnej organizácie, nadnárodnej organizácie alebo združenia štátov, na ochranu záujmov ktorých sa Slovenská republika zaviazala, označenú podľa zákona stupňom utajenie Prísne tajné alebo Tajné, nepovolanej osobe, alebo spôsobí stratu listiny alebo veci obsahujúcej takú utajovanú skutočnosť, potrestá sa odňatím slobody až na tri roky.
[977] Ustanovenie §353 TZ znie:
(1) Kto vyzvedá skutočnosť utajovanú na ochranu záujmov Slovenskej republiky alebo na ochranu záujmov iného štátu, medzinárodnej organizácie, nadnárodnej organizácie alebo združenia štátov, na ochranu záujmov ktorých sa Slovenská republika zaviazala, označenú podľa zákona stupňom utajenia Dôverné alebo Vyhradené, s cieľom vyzradiť ju nepovolanej osobe, alebo kto s takým cieľom zbiera údaje obsahujúce takú utajovanú skutočnosť, alebo kto takú utajovanú skutočnosť nepovolanej osobe úmyselne vyzradí, potrestá sa odňatím slobody až na jeden rok.
(2) Kto utajovanú skutočnosť uvedenú v odseku 1 vyzvedá s úmyslom vyzradiť ju do cudziny alebo kto takú utajovanú skutočnosť úmyselne do cudziny vyzradí, potrestá sa odňatím slobody na šesť mesiacov až tri roky.

tento trestný čin od trestného činu Ohrozenia utajovanej skutočnosti, kde sa ochrana poskytuje týmto druhom utajovaných skutočností pred ich zverejnením **akejkoľvek neoprávnenej osobe.**

Ustanovenie obsahuje jednu základnú skutkovú podstatu, ktorá je zločinom, a dve kvalifikované skutkové podstaty, z ktorých prvá (odsek 2) je zločinom a druhá (odsek 3) je obzvlášť závažným zločinom.

Na trestný čin vyzvedačstva sa z hľadiska pôsobnosti Trestného zákona vzťahuje zásada univerzality podľa § 5a TZ- extrateritoriálnu pôsobnosť Trestného zákona.

Pri trestnom čine podľa § 318 TZ je vylúčená aplikácia okolnosti vylučujúcej protiprávnosť podľa § 30 ods. 2 TZ – oprávnené použitie agenta, keď osoba koná ako agent podľa §117 TP, protiprávnosť konania nie je vylúčená, ak svojim konaním naplní skutkovú podstatu vyzvedačstva. Na trestný čin vyzvedačstva sa aplikujú aj všeobecné ustanovenia o účinnej ľútosti podľa § 85 TZ.

Jednočinný súbeh s trestným činom ohrozenia utajovanej skutočnosti (§ 319 TZ) je vylúčený, keďže trestný čin podľa § 319 TZ je subsidiárnym ustanovením. Jednočinný súbeh trestného činu vyzvedačstva a trestného činu prijímania úplatku (§ 329 TZ) je možný.[978]

Objektívna stránka spočíva alternatívne vo:

- vyzvedaní utajovaných skutočností alebo
- zbieraní utajovaných skutočností
- vyzradení utajovaných skutočností cudzej moci, alebo cudziemu činiteľovi ktoré sú označené ako Prísne tajné" alebo „Tajné".[979] ktoré by mohli vážne ohroziť:
- ústavnosť, zvrchovanosť alebo územnú celistvosť Slovenskej republiky,
- bezpečnosť a obranu štátu,
- jeho zahraničnopolitické postavenie alebo medzinárodné záväzky.

Utajovanou skutočnosťou sa rozumie informácia alebo vec určená pôvodcom, ktorú vzhľadom na záujem Slovenskej republiky treba chrániť pred vyzradením, zneužitím, poškodením, neoprávneným rozmnožením, zničením, stratou alebo odcudzením a ktorá môže vznikať len v oblastiach, ktoré ustanoví vláda nariadením.[980]

[978] Rozsudok ŠTS sp. zn. 15T/1/2023.
[979] Nariadenie vlády č. 216/2004 Z. z., ktorým sa ustanovujú oblasti utajovaných skutočností. K podrobnostiam pozri bližšie vyhlášku Národného bezpečnostného úradu č. 48/2019 Z. z., ktorou sa ustanovujú podrobnosti o administratívnej bezpečnosti utajovaných skutočností.
[980] §2 ods. 1 zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností v znení neskorších predpisov

Vyzvedaním sa akékoľvek neoprávnené získavanie informácií, alebo časti informácií klasifikovaných spôsobom „Prísne tajné" alebo „Tajné", bez ohľadu na to, či páchateľ uspeje, alebo nie. Vo vzťahu ku kybernetickej kriminalite pôjde najmä o konanie spočívajúce v zavedení škodlivej aplikácie, softwaru, ktorý je schopný sledovať obsah, alebo stláčanie kláves a týmto vyzvedať utajované skutočnosti. Vzhľadom na administratívne a objektové požiadavky kladené na manipuláciu s týmto druhom utajovaných skutočností pôjde spravidla o kumuláciu aplikácií, softwarov na sledovanie a exfiltráciu dát, keyleoggerov a nejakej formy fyzického konania osoby páchateľa alebo inej osoby. Uvedené konanie nezahŕňa iba systematické sústreďovanie údajov s cieľom ich následného odovzdania cudzej moci, ale postačuje už samotné neoprávnené disponovanie s takýmito údajmi, napríklad ich neoprávnené uchovávanie, archivovanie alebo príprava na ich ďalší prenos.[981]

Zbieraním údajov sa rozumie neoprávnené zhromažďovanie, zber, alebo uchovávanie utajovaných skutočnosti, alebo časti týchto informácií s úmyslom ich odovzdania cudzej moci, alebo cudziemu činiteľovi.

Vyzradením cudzej moci, alebo cudziemu činiteľovi sa rozumie sprístupnenie utajovanej informácie subjektu, ktorý predstavuje cudziu moc, ktorou sa v zmysle § 133 ods. 1 TZ považuje akýkoľvek iný štát, ako je Slovenská republika, ako aj jeho orgány alebo zložky, vrátane spravodajských služieb, ozbrojených síl, diplomatických misií,[982] štátnych úradníkov, resp. vojenské alebo iné zoskupenia štátov.

Podľa § 133 ods. 2 TZ **je cudzím činiteľom** fyzická alebo právnická osoba, ktorá síce nie je predstaviteľom cudzej moci v zmysle orgánu štátu, avšak má významný vplyv v oblasti politiky, hospodárstva alebo spoločenských štruktúr pôsobí významne v rámci štátu, vo vzťahoch medzi štátmi alebo v medzinárodnom priestore. Ide napríklad o vplyvného podnikateľa, lobistu, politicky exponovanú osobu atď.

Pokiaľ páchateľ koná spôsobom v odseku 1, avšak uvedené informácie vyzvedá, zbiera s úmyslom ich sprístupniť **inej osobe alebo vyzradí ich inej osobe (ktorá nie je predstaviteľom cudzej moci, alebo cudzím činiteľom)**, pôjde o skutok, ktorý je potrebné kvalifikovať ako trestný čin ohrozenia Ohrozenie utajovanej skutočnosti podľa §319 alebo §320 TZ, ktoré upravuje konanie z nedbanlivosti, ktoré by mohlo byť naplnené napr.

[981] Porovnaj R 4/1974.
[982] Rozsudok ŠTS 15 T 1/2023.

neopatrným konaním, ktoré porušuje ustanovenia o nakladaní, tvorbe a uchovávaní utajovaných skutočností stupňa „Prísne tajné" alebo „Tajné".[983]

Pokiaľ páchateľ konal spôsobom v odseku 1, avšak vyzvedá, zbiera, alebo vyzradí utajované skutočnosti stupňa „Dôverné" alebo „Vyhradené"[984], pôjde o trestný čin Ohrozenie dôvernej skutočnosti a vyhradenej skutočnosti podľa §353 TZ. Z pohľadu modu operandi pôjde o konanie veľmi podobné alebo totožné, ako je uvedené vyššie.

Subjektom tohto trestného činu môže byť ktorákoľvek trestne zodpovedná fyzická osoba.

Z hľadiska subjektívnej stránky sa vyžaduje úmyselné zavinenie. Nezáleží teda na miere istoty úspešnosti konania páchateľa, ale na tom, že konal vedome a chcel alebo bol uzrozumený s následkom, ktorým je získanie alebo vyzradenie utajovaných skutočností. Pri konaní spočívajúcom vo vyzvedaní, alebo zbere informácií sa vyžaduje osobitný motív vo forme úmyslu takto vyzvedané údaje, alebo zozbierané údaje sprístupniť cudzej moci, alebo cudziemu činiteľovi. Ak páchateľ až následne pojme cieľ vyzradiť utajované skutočnosti po tom, čo ich už nejaký čas neoprávnene prechovával, pácha trestný čin od momentu, keď pojal tento cieľ.[985]

[983] Nariadenie vlády č. 216/2004 Z. z., ktorým sa ustanovujú oblasti utajovaných skutočností. K podrobnostiam pozri bližšie vyhlášku Národného bezpečnostného úradu č. 48/2019 Z. z., ktorou sa ustanovujú podrobnosti o administratívnej bezpečnosti utajovaných skutočností.
[984] Nariadenie vlády č. 216/2004 Z. z., ktorým sa ustanovujú oblasti utajovaných skutočností. K podrobnostiam pozri bližšie vyhlášku Národného bezpečnostného úradu č. 48/2019 Z. z., ktorou sa ustanovujú podrobnosti o administratívnej bezpečnosti utajovaných skutočností.
[985] Primerane R 4/1974.

Ochrana súkromia v obydlí (§194a TZ)[986] a Porušenie dôvernosti ústneho prejavu osobnej povahy (§377 TZ)[987]

Objektom je právo na súkromie v obydlí, zaručené aj čl. 16 ods. 1 a čl. 19 ods. 2 Ústavy SR.

Objektívna stránka spočíva v konaní páchateľa, ktorý úmyselne bez súhlasu užívateľa sleduje jeho život a životy osôb, ktoré sa zdržiavajú obydlí a súčasne s využitím informačno-technických prostriedkov a iných technických prostriedkov toto pozorovanie zaznamenáva alebo vyhotovuje inú dokumentáciu záznamy alebo inú dokumentáciu. Ide o špeciálnu formu stalkingu (nebezpečného prenasledovania podľa §360a TZ) vo vzťahu k porušovaniu práva na súkromie a bezpečnosť v obydlí, pri ktorom sa však nevyžaduje spôsobenie dôvodnej obavy o život alebo zdravie, život alebo zdravie jemu blízkej osoby alebo podstatné zhoršenie kvalitu jeho života.

Informačno-technické prostriedky sú v zmysle § 10 ods. 21 TP elektrotechnické, rádiotechnické, fototechnické, optické, mechanické, chemické a iné technické prostriedky a zariadenia alebo ich súbory použité utajovaným spôsobom pri odpočúvaní a zázname prevádzky v elektronických komunikačných sieťach, obrazových, zvukových alebo obrazovo-

---

[986] Ustanovenie §194a TZ:
(1) Kto úmyselne poruší právo iného na jeho súkromie v obydlí, právo na jeho súkromný a rodinný život vedený v obydlí tým, že bez jeho súhlasu zadovažuje pre seba alebo iné osoby neoprávneným sledovaním jeho obydlia poznatky o jeho živote a živote osôb, ktoré sa zdržiavajú v jeho obydlí, a s využitím informačno-technických prostriedkov a iných technických prostriedkov vyhotovuje z tohto pozorovania záznamy alebo inú dokumentáciu, potrestá sa odňatím slobody až na jeden rok.
Kopírovať
(2)Odňatím slobody na jeden rok až dva roky sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a)závažnejším spôsobom konania,
b)prekonaním prekážky, ktorej účelom je zabrániť vniknutiu do obydlia,
c) najmenej s dvoma osobami, alebo
d)z osobitného motívu.
(3) Odňatím slobody na dva až štyri roky sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) voči chránenej osobe, alebo
b) ako člen nebezpečného zoskupenia.

[987] Ustanovenie §377 TZ znie:
(1)Kto poruší dôvernosť neverejne prednesených slov alebo iného prejavu osobnej povahy tým, že ho neoprávnene zachytí záznamovým zariadením a takto zhotovený záznam sprístupní tretej osobe alebo ho iným spôsobom použije a inému tým spôsobí vážnu ujmu na právach, potrestá sa odňatím slobody až na dva roky.
(2)Odňatím slobody na šesť mesiacov až tri roky sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a)ako člen organizovanej skupiny,
b)a spôsobí takým činom značnú škodu, alebo
c)s úmyslom získať pre seba alebo iného značný prospech.
(3)Odňatím slobody na šesť mesiacov až päť rokov sa páchateľ potrestá, ak
a)spácha čin uvedený v odseku 1 ako verejný činiteľ,
b)spôsobí takým činom škodu veľkého rozsahu, alebo
c)spácha taký čin s úmyslom získať pre seba alebo pre iného prospech veľkého rozsahu.

zvukových záznamov alebo pri vyhľadávaní, otváraní a skúmaní zásielok, ak sa ich použitím zasahuje do základných ľudských práv a slobôd.

V zmysle § 122 ods. 5 TZ **je trestný čin spáchaný v obydlí,** ak je spáchaný v dome alebo byte iného alebo v iných priestoroch slúžiacich na bývanie vrátane priestorov a pozemkov k nim patriacim, ak sú ako súčasť obydlia uzavreté. **V tomto prípade je rozhodujúce, že dôjde k sledovaniu a záznamu prejavov osôb v obydlí. Pre posúdenie trestnosti** skutku podľa tohto ustanovenia, je irelevantné či sa záznamové zariadenie v čase vyhotovania záznamu nachádzalo v obydlí, alebo mimo obydlie (vonku), napr. diaľkový smerový mikrofón, kamera atď., ak zachytené prejavy pochádzajú z obydlia. V prípade, že by páchateľ pri inštalácií sledovacieho záznamového zariadenia aj fyzicky vnikol do obydlia, išlo by o kvalifikačný znak, podmieňujúci vyššiu trestnú sadzbu.

Trestný čin podľa odseku 1 je prečinom.

Predmetom útoku je obydlie.

Subjektívna stránka vyžaduje úmyselné zavinenie (§ 15 TZ). Z tohto dôvodu nebude trestne zodpovedný ten, kto z nedbanlivosti inštaluje bezpečnostné kamery na nehnuteľnosti, svojej alebo cudzej spôsobom, že táto kamera zaberá časť obydlia v susedstve. Ak však k monitorovaniu dochádza i po upozornení, alebo zhliadnutí takto „omylom" vykonaného záznamu, pôjde už o nepriamy úmysel a fyzická osoba prevádzkujúca túto kameru bude svojim konaním napĺňať znaky trestného činu ochrany súkromia v obydlí podľa §184a TZ.

Subjekt je všeobecný, teda ním môže byť ktorákoľvek trestne zodpovedná fyzická osoba. Trestný čin nebezpečného prenasledovania podľa § 360a TZ bude spravidla konzumovať aj trestný čin ochrany súkromia v obydlí podľa § 194a TZ. Trestný čin ochrany súkromia v obydlí podľa § 194a TZ je trestnému činu **porušenia dôvernosti ústneho prejavu a iného prejavu osobnej povahy podľa § 377 TZ vo vzťahu subsidiarity nakoľko pre trestnosť tohto trestného činu sa navyše okrem zachytenia súkromného neverejného prejavu osobnej povahy navyše vyžaduje aby takto zhotovený záznam páchateľ sprístupnil tretej osobe alebo ho iným spôsobom použil a tým inému spôsobí vážnu ujmu na právach,** napríklad napadnutie bezúhonnosti či dobrého mena. Trestný čin Porušenia dôvernosti ústneho prejavu a iného prejavu osobnej povahy sa líši od trestného činu

Nebezpečného elektronického obťažovania podľa §360b, ods.1, písm. b) TZ[988] v tom, že v tomto prípade bol záznam osobného neverejného prejavu získaný **proti vôli osoby a bez jej súhlasu,** zatiaľ čo pri trestnom čine Nebezpečného elektronického obťažovania podľa §360b ods. 1, písm.b) TZ sa neoprávnene zverejní prejav osobnej povahy **získaný so súhlasom obete tohto trestného činu.**

12.4.4.3 Poškodzujúce súvisiace počítačové trestné činy, kybernetický terorizmus, vojnové a medzinárodné zločiny

Ide o skupinu rôznych trestných činov najmä zo siedmej a dvanástej hlavy, čiastočne šiestej hlavy Osobitnej časti Trestného zákona, ktoré majú spoločný objekt najmä v ochrane subjektov a prvkov kritickej infraštruktúry v čase mieru najmä pred teroristickými útokmi a v čase vojny pred rôznymi formami vojnových zločinov alebo medzinárodných zločinov.

[988] Pozri výklad ďalej.

Všeobecné ohrozenie (§284 TZ)[989], Poškodzovanie všeobecne prospešného zariadenia (§286 TZ)[990], Záškodníctvo (§315 TZ)[991] a Teroristický útok (§419 TZ)[992]

[989]Ustanovenie §284 TZ:
(1) Kto úmyselne
a. vydá ľudí do nebezpečenstva smrti alebo ťažkej ujmy na zdraví alebo cudzí majetok do nebezpečenstva škody veľkého rozsahu tým, že spôsobí požiar alebo povodeň, alebo poruchu, či haváriu prostriedku hromadnej prepravy, alebo škodlivý účinok výbušnín, plynu, elektriny, rádioaktivity alebo iných podobne nebezpečných látok alebo síl, alebo sa dopustí iného podobného nebezpečného konania (všeobecné nebezpečenstvo), alebo
b. všeobecné nebezpečenstvo zvýši alebo sťaží jeho odvrátenie alebo zmiernenie,
potrestá sa odňatím slobody na štyri roky až desať rokov.
(2) Odňatím slobody na desať rokov až pätnásť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a. závažnejším spôsobom konania,
b. na chránenej osobe,
c. z osobitného motívu, alebo
d. preto, aby inému zmaril alebo sťažil uplatnenie jeho základných práv a slobôd.
(3) Odňatím slobody na pätnásť rokov až dvadsať rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a. a spôsobí ním ťažkú ujmu na zdraví alebo smrť, alebo
b. ako člen nebezpečného zoskupenia.
(4) Odňatím slobody na dvadsať rokov až dvadsaťpäť rokov alebo trestom odňatia slobody na doživotie sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a. a spôsobí ním ťažkú ujmu na zdraví viacerým osobám alebo smrť viacerých osôb, alebo
b. za krízovej situácie.

[990] Ustanovenie §286 TZ:
Kto úmyselne ohrozí prevádzku:
a) verejného telekomunikačného zariadenia, verejnej poštovej siete alebo prostriedku hromadnej prepravy alebo odstráni, alebo urobí neupotrebiteľnou zvislú dopravnú značku zákazovú alebo príkazovú,
b) ochranného zariadenia proti úniku znečisťujúcich látok,
c) energetického zariadenia alebo verejného vodovodu, alebo verejnej kanalizácie,
d) verejného ochranného zariadenia proti požiaru, povodni alebo inej mimoriadnej udalosti,
e) podmorského kábla alebo podmorského potrubia,
f) obranného alebo ochranného zariadenia proti leteckým a iným podobným útokom alebo ich následkom,
g) stavieb a zariadení slúžiacich lesnému hospodárstvu, alebo
h) podobného všeobecne prospešného zariadenia, potrestá sa odňatím slobody na jeden rok až päť rokov.
(2) Odňatím slobody na štyri roky až osem rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) a spôsobí ním poruchu prevádzky všeobecne prospešného zariadenia, alebo
b) za krízovej situácie.

[991]Ustanovenie § 315 TZ znie.
(1)Kto v úmysle poškodiť ústavné zriadenie alebo obranyschopnosť Slovenskej republiky
a)vydá skupinu osôb do nebezpečenstva smrti, ťažkej ujmy na zdraví alebo cudzí majetok do nebezpečenstva škody veľkého rozsahu tým, že spôsobí požiar, povodeň alebo poruchu, či haváriu prostriedku hromadnej prepravy, alebo škodlivý účinok výbušnín, plynu, elektriny, rádioaktivity alebo iných podobne nebezpečných látok alebo síl, alebo nebezpečenstvo zvýši, alebo sťaží jeho odvrátenie alebo zmiernenie, alebo
b)dopustí sa iného podobného nebezpečného konania,
potrestá sa odňatím slobody na sedem rokov až dvanásť rokov.
(2)Odňatím slobody na dvanásť rokov až dvadsať rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a)a spôsobí ním väčšiu škodu,
b) závažnejším spôsobom konania, alebo
c) na chránenej osobe.
(3) Odňatím slobody na pätnásť rokov až dvadsaťpäť rokov alebo trestom odňatia slobody na doživotie sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a)a spôsobí ním ťažkú ujmu na zdraví alebo smrť,
b)a spôsobí ním škodu veľkého rozsahu alebo iný obzvlášť závažný následok, alebo
c)ako člen nebezpečného zoskupenia.

Objektom tohto trestného činu je ochrana obyvateľstva resp. aspoň skupiny osôb siedmich ľudí[993] pred „hromadným nebezpečenstvom"[994], ktoré môže ohroziť, život, zdravie alebo majetok (vo veľkom rozsahu).

Objektívna stránka tohto trestného činu spočíva alternatívne v:

- spôsobení (vzniku) nebezpečenstva
- zvýšení nebezpečenstva (už existujúceho) alebo
- sťažení odstránenia alebo odvrátenia (už existujúceho) nebezpečenstva ohrozujúceho

(4)Odňatím slobody na dvadsať rokov až dvadsaťpäť rokov alebo trestom odňatia slobody na doživotie sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a)a spôsobí ním ťažkú ujmu na zdraví viacerým osobám alebo smrť viacerých osôb, alebo
b)za krízovej situácie.

[992] Ustanovenie §419 TZ znie:
(1) Kto v úmysle poškodiť ústavné zriadenie alebo obranyschopnosť štátu, narušiť alebo zničiť základnú politickú, hospodársku alebo spoločenskú štruktúru štátu alebo medzinárodnej organizácie, závažným spôsobom zastrašiť obyvateľstvo alebo donútiť vládu štátu alebo iný orgán verejnej moci alebo medzinárodnej organizácie, aby niečo konala, opomenula alebo strpela
a)hrozí spáchaním útoku alebo spácha útok ohrozujúci život, zdravie človeka alebo jeho osobnú slobodu,
b)zničí, znefunkční alebo poškodí verejné zariadenie, dopravný systém, telekomunikačný systém, informačný systém, vrátane závažného bránenia vo fungovaní informačného systému alebo prerušenia fungovania informačného systému, pevnú plošinu na podmorskej plytčine, energetické zariadenie, vodárenské zariadenie, zdravotnícke zariadenie alebo iné dôležité zariadenie, verejné priestranstvo alebo majetok, alebo takým konaním hrozí,
c)naruší, znefunkční alebo preruší dodávku vody, elektrickej energie alebo iného základného prírodného zdroja s cieľom vydať ľudí do nebezpečenstva smrti alebo ťažkej ujmy na zdraví alebo cudzí majetok do nebezpečenstva škody veľkého rozsahu, alebo takým konaním hrozí,
d)zmocní sa lietadla, lode, iného prostriedku osobnej dopravy alebo nákladnej dopravy alebo pevnej plošiny na podmorskej plytčine, alebo nad takým dopravným prostriedkom alebo pevnou plošinou vykonáva kontrolu, alebo zničí alebo vážne poškodí navigačné zariadenie alebo zasahuje do jeho prevádzky, alebo oznámi nepravdivú informáciu, čím ohrozí život alebo zdravie ľudí, bezpečnosť takého dopravného prostriedku, alebo vydá cudzí majetok do nebezpečenstva škody veľkého rozsahu, alebo takým konaním hrozí,
e)požaduje, vyrobí, získa, prechováva, vlastní, drží, dovezie, vyvezie, prevezie, dá prepraviť, dodá alebo inak použije výbušninu, jadrový materiál, rádioaktívnu látku, chemickú látku, biologický agens alebo toxín, strelnú zbraň, jadrovú zbraň, rádiologickú zbraň, biologickú zbraň, chemickú zbraň alebo inú zbraň, bojový prostriedok alebo materiál obdobnej povahy, alebo robí výskum a vývoj jadrovej zbrane, biologickej zbrane, chemickej zbrane alebo inej zbrane alebo bojového prostriedku alebo výbušniny, alebo zariadenia na výrobu, úpravu, skladovanie alebo použitie jadrových materiálov, rádioaktívnych látok, chemických látok alebo biologických agensov a toxínov, alebo takým konaním hrozí, alebo
f)vydá ľudí do nebezpečenstva smrti alebo ťažkej ujmy na zdraví, alebo cudzí majetok do nebezpečenstva škody veľkého rozsahu tým, že spôsobí požiar alebo povodeň alebo škodlivý účinok výbušnín, plynu, elektriny alebo iných podobne nebezpečných látok alebo síl alebo sa dopustí iného podobne nebezpečného konania, alebo také nebezpečenstvo zvýši alebo sťaží jeho odvrátenie alebo zmiernenie, alebo takým konaním hrozí,
potrestá sa odňatím slobody na dvadsať rokov až dvadsaťpäť rokov alebo trestom odňatia slobody na doživotie.
(2)Trestom odňatia slobody na doživotie sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a)a spôsobí ním ťažkú ujmu na zdraví viacerým osobám alebo smrť viacerých osôb,
b)na chránenej osobe,
c)voči ozbrojeným silám alebo voči ozbrojeným zborom,
d)ako člen nebezpečného zoskupenia, alebo
e)za krízovej situácie.

[993] R 39/1982.

[994] Povodňou, požiarom, hrubou bezohľadnou jazdou (R 41/2024), alebo inak.

život, zdravie, alebo veľkú škodu na majetku. Z hľadiska následku ide o ohrozovací trestný čin, čo znamená, že je predčasne dokonaný trestného činu (pokus trestného činu je za daných okolností možný len v prípade použitia nespôsobilého prostriedku alebo nespôsobilého predmetu útoku) vydanie ľudí do nebezpečenstva smrti alebo ťažkej ujmy na zdraví alebo cudzieho majetku do nebezpečenstva škody veľkého rozsahu príslušnou formou nebezpečného konania.

PRÍKLAD

Z pohľadu kybernetickej kriminality pôjde spravidla o rôzne formy kybernetických útokov, ktoré cielia **najmä na prvky a subjekty kritickej infraštruktúry (nemocnice, letiská, elektrárne a rozvádzače, telekomunikační operátori atď.),**[995] pričom výpadok energie alebo dostupnosti služieb (napr. telekomunikačné spojenie, vykurovanie, voda) môže ohroziť život, zdravie, alebo majetok vo veľkom rozsahu. (nemožnosť núdzových volaní, havárie, nedostupnosť zdravotnej starostlivosti apod.)

Z pohľadu subjektívnej stránky je trestný čin všeobecného ohrozenia je v podmienkach § 284 TZ úmyselným trestným činom. V prípade, že by takýto **kybernetický**

[995] S poukazom na §2, písm.c) zákona č. 367/2024 Z. z. o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov je kritickým subjektom právnická osoba alebo fyzická osoba – podnikateľ, ktorá poskytuje základnú službu a ktorá je postupom podľa tohto zákona identifikovaná ako kritický subjekt, podľa prílohy č. 1 k zákonu: elektroenergetické podniky podľa osobitného predpisu, prevádzkovatelia distribučnej sústavy podľa osobitného predpisu, prevádzkovatelia prenosovej sústavy podľa osobitného predpisu, výrobcovia elektriny podľa osobitného predpisu, dodávateľské podniky podľa osobitného predpisu, prevádzkovatelia distribučnej siete podľa osobitného predpisu, prevádzkovatelia prepravnej siete podľa osobitného predpisu, prevádzkovatelia zásobníkov podľa osobitného predpisu, prevádzkovatelia zariadení na skvapalňovanie zemného plynu podľa osobitného predpisu, plynárenské podniky podľa osobitného predpisu, prevádzkovatelia zariadení na rafinovanie a spracovanie zemného plynu, letecký dopravcovia podľa osobitného predpisu, prevádzkovatelia letiska podľa osobitného predpisu, vrátane hlavných letísk podľa osobitného predpisu, prevádzkovatelia kontroly riadenia dopravy poskytujúci služby riadenia letovej prevádzky (ATC) podľa osobitného predpisu, železničné podniky podľa osobitného predpisu46) služby železničnej dopravy (osobnej a nákladnej) prevádzkovatelia servisných zariadení podľa osobitného predpisu, spoločnosti prevádzkujúce vnútrozemskú, námornú a pribrežnú osobnú a nákladnú lodnú dopravu podľa osobitného predpisu, prístavné orgány, prevádzkovatelia prístavov a prístavných zariadení (kotviská, výväziská, prekladiská a prístaviská) vrátane ich prístavných zariadení podľa osobitného predpisu49) a užívatelia prístavov a prístavných zariadení, prevádzkovatelia plavebno-prevádzkových služieb podľa osobitného predpisu, správcovia pozemných komunikácií podľa osobitného predpisu, prevádzkovatelia inteligentných dopravných systémov, poskytovatelia služieb vo verejnom záujme podľa osobitného predpisu, poskytovatelia univerzálnej poštovej služby podľa osobitného predpisu, poskytovatelia zdravotnej starostlivosti podľa osobitného predpisu, poskytovanie služieb zdravotnej starostlivosti, referenčné laboratóriá EÚ podľa osobitného predpisu, subjekty vykonávajúce činnosti vo výskume a vývoji liekov podľa osobitného predpisu, subjekty vyrábajúce zdravotnícke pomôcky považované za kritické v núdzovej situácii v oblasti verejného zdravia podľa osobitného predpisu, subjekty, ktoré sú držiteľmi povolenia na distribúciu liekov podľa osobitného predpisu atď.

útok bol spáchaný v úmysle (s cieľom) poškodiť ústavné zriadenie Slovenskej republiky alebo obranyschopnosť štátu, narušiť alebo zničiť základnú politickú, hospodársku alebo spoločenskú štruktúru štátu alebo medzinárodnej organizácie, závažným spôsobom zastrašiť obyvateľstvo alebo donútiť vládu štátu alebo iný orgán verejnej moci alebo medzinárodnej organizácie, aby niečo konala, opomenula alebo strpela,[996] išlo by o trestný čin Teroristického útoku podľa §419 ods.1 písm.a)[997] písm.b)[998], písm.c)[999], písm.d)[1000], písm. f)[1001], ktorý v zmysle §140 písm.d) TZ je špeciálnym ustanovením k trestnému činu Všeobecného ohrozenia podľa §284 TZ, Záškodníctva podľa §315 TZ alebo §316 TZ (ak by bola poškodená kybernetickým útokom vec dôležitá pre ochranu ústavného zriadenia SR, alebo ktorej poškodením by bolo možné ohroziť ústavné zriadenie SR). **V zásade platí, že v prípade prítomnosti tzv. teroristického úmyslu pri akomkoľvek trestnom čine v Osobitnej časti TZ, pôjde vždy o trestný čin Teroristického útoku podľa §419 TZ, napr. šírenie poplašnej správy s poukazom na §419, ods. 1, písm. d) – oznámenie nepravdivej informácie s teroristickým úmyslom.[1002]**

Subjekt tohto trestného činu je všeobecný, môže ním byť každá trestne zodpovedná fyzická ale i právnická osoba.

V prípade, že **nebudú splnené kumulatívne podmienky ohrozenia života, zdravia alebo majetku veľkého rozsahu nefunkčnosťou/nedostupnosťou služieb niektorých zo subjektov najmä kritickej infraštruktúry aspoň siedmich osôb (skupiny obyvateľstva)**

---

[996] obligatórny znak trestného činu Teroristického útoku tzv. teroristický úmysel. K tomu viac STRÉMY, T., KURILOVSKÁ, L., REMETA, R. a kol.. Trestný zákon- praktický komentár. Wolters Kluwer, Bratislava, ISBN: 978-80-286-0378-6, 2025 s. 560

[997] Hrozí spáchaním útoku alebo spácha útok ohrozujúci život, zdravie človeka.

[998] Zničí, znefunkční alebo poškodí verejné zariadenie, dopravný systém, telekomunikačný systém, informačný systém, vrátane závažného bránenia vo fungovaní informačného systému alebo prerušenia fungovania informačného systému, pevnú plošinu na podmorskej plytčine, energetické zariadenie, vodárenské zariadenie, zdravotnícke zariadenie alebo iné dôležité zariadenie, verejné priestranstvo alebo majetok, alebo takým konaním hrozí,

[999] Naruší, znefunkční alebo preruší dodávku vody, elektrickej energie alebo iného základného prírodného zdroja s cieľom vydať ľudí do nebezpečenstva smrti alebo ťažkej ujmy na zdraví alebo cudzí majetok do nebezpečenstva škody veľkého rozsahu, alebo takým konaním hrozí

[1000] Nad takým dopravným prostriedkom alebo pevnou plošinou vykonáva kontrolu, alebo zničí alebo vážne poškodí navigačné zariadenie alebo zasahuje do jeho prevádzky, alebo oznámi nepravdivú informáciu, čím ohrozí život alebo zdravie ľudí, bezpečnosť takého dopravného prostriedku, alebo vydá cudzí majetok do nebezpečenstva škody veľkého rozsahu, alebo takým konaním hrozí

[1001] Vydá ľudí do nebezpečenstva smrti alebo ťažkej ujmy na zdraví, alebo cudzí majetok do nebezpečenstva škody veľkého rozsahu tým, že spôsobí požiar alebo povodeň alebo škodlivý účinok výbušnín, plynu, elektriny alebo iných podobne nebezpečných látok alebo síl alebo sa dopustí iného podobne nebezpečného konania, alebo také nebezpečenstvo zvýši alebo sťaží jeho odvrátenie alebo zmiernenie, alebo takým konaním hrozí.

[1002] STRÉMY, T.; KURILOVSKÁ, L.; REMETA, R. a kol. Trestný zákon - praktický komentár. Wolters Kluwer, Bratislava, ISBN: 978-80-286-0378-6, 2025 s. 560.

daným kybernetickým útokom spravidla pôjde o trestný čin Poškodzovania všeobecne prospešného zariadenia podľa §286 ods.1 TZ.

V prípade, že bude útok **namierený proti civilnému obyvateľstvu na obsadených územiach** v čase vojny pôjde o trestný čin **perzekúcie obyvateľstva podľa §432 ods. 2, písm.a) TZ.**

Používanie zakázaného bojového prostriedku a nedovolené vedenie boja (§426 TZ)[1003], Perzekúcia obyvateľstva (§432 TZ)[1004], Vojnové bezprávie (§433 TZ)[1005]

[1003] Ustanovenie §426 TZ znie:
(1) Kto počas vojny nariadi
a. použitie zakázaného bojového prostriedku alebo materiálu obdobnej povahy, alebo taký prostriedok alebo materiál použije, alebo
b. vedenie boja zakázaným spôsobom, alebo sám takto boj vedie,
potrestá sa odňatím slobody na štyri roky až desať rokov.
(2) Rovnako ako v odseku 1 sa potrestá, kto ako veliteľ, ktorý v rozpore s ustanoveniami medzinárodného práva o prostriedkoch a spôsoboch vedenia vojny úmyselne
a. poškodí vojenskou operáciou civilné osoby na živote, zdraví alebo majetku, alebo vedie útok proti nim z dôvodu represálií, vedie útok proti nebránenému miestu alebo demilitarizovanému pásmu,
b. zničí alebo poškodí priehradu, jadrovú elektráreň alebo obdobné zariadenie obsahujúce nebezpečné sily, alebo
c. zničí alebo poškodí objekt určený na humanitárne účely alebo medzinárodne uznávanú kultúrnu alebo prírodnú pamiatku.
(3) Odňatím slobody na desať rokov až dvadsať rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 alebo 2 a spôsobí ním
a. ťažkú ujmu na zdraví viacerým osobám alebo smrť viacerých osôb,
b. škodu veľkého rozsahu, alebo
c. iný obzvlášť závažný následok.
[1004] Ustanovenie §432 TZ znie:
(1) Kto počas vojny pácha neľudské činy vyplývajúce z národnostnej, rasovej alebo etnickej diskriminácie alebo terorizuje bezbranné civilné obyvateľstvo násilím alebo hrozbou jeho použitia, potrestá sa odňatím slobody na štyri roky až desať rokov.
(2) Rovnako ako v odseku 1 sa potrestá, kto v dobe uvedenej v odseku 1
a. zničí alebo vážne naruší zdroj základných životných potrieb civilného obyvateľstva na obsadenom území alebo v dotykovej zóne, alebo svojvoľne neposkytne obyvateľstvu pomoc nevyhnutnú na prežitie,
b. bezdôvodne odďaľuje návrat civilného obyvateľstva alebo vojnových zajatcov,
c. bezdôvodne presídľuje civilné obyvateľstvo obsadeného územia,
d. osídľuje obsadené územie obyvateľstvom vlastnej krajiny, alebo
e. svojvoľne znemožní civilnému obyvateľstvu alebo vojnovým zajatcom, aby sa o ich trestných činoch rozhodovalo v spravodlivom konaní.
(3) Odňatím slobody na desať rokov až dvadsaťpäť rokov alebo trestom odňatia slobody na doživotie sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 alebo 2 a spôsobí ním ťažkú ujmu na zdraví alebo smrť alebo iný obzvlášť závažný následok.
[1005] Ustanovenie §433 znie:
(1) Kto spácha čin považovaný článkom 8 Rímskeho štatútu Medzinárodného trestného súdu za vojnový zločin, potrestá sa odňatím slobody na dvanásť rokov až dvadsaťpäť rokov alebo trestom odňatia slobody na doživotie.
(2) Trestom odňatia slobody na doživotie sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a. a spôsobí ním ťažkú ujmu na zdraví viacerým osobám alebo smrť viacerých osôb alebo iný obzvlášť závažný následok, alebo
b. za odplatu.

Trestné činy proti mieru, proti ľudskosti a trestné činy vojnové **nepodliehajú premlčaniu** trestného stíhania v zmysle §88 TZ a ani premlčaniu výkonu trestu v zmysle §91 TZ.

Pre trestné činy používania zakázaného bojového prostriedku a nedovoleného vedenia boja § 426 TZ, , perzekúcie obyvateľstva podľa § 432 TZ, vojnového bezprávia podľa § 433 TZ je daná pôsobnosť Trestného zákona aj vtedy, ak taký trestný čin spáchal mimo územia Slovenskej republiky cudzinec, ktorý nemá na území Slovenskej republiky trvalý pobyt **t.j. na tieto trestné činy sa vzťahuje tzv. univerzálna jurisdikcia v zmysle §5 TZ**

Charakteristickým znakom taktiež je, že ustanovenie §28 ods. 3 TZ, okolnosť vylučujúca protiprávnosť činu- výkon práv a povinností, nepoužije, ak bol spáchaný trestný čin vojnového bezprávia podľa § 433 splnením nariadenia, príkazu, rozkazu alebo pokynu orgánu výkonnej moci alebo nadriadeného, okrem prípadu, ak osoba, ktorá plnila také nariadenie, príkaz, rozkaz alebo pokyn,

a. mala zákonnú povinnosť splniť také nariadenie, príkaz, rozkaz alebo pokyn,
b. nevedela, že také nariadenie, príkaz, rozkaz alebo pokyn je nezákonné, a
c. obsah takého nariadenia, príkazu, rozkazu alebo pokynu nenasvedčoval, že je nezákonné.

Objektom trestného činu používania zakázaného bojového prostriedku a nedovoleného vedenia boja je ochrana civilného obyvateľstva a civilných objektov počas vojny počas ozbrojeného konfliktu, a to s cieľom minimalizovať ich zásah, v súlade s medzinárodnými dohovormi.

Objektívna stránka tohto trestného činu spočíva v nariadení

a) použiť zakázaný bojový prostriedok alebo materiál obdobnej povahy, alebo taký prostriedok alebo materiál použije, alebo

b) viesť boj zakázaným spôsobom, alebo sám takto boj vedie,

Ďalšou obligatórnou súčasťou objektívnej stránky skutkovej podstaty je skutočnosť, že nariadenie, špecifikované v §426 ods. 1 písm. a) alebo b) TZ musí byť urobené **počas vojny.**[1006]

Predmetné ustanovenie reflektuje uznávané zásady medzinárodného humanitárneho práva, podľa ktorých sú zúčastnené strany vo vojnovom konflikte obmedzené na výber prostriedkov, ktorými môžu viesť boj a spôsobiť ujmu nepriateľovi.

Za vojnu sa v zmysle §435 ods. 1 TZ, **ktorú je možné v dnešnej dobe viesť čisto kybernetickými zbraňami, silami a prostriedkami**[1007], považuje medzinárodný ozbrojený konflikt alebo zdĺhavý ozbrojený konflikt na území štátu medzi vládnymi orgánmi a organizovanými ozbrojenými skupinami alebo medzi takýmito skupinami navzájom s výnimkou vnútorných nepokojov a napätí, ako sú vzbury, izolované a ojedinelé akty násilia alebo iné akty podobnej povahy. Ustanovenie §435 ods.1 TZ **definuje pojem vojna v súlade s medzinárodným právom trestným a súčasne rozlišuje medzi medzinárodným a vnútroštátnym ozbrojeným konfliktom. Toto členenie má význam hlavne vo vzťahu k trestnému činu vojnového bezprávia podľa §433 TZ,** ktorý priamo odkazuje na článok 8, odsek 2 Rímskeho štatútu, ktorý rozoznáva a rozlišuje medzi medzinárodným ozbrojeným konfliktom v zmysle článku 8, ods.2 písm. a) a písm. b) Rímskeho štatútu a vnútroštátnym ozbrojeným konfliktom v zmysle článku 8 ods.2 písm. c) a písm. d) Rímskeho štatútu vo vzťahu k spáchaným vojnovým zločinom.

Medzinárodným ozbrojeným konfliktom v zmysle §435 ods. 1 písm. a) TZ sa v súčasnosti má na mysli tradičný medzištátny konflikt a boje za národné oslobodenie. Medzištátny konflikt sa odohráva medzi „Vysokými zmluvnými stranami" t.j. medzi štátmi alebo skupinami štátov.[1008] Boj za národné oslobodenie podľa článku 1 odsek 4 Dodatkového protokolu I k Ženevským dohovorom z roku 1949 *„predstavuje ozbrojené konflikty v ktorých národy bojujú proti koloniálnej nadvláde, cudzej okupácii, rasistickému režimu za účelom uplatnenia svojho práva na sebaurčenie, ktoré je zakotvené v Charte OSN a v Deklarácii zásad medzinárodného práva, upravujúcich priateľské vzťahy a spoluprácu medzi všetkými štátmi s Chartou OSN."* [1009]

Zakázaným bojovým prostriedkom sú v zmysle kybernetickej kriminality tzv. LAW systémy[1010] ktoré dokážu fungovať bez ľudského riadenia/ovládania ako vzdušné bojové prostriedky, plavidlá a aj pozemné sily. [1011]

Materiál obdobnej povahy je akýkoľvek materiál, ktorý je svojimi škodlivými účinkami porovnateľný s niektorým zo zakázaných prostriedkov.

[1007] Tallinn Manual. Dostupné na: LINK
[1008] Ibid, s. 30.
[1009] Ibid, s. 34.
[1010] Lethal Autonomous Weapon.
[1011] EYUSUN, H. Lethal Autonomous Weapons: The Next Frontier in International Security and Arms Control, Stanford International Policy Review, Ford Dorsey Masters in International Policy, 30th January 2025, dostupné dňa 13.12.2025 na LINK.

Zakázaný spôsob vedenia boja je podľa medzinárodných dokumentov taký spôsob boja, ktorý poškodzuje ranených, zajatcov, civilné obyvateľstvo, ďalej útoky na chránené objekty, napr. priehrady a elektrárne, útoky na nebránené miesta a tzv. perfídne spôsoby vedenia boja. Z pohľadu kybernetickej kriminality **pôjde o nasadenia takých LAW systémov, ktoré:**[1012]

a. nie sú riadené a ovládané ľudským operátorom alebo jeho ovládanie nezohľadňuje ľudský úsudok;
b. nedefinujú zodpovednosť za LAW systém;
c. neumožňujú spoľahlivo predvídať, stopovať a vysvetliť účinky (útoky) LAW systému;
d. účinky (útok) LAW systému nerozlišujú civilné ciele a obyvateľstvo;
e. LAW systém nie je trénovaný na dostatočných alebo žiadnych dátach, alebo tieto dáta sú vyberané nesprávne (predpojaté)
f. LAW systém sám nie je oprávnený výlučne sám meniť nastavenia svojich účinkov (útokov), alebo parametrov misie;

Nie je však zakázaná a ani trestná v zmysle Trestného zákona *vojnová lesť.*[1013] Pod týmto pojmom sa rozumejú činy, ktorých účelom je uviesť protivníka do omylu alebo ho primäť k nerozvážnemu konaniu. Tieto činy nie sú vierolomné, pretože nezneužívajú dobrú vieru protivníka, pokiaľ ide o poskytnutie ochrany podľa medzinárodného práva. Jedna sa

[1012] Group Governmental Expert Rolling Text of the Convention on Certain Conventional Weapons, July 26th, 2024; dostupné dňa 13.12.2025 na LINK

[1013] Ustanovenie § 435 ods. 1 TZ definuje pojem vojna v súlade s medzinárodným právom trestným a súčasne rozlišuje medzi medzinárodným a vnútroštátnym ozbrojeným konfliktom. Toto členenie má význam hlavne vo vzťahu k trestnému činu vojnového bezprávia podľa § 433 TZ, ktorý priamo odkazuje na čl. 8 ods. 2 Rímskeho štatútu, ktorý rozoznáva a rozlišuje medzi medzinárodným ozbrojeným konfliktom v zmysle čl. 8, ods. 2 písm. a) a písm. b) Rímskeho štatútu a vnútroštátnym ozbrojeným konfliktom v zmysle čl. 8 ods. 2 písm. c) a písm. d) Rímskeho štatútu vo vzťahu k spáchaným vojnovým zločinom. Uvedené členenie medzinárodných konfliktov zodpovedá členeniu podľa charakteru priestoru, na ktorom je vedený ozbrojený konflikt a charakteru zúčastnených aktérov. In: BÍLKOVÁ V. Úprava vnitrostátních ozbrojených konfliktů v mezinárodním humanitárním právu. Univerzita Karlova v Praze, Právnická fakulta, Praha, 2007, ISBN: 80-85889-82-6, s. 29.
Medzinárodným ozbrojeným konfliktom v zmysle § 435 ods. 1 písm. a) TZ sa v súčasnosti má na mysli tradičný medzištátny konflikt a boje za národné oslobodenie. Medzištátny konflikt sa odohráva medzi vysokými zmluvnými stranami, t. j. medzi štátmi alebo skupinami štátov. In: BÍLKOVÁ V. Úprava vnitrostátních ozbrojených konfliktů v mezinárodním humanitárním právu. Univerzita Karlova v Praze, Právnická fakulta, Praha, 2007, ISBN: 80-85889-82-6, s. 30.
Boj za národné oslobodenie podľa čl.1 ods. 4 Dodatkového protokolu I k Ženevským dohovorom z roku 1949 *„predstavuje ozbrojené konflikty, v ktorých národy bojujú proti koloniálnej nadvláde, cudzej okupácii, rasistickému režimu za účelom uplatnenia svojho práva na sebaurčenie, ktoré je zakotvené v Charte OSN a v Deklarácii zásad medzinárodného práva, upravujúcich priateľské vzťahy a spoluprácu medzi všetkými štátmi s Chartou OSN.*" In: BÍLKOVÁ V. Úprava vnitrostátních ozbrojených konfliktů v mezinárodním humanitárním právu. Univerzita Karlova v Praze, Právnická fakulta, Praha, 2007, ISBN: 80-85889-82-6, s. 34.

o použitie kamufláže, pasce **a z pohľadu kybernetickej kriminality ide o predstieranie operácii, falošných správ a dezinformácii**.

Zmyslom alternatívnej základnej skutkovej podstaty podľa §426 ods. 2 TZ je stanoviť expressis verbis trestnosť správania veliteľa, ktorý nerešpektuje jednu zo základných zásad humanitárneho práva- rozlišovať medzi civilným obyvateľstvom a kombatantami (§ 426 ods. 2 písm. a) TZ), medzi civilnými objektmi a vojenskými objektmi. (§426 ods. 2 písm. b) TZ) a ničiť a poškodzovať objekt určený na humanitárne účely, alebo kultúrnu a prírodnú pamiatku (§426 ods.2 písm. c) TZ). Všetky tieto osoby a objekty „sú vyňaté z ozbrojeného konfliktu" pretože na ňom priamo neparticipujú, alebo mu neslúžia a práve naopak, snažia sa zmierniť dopady ozbrojeného konfliktu na civilné obyvateľstvo (napr. nemocnice, lazarety atď.).

PRÍKLAD
Z pohľadu kybernetickej kriminality, kybernetických zbraní, resp. vedenia kybernetickej vojny ide o konanie vojenského veliteľa, ktorý nariadi nasadenie LAW systému v rozpore so zásadami uvedenými vyššie, alebo nariadi hackerský útok, ktorý by zasiahol, alebo mieril primárne[1014] proti civilnému obyvateľstvu, alebo by ako vojenský veliteľ takýto hackerský útok, alebo LAW systém jednotkami pod svojim velením podporoval, alebo zabezpečoval.

Represálie znamenajú odvetu alebo odplatu za určité skutky alebo činy. Represálie sú zakázané len voči civilnému obyvateľstvu a netýkajú sa osôb, ktoré sa priamo zúčastňujú ozbrojeného konfliktu. Výnimku tvoria, zranení, vojnoví zajatci, zdravotnícky a duchovný personál, t. j. osoby. ktoré priamo neparticipujú na ozbrojenom konflikte ak sa dodrží zásada proporcionality.[1015]

Vojenským veliteľom je v zmysle §426 ods. 2 TZ s poukazom na §435 TZ osoba príslušná veliť podľa vzťahu reťaze velenia t.j. **de iure vojensky veliteľ**. §435 ods.2 TZ taktiež definuje tzv. **de facto veliteľa.** Jedná sa o osobu, ktorá síce nie je vojenským resp. armádnym veliteľom v tom zmysle, že nemá oficiálnu vojenskú právomoc, avšak správa sa tak a je

[1014] ICC, Office of the Prosecutor, Draft policy on cyber-enabled crimes under the Rome Statute, 6. marec 2025, s. 20 – 22. Dostupné dňa 05.12.2025 na: LINK

[1015] BÍLKOVÁ V. Úprava vnitrostátních ozbrojených konfliktů v mezinárodním humanitárním právu. Univerzita Karlova v Praze, Právnická fakulta, Praha, 2007, ISBN: 80-85889-82-6, s. 240.

akceptovaný ako veliteľ svojim okolím.[1016]. V týchto prípadoch sú **de facto veliteľmi** osoby, ktoré nemajú väzbu na riadne armádne zložky pretože sa zväčša jedná o prípady, kedy títo páchatelia sami bojujú proti štátom uznanej armáde resp. vláde.[1017] Ďalším spoločným pojmom, ktorý sa používa v XII. hlave je pojem **nadriadený.** Jedná sa o osoby, ktoré sú v politickej funkcii, alebo sú predstavenými určitej zložky či útvaru, ktoré v čase vojny plnia zákonom stanovené úlohy (prezident, minister, starosta, prednosta obvodného úradu, okresný či krajský riaditeľ Hasičského a záchranného zboru, štatutár strategického podniku apod.). Vo vzťahu k „civilnému" nadriadenému sa uplatňujú tie isté princípy zodpovednosti ako vo vzťahu k vojenskému veliteľovi s výnimkou, že uvedené trestné činy, ktorých sa dopustili páchatelia- podriadení, spadali do právomoci tohto nadriadeného. Pre ostatné prvky zodpovednosti platí primerane výklad o zodpovednosti vojenského veliteľa. Vo vzťahu k trestnej zodpovednosti páchateľa je potrebné uviesť, že **trestná zodpovednosť veliteľa sa nestotožňuje so zásadou individuálnej trestnej zodpovednosti,** ktorá sa týka iba „priamej" zodpovednosti veliteľa, ktorý vydal rozkaz na spáchanie trestných činov uvedených v druhom diely alebo nariadil páchanie takýchto trestných činov. **Ide teda o osobitný druh trestnej zodpovednosti za „konanie podriadených" a väčšina autorov považuje túto zodpovednosť za „ďalší druh trestnej zodpovednosti".**[1018]

Páchateľom tohto trestného činu nemôže byť ktokoľvek. **Páchateľom môže byť len príslušník ozbrojených síl alebo ozbrojených zborov, prípadne veliteľ v ods. 2.**

Zo subjektívnej stránky sa vyžaduje úmyselné zavinenie.

V prípade, že **bude útok v čase vojny namierený proti civilnému obyvateľstvu na obsadených územiach,** avšak mimo prebiehajúce vojenské operácie, pôjde o trestný čin perzekúcie obyvateľstva podľa §432 ods.2 TZ, ktorý poskytuje ochranu civilnému obyvateľstvu a vojnovým zajatcom počas vojny vyplývajúcich mu z medzinárodných zmlúv,

[1016] Ide najmä o prípady povstaleckých skupín, polovojenských skupín, milícii, či guerill ktoré kontrolujú určité územie.

[1017] Zmyslom uvedenej úpravy je neobmedzenie trestnej zodpovednosti veliteľa iba na *de iure* vojenského veliteľa, ktoré by tak fakticky znemožnilo trestné stíhať väčšinu páchateľov trestných činov vojnových vo vnútroštátnych konfliktoch, ktorí sa dopustili trestných činov v postavení *de facto* veliteľov.

[1018] Napr. BASSIOUNI, M.; CHERIF, M. Introduction to International Criminal Law, Transnational publishers, New York, ISBN: 1-57105-286-0, 2003. ŠTURMA, P. Mezinárodní trestní soud a stíhaní zločinu podle mezinárodního práva, Nakladatelství Karolínum, Praha 2002, ISBN 80-246-0305-5, s. 155. KNOOPS, G. Defenses in contemporary international criminal law, 2nd Edition, Koninklijke Brill NV, Leiden, The Netherlands, 2008, ISBN: 978-1-57105-158-5, s. 33 – 34.

ako napríklad právo na zabezpečenie základných potrieb a nevyhnutnú pomoc na prežitie, právo na spravodlivý proces a pod. [1019]

Z pohľadu zamerania textu tejto kapitoly sa ako ťažiskové ustanovenie javí §432 ods.2, písm. a) TZ, kedy páchateľ kybernetickým útokom najmä na prvky kritickej infraštruktúry ohrozí civilné obyvateľstvo, z pohľadu objektívnej stránky pôjde o veľmi podobné konania **ako pri trestnom čine všeobecného ohrozenia podľa §284 TZ[1020], avšak cielené na civilné o obyvateľstvo na okupovaných územiach v čase vojny, ktoré čiastočne v §432 ods.2, písm. b)** a nasl. už napĺňa i genocidiálny (špeciálny) úmysel.

Ak by páchateľ svojim konaním naplnil skutkovú podstatu vojnového zločinu podľa čl. 8 Rímskeho štatútu[1021], dopustil by sa týmto konaním trestného činu vojnového bezprávia podľa § 433 TZ, ak by takéto konanie nebolo „**dostatočne závažne"** porušenie medzinárodného humanitárneho práva, čím by bola daná pôsobnosť Medzinárodného trestného súdu podľa čl. 5 ods. 1 Rímskeho štatútu.

12.4.4.4Počítačové trestné činy súvisiace s nezákonným obsahom

Ide o skupinu trestných činov, ktorých páchanie spočíva vo vytvorení trestnoprávne relevantného digitálneho obsahu , alebo predstavujú útok na tento digitálny obsah.

Porušovanie autorského práva (§283, ods. 1, ods. 2, písm. d) TZ)[1022]

Objektom tohto trestného činu je nerušený výkon majetkových práv k dielu, umeleckému výkonu, zvukovému záznamu alebo zvukovo-obrazového záznamu,

[1019] Čl. 55 a 59 Ženevského dohovoru o ochrane civilných osôb počas vojny.
[1020] Pozri výklad vyššie.
[1021] Oznámenie Ministerstva zahraničných vecí č. 333/2002 Z. z.
[1022] Ustanovenie §283 TZ znie:
(1) Kto neoprávnene zasiahne do zákonom chránených práv k dielu, umeleckému výkonu, zvukovému záznamu alebo zvukovo-obrazovému záznamu, rozhlasovému vysielaniu alebo televíznemu vysielaniu alebo databáze, potrestá sa odňatím slobody až na jeden rok.
(2) Odňatím slobody až na dva roky sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a. a spôsobí ním väčšiu škodu,
b. závažnejším spôsobom konania,
c. z osobitného motívu, alebo
d. prostredníctvom počítačového systému.
(3) Odňatím slobody na šesť mesiacov až tri roky sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 a spôsobí ním značnú škodu.
(4) Odňatím slobody na jeden rok až päť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a. a spôsobí ním škodu veľkého rozsahu, alebo
b. ako člen nebezpečného zoskupenia.

rozhlasovému vysielaniu alebo televíznemu vysielaniu alebo databáze, teda pred ich neoprávneným užívaním.

Objektívna stránka spočíva v neoprávnenom zásahu do chránených (majetkových) práv k dielu, umeleckému výkonu, zvukovému záznamu alebo zvukovo-obrazovému záznamu, rozhlasovému vysielaniu alebo televíznemu vysielaniu alebo databáze. **Vzhľadom na široko koncipované znenie skutkovej podstaty, naráža na samotnú zásadu *nullum crime sine lege*, nakoľko nie je úplné jednoznačné, aké porušenie autorských práv bude trestné** a aké porušenie autorských práv je priestupkom podľa §32 ods.1, písm. b) zákona č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov. Z pohľadu kybernetickej kriminality pôjde najmä o prípady používania nelicencovaných softwarov, alebo rôzne torrent stránky, pri ktorých všeobecne platí, že osobné použitie obsahu stiahnutého cez torrent nie je trestným činom, avšak jeho komerčné využitie už áno[1023] a to najmä s poukazom na §283 ods. 1, ods. 2, písm.d), **kedy by bol naplnený kvalifikačný znak spáchania trestného činu prostredníctvom počítačového systému.**

Subjekt je všeobecný, preto páchateľom môže byť akákoľvek fyzická osoba. Právnická osoba tento trestný čin nemôže spáchať.

Subjektívna stránka vyžaduje úmyselné zavinenie.

Nebezpečné vyhrážanie (§360 TZ)[1024]

Objektom tohto trestného činu je ochrana medziľudských vzťahov, ako aj riadne občianske spolunažívanie pred prejavmi nenávisti a závažným vyhrážaním, ktoré ohrozuje život a zdravie.

[1023] Napr. Rozsudok Súdny dvor EÚ, C-610/15 vo veci Stichting Brein proti Ziggo BV and XS4ALL Internet BV ('XS4ALL')

[1024] Znenie §360 TZ znie:
(1) Kto sa inému vyhráža smrťou, ťažkou ujmou na zdraví alebo inou ťažkou ujmou takým spôsobom, že to môže vzbudiť dôvodnú obavu, potrestá sa odňatím slobody až na jeden rok.
(2) Odňatím slobody na šesť mesiacov až tri roky sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a. závažnejším spôsobom konania,
b.na chránenej osobe,
c. preto, aby inému zmaril alebo sťažil uplatnenie jeho základných práv a slobôd,
d. z osobitného motívu, alebo
e. verejne.

PRÍKLAD

Na rozdiel od skutkov nebezpečného vyhrážania elektronickou formou konkrétnej osobe je toto konanie typické vyhrážaním sa a prejavmi nenávisti v online priestore, na sociálnych sieťach, diskusných fórach apod., ktoré smerujú jednak voči verejne známej osobe, alebo skupine osôb. Alebo ide o reakciu na iného diskutujúceho. Spoločným menovateľom v tomto prípade je skutočnosť, že páchateľ osobne obeť, alebo obete nemusí poznať a primárnym účelom je šírenie nenávisti a vyhrážanie sa smrťou alebo poškodením zdravia obete pre jej názor alebo stanovisko, vystúpenie, avšak nie z dôvodu rasy, národnosti apod., čo by tento trestný čin zaraďovalo **medzi extrémistické trestné činy v závislosti od obsahu vyhrážky.**[1025]

Práve používanie sociálnych sietí, diskusií pod článkami, blogmi atď. odlišuje toto konanie od individuálneho nebezpečného vyhrážania vzhľadom na mimotrestnú právnu úpravu odstraňovania nezákonného obsahu ktorý sa týka neznášanlivosti k určitej skupine ľudí, popierania holokaustu, detskej pornografie alebo terorizmu podľa ustanovení §152 a nasledujúce Zákona o mediálnych službách[1026]. Na predchádzanie šírenia a odstraňovanie škodlivého [1027]a nezákonného obsahu je potrebné zo strany online platforiem posudzovať a zmierňovať rizík a auditovania. Korektná a efektívna aplikácia týchto inštitútov môže viesť k výraznej zmene v dizajne platforiem, ktorá nebude umožňovať zvýraznenie škodlivého obsahu alebo umožní označovanie takéhoto obsahu či zákaz reklamy takéhoto obsahu. [1028]

Objektívna stránka spočíva v konaní páchateľa, kedy sa inému vyhráža smrťou, ťažkou ujmou na zdraví alebo inou ťažkou ujmou takým spôsobom, že to môže vzbudiť v obeti dôvodnú obavu. Na naplnenie objektívnej stránky sa vyžaduje, aby išlo o závažné protiprávne konania, inak budú takéto konania priestupkami čo je v aplikačnej praxi pomerné náročné rozlíšiť. Vždy sa musia posúdiť všetky okolnosti prípadu, kontext ako aj prostriedky, ktoré páchateľ použil. Ak však pôjde o opakovanie takýchto skutkov, malo by sa to posúdiť ako

[1025] Pozri výklad ďalej.
[1026] § 150 zákona č. 264/2022 Z. z. o mediálnych službách a o zmene a doplnení niektorých zákonov (zákon o mediálnych službách) v znení neskorších predpisov.
[1027] § 12 a nasl. zákona č. 40/2015 Z. z. o audiovízii a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
[1028] MESARČÍK, M. Nástroje verejného práva pre boj s dezinformáciami v online prostredí. 1. vydanie. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2023, ISBN: 978-80-7160-706-9, s. 175.

trestný čin. Na naplnenie skutkovej podstaty stačí, že existuje možnosť vzbudenia dôvodnej obavy a nie, že k dôvodnej obave skutočne aj dôjde.[1029]

Vyhrážanie sa je možné charakterizovať ako aktívne konanie páchateľa, ktorým vyvolá u poškodeného dôvodnú obavu o svoje život alebo zdravie. V tomto prípade je teda obligatórnym znakom objektívnej stránky aj spôsob spáchania trestného činu.. Z hľadiska objektívnej stránky sa teda vyžaduje nielen samotná vyhrážka, ale práve aj spôsobenie dôvodnej obavy, pričom obidva znaky sa musia posudzovať samostatne. [1030]

Subjekt je všeobecný. Páchateľom môže byť každá trestne zodpovedná fyzická ako i právnická osoba.

Subjektívna stránka vyžaduje úmyselné zavinenie. Samotná vyhrážka musí byť mienená vážne, avšak nie z hľadiska úmyslu jej naplnenia, ale z hľadiska úmyslu jej vyslovenia, teda, že ju človek chcel vysloviť a mala pôsobiť ako vyhrážka. Zároveň úmysel musí smerovať k takému spôsobu vyjadrenia vyhrážky, aby bol spôsobilý vyvolať dôvodnú obavu z tejto vyhrážky.[1031]

Šírenie poplašnej správy (§361 TZ)[1032]

Objektom tohto trestného činu je ochrana bezpečnosti a verejného poriadku, riadny chod inštitúcií a organizácií. Nebezpečnosť tohto konania spočíva v šírení strachu, neistoty a paniky.

Objektívna stránka spočíva v hrozbe vážneho znepokojenia aspoň časti obyvateľstva nejakého miesta tým, že rozširuje poplašnú správu, ktorá je nepravdivá, alebo sa dopustí iného obdobného konania spôsobilého vyvolať také nebezpečenstvo (napr. inštalácia atrapy

[1029] STRÉMY, T.; KURILOVSKÁ, L.; REMETA, R. a kol. Trestný zákon - praktický komentár. Wolters Kluwer, Bratislava, ISBN: 978-80-286-0378-6, 2025 s. 1195.
[1030] Ibid.
[1031] Ibid.
[1032] Ustanovenie §361 TZ znie:
(1) Kto úmyselne spôsobí nebezpečenstvo vážneho znepokojenia aspoň časti obyvateľstva nejakého miesta tým, že rozširuje poplašnú správu, ktorá je nepravdivá, alebo sa dopustí iného obdobného konania spôsobilého vyvolať také nebezpečenstvo, potrestá sa odňatím slobody až na dva roky.
(2) Kto správu alebo iné obdobné konanie uvedené v odseku 1, hoci vie, že sú nepravdivé a môžu vyvolať opatrenie vedúce k nebezpečenstvu vážneho znepokojenia aspoň časti obyvateľstva nejakého miesta, oznámi právnickej osobe alebo Policajnému zboru alebo inému štátnemu orgánu alebo hromadnému informačnému prostriedku, potrestá sa odňatím slobody na jeden rok až päť rokov.
(3) Odňatím slobody na tri roky až osem rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 2
a) a už bol za taký čin odsúdený, alebo
b) a spôsobí ním vážnu poruchu v hospodárskej prevádzke alebo hospodárskej činnosti právnickej osobe alebo v činnosti štátneho orgánu alebo iný obzvlášť závažný následok.

nástrahového výbušného systému na určitom mieste, imitácia otravy, spustenie poplašných sirén resp. ich imitácia).

Poplašná správa musí byť nepravdivá správa spôsobilá vyvolať obavy a znepokojenie z nejakých budúcich udalostí

- musí byť nie len poplašná, ale aj nepravdivá
- musí nepriaznivo zasiahnuť do života určitých užívateľov

Pojem vážne znepokojenie, jeho podstata spočíva v presvedčení ohrozenej časti obyvateľstva, resp. skupiny osôb, že skutočne dôjde k realizácii nebezpečenstva s následkom ujmy na životoch, zdraví alebo v spôsobení škody na majetku a pod. Pôjde napríklad o správu, že na určitom mieste sa nachádza nástražný výbušný systém a pod.

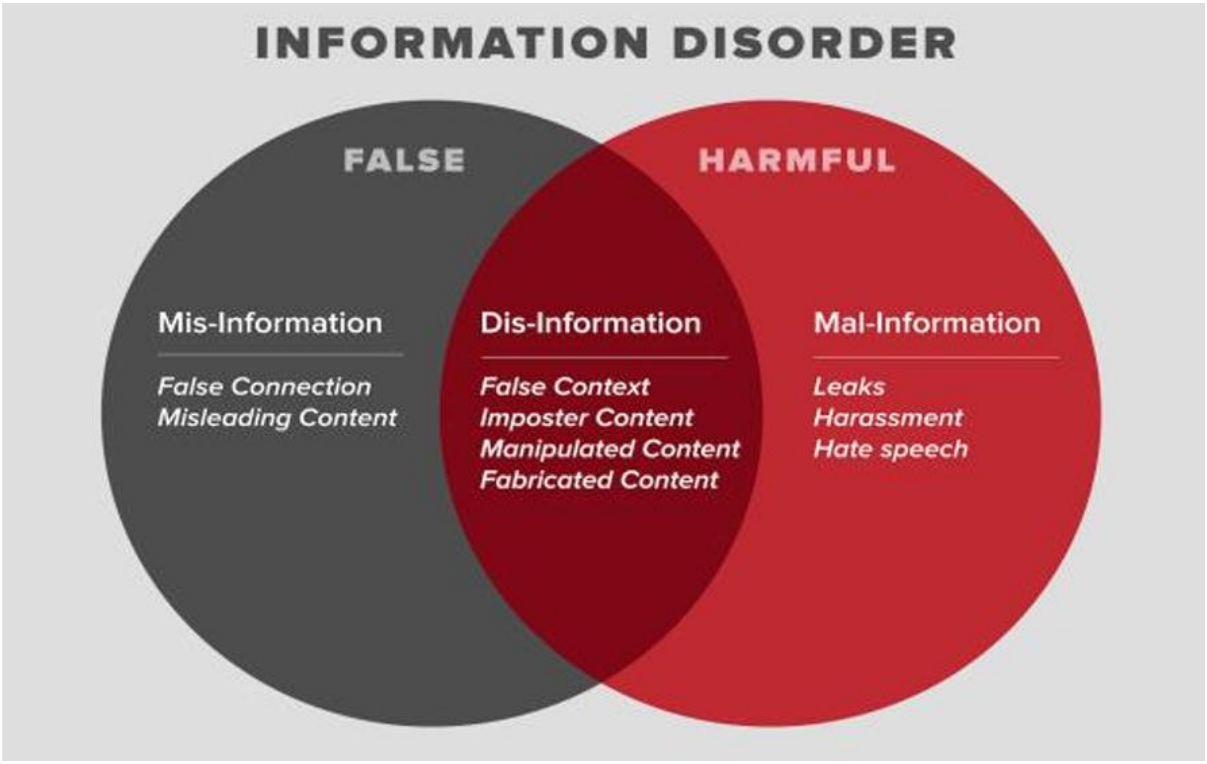
Časťou obyvateľstva nejakého miesta sa rozumie neurčitý, väčší počet osôb. Zákon tento pojem nešpecifikuje, ale kvantita osôb bude určite presahovať počet vyjadrený v pojme „skupina osôb" podľa § 129 ods. 1 TZ alebo v pojme „viaceré osoby" podľa § 127 ods. 12 TZ. Použitie tejto skutkovej podstaty sa najčastejšie objavuje aj v súvislosti s trestným stíhaním dezinformácií.[1033] **I keď neexistuje legálna definícia dezinformácie,** jednu z najpoužívanejších a všeobecne akceptovaných definícií sformulovali **Wardová a Derakhshan** [1034] ako **vedomú nepravdivú informáciu s cieľom poškodiť** osobu, skupinu osôb, organizáciu, alebo krajinu, vrátane súkromných organizácií, obchodných spoločnosti a korporácií.

Subjektívna stránka podľa § 361 ods. 1 vyžaduje úmyselné zavinenie, čo pri preukazovaní šírenia dezinformácií majúcich charakter poplašných správ bude obtiažne dokázať najmä vo vzťahu k dokazovaniu vedomosti o nepravdivosti správy. Zatiaľ neboli zaznamenané prípady, že by sa orgány činné v trestnom konaní snažili dokazovať úmysel pomocou vzdelania osoby šíriacej dezinformáciu (so znakmi poplašnej správy), a súhlasom so

[1033] Keď bol v roku 2021 predstavený legislatívny návrh na doplnenie Trestného zákona skutkovej podstaty trestného činu šírenia nepravdivej informácie a zmenu skutkovej podstaty trestného činu šírenia poplašnej správy, v rámci kritiky a následného vyhodnotenia pripomienok bolo poukazované na to, že trestný čin šírenia poplašnej správy, ako je *de lege lata* uvedený a rozdelený do § 361 a § 362 Trestného zákona, je na postihovanie šírenia najzávažnejších dezinformácií postačujúci. In: ADAMKOVIČ, M. Šírenie poplašnej správy a aplikačné problémy v kontexte súčasného smerovania spoločnosti In: MARKOVÁ, V.; PAULÍČKOVÁ, N. (zost.) Aktuálne otázky trestného práva v teórii a praxi. Zborník príspevkov z 12. roč. interdisciplinárnej celoštátnej vedeckej konferencie s medzinárodnou účasťou. Bratislava: Akadémia Policajného zboru v Bratislave. 2024, s. 24. ISBN 978-80-8293-020-0. Dostupné na: LINK

[1034] WARDLE, C., DERAKSHANB, H. Information Disorder, Council of Europe, Strasbourg, 2017, s. 20.

zmluvnými podmienkami sociálnych sietí – to by sa týkalo samozrejme len tých, ktoré by zakazovali šíriť určitý obsah.[1035]



Obrázok č. 14: Mis-information, Dis-Information, Mal-Information. [1036]

Z doktrinálneho hľadiska má ísť o objektívne nepravdivú správu, kam možno zaradiť podľa Ivora i správu značne skresľujúcu alebo tendenčnú. [1037] Dôležitým z hľadiska dodržania slobody prejavu je tiež rozlišovanie medzi šírením nepravdivého tvrdenia ako faktu, a hodnotiacimi tvrdeniami vrátane kritiky, kedy je potrebné hodnotiť konanie páchateľa z pohľadu charakteru a povahy jeho prejavu, aby bolo odlíšené šírenie poplašnej správy od hodnotenia situácie.[1038]

Subjekt je všeobecný, t.j. páchateľom môže byť každá trestne zodpovedná fyzická osoba.

[1035]ADAMKOVIČ, M. Šírenie poplašnej správy a aplikačné problémy v kontexte súčasného smerovania spoločnosti In: MARKOVÁ, V.; PAULÍČKOVÁ, N. (zost.) Aktuálne otázky trestného práva v teórii a praxi. Zborník príspevkov z 12. roč. interdisciplinárnej celoštátnej vedeckej konferencie s medzinárodnou účasťou. Bratislava: Akadémia Policajného zboru v Bratislave. 2024, s. 26. ISBN 978-80-8293-020-0. Dostupné na: LINK
[1036] WARDLE, C., DERAKSHANB, H,; Information Disorder, Council of Europe, Strasbourg, 2017, s. 20.
[1037] IVOR, I.; POLÁK, P.; ZÁHORA, J. Trestné právo hmotné II. Osobitná časť. 2. vydanie. Bratislava: Wolters Kluwer SR s.r.o., 2021, s. 499. Rovnako aj WARDLE, C., DERAKSHANB, H. Information Disorder, Council of Europe, Strassbourg, 2017, s. 20.
[1038] NSČR 3 Tdo 1031/2021.

Vo vzťahu k šíreniu dezinformácií možno konštatovať, že taktiež ide o škodlivý a v istej časti i nezákonný obsah, na ktoré sa vzťahujú mimo trestné predpisy mediálneho práva ako i vlastné analýzy rizík a implementácia opatrení, ktorými sa riziko publikovania a šírenia dezinformácií musí znižovať.[1039]

Detská pornografia (§368 až 370 TZ)[1040]

Výskyt detskej pornografie, ktorú tvoria snímky zobrazujúce sexuálne zneužívanie detí, a iných zvlášť závažných foriem sexuálneho zneužívania a sexuálneho vykorisťovania detí narastá a rozširuje sa používaním nových technológií a internetu. Detská pornografia, ktorú tvoria snímky zobrazujúce sexuálne zneužívanie detí, je osobitným druhom obsahu, ktorý nemožno prezentovať ako vyjadrenie názoru.[1041] Možnosť nadobudnutia plnoletosti

[1039] Pozri výklad k trestnému činu nebezpečného vyhrážania.

[1040] Ustanovenie § 368 znie:
(1)Kto využije, získa, ponúkne alebo inak zneužije dieťa na výrobu detskej pornografie alebo detského pornografického predstavenia alebo umožní také jeho zneužitie, alebo sa inak podieľa na takejto výrobe, potrestá sa odňatím slobody na štyri roky až desať rokov.
(2)Odňatím slobody na sedem rokov až dvanásť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a)na dieťati mladšom ako dvanásť rokov,
b)závažnejším spôsobom konania,
c)verejne,
d)spoločným konaním najmenej dvoch osôb, alebo
e)a bezprostredne ním ohrozí život dieťaťa.
(3)Odňatím slobody na desať rokov až pätnásť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a)a spôsobí ním ťažkú ujmu na zdraví alebo smrť, alebo
b)a získa ním značný prospech.
(4)Odňatím slobody na dvanásť rokov až dvadsať rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a)a spôsobí ním ťažkú ujmu na zdraví viacerým osobám alebo smrť viacerých osôb,
b)a získa ním prospech veľkého rozsahu, alebo
c)ako člen nebezpečného zoskupenia.

Ustanovenie §369 znie:
(1) Kto rozmnožuje, prepravuje, zadovažuje, sprístupňuje alebo inak rozširuje detskú pornografiu, potrestá sa odňatím slobody na jeden rok až päť rokov.
(2)Odňatím slobody na tri roky až osem rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a)závažnejším spôsobom konania, alebo
b)verejne.
(3)Odňatím slobody na štyri roky až desať rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 a získa ním značný prospech.
(4)Odňatím slobody na sedem rokov až dvanásť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 a získa ním prospech veľkého rozsahu.

Ustanovenie § 370 znie:
(1) Kto prechováva detskú pornografiu alebo kto koná v úmysle získať prístup k detskej pornografii prostredníctvom elektronickej komunikačnej služby, potrestá sa odňatím slobody až na dva roky.
(2) Rovnako ako v odseku 1 sa potrestá, kto sa úmyselne zúčastní detského pornografického predstavenia.

[1041] TURAY, L.; MIHÁLIK, S.; CÁDRA, R.; PETRIČKO, D. a kol. Trestný zákon. Komentár. 1. vydanie. Bratislava: C. H. Beck, 2025, s. 1378.

pred dovŕšením 18 rokov uzavretím manželstva nezakladá dôvodv pre obmedzenie rozsahu trestnoprávnej ochrany dieťaťa v trestnom konaní v zmysle medzinárodných dohovorov.[1042]

Trestné stíhanie sa podľa § 87 ods. 5 TZ premlčí najskôr pätnásť rokov potom, čo osoba, na ktorej bol spáchaný trestný čin výroby detskej pornografie podľa dovŕšila osemnásty rok svojho veku. Trestný čin výroby detskej pornografie je v prvých dvoch odsekoch zločinom, v treťom, štvrtom a piatom odseku obzvlášť závažným zločinom. Trestný čin výroby detskej pornografie podľa § 368 ods. 1 TZ je zločinom a základnou skutkovou podstatou.

Objektom tohto trestného činu je ochrana detí pred ich zneužívaním na výrobu detskej pornografie, ľudská dôstojnosť a telesná integrita dieťaťa.

Hmotným predmetom útoku predmetného trestného činu je dieťa. Dieťaťom sa na účely tohto ustanovenia rozumie osoba mladšia ako osemnásť rokov. Bližšie k tomuto pojmu pozri komentár k § 127 ods. 1 TZ.

Objektívna stránka predmetného trestného činu spočíva vo využití, získaní, ponúknutí alebo v inom zneužití dieťaťa na výrobu detskej pornografie alebo detského pornografického predstavenia alebo v umožnení zneužitia dieťaťa na uvedený účel alebo v inom podieľaní sa na tejto výrobe.

Základná skutková podstata trestného činu výroby detskej pornografie je dokonaná okamihom vyhotovenia detského pornografického diela. Skutočnosť, že páchateľ následne niektoré fotky vymazal, respektíve, že niektoré fotky vymazal okamžite po ich vyhotovení, nemá na posudzovanie tohto trestného činu žiadny vplyv, pretože k vymazaniu došlo až po dokonaní trestného činu. Pokiaľ páchateľ dieťa nepohne k detskej pornografií, ale iba v rozširuje detskú pornografiu alternatívnou formou, a to rozmnožovaním, prepravou, zadovažovaním, sprístupňovaním alebo iným rozširovaním pôjde o trestný čin Rozširovania detskej pornografie podľa §369. TZ S prihliadnutím na formuláciu objektívnej stránky je zrejmé, že nepôjde o jednorazové konania páchateľa, ale o opakovanú činnosť.[1043] Pokiaľ páchateľ iba neoprávnené drží detskú pornografiu po akýkoľvek čas, možno rozumieť neoprávnenú držbu detskej pornografie po akýkoľvek čas alebo vedomé získava prístup k detskej pornografii prostredníctvom informačných a komunikačných technológií, t.j. musí

[1042] STRÉMY, T.; KURILOVSKÁ, L.; REMETA, R. a kol. Trestný zákon - praktický komentár. Wolters Kluwer, Bratislava, ISBN: 978-80-286-0378-6, 2025 s. 1229.
[1043] TURAY, L.; MIHÁLIK, S.; CÁDRA, R.; PETRIČKO, D. a kol. Trestný zákon. Komentár. 1. vydanie. Bratislava: C. H. Beck, 2025, s. 1380.

mať v úmysle navštíviť stránku s detskou pornografiou a zároveň vedieť, že sa na nej nachádzajú príslušné vyobrazenia. V kontexte interpretovaného ustanovenia pôjde o získavanie prístupu k rôznym distribučným kanálom obsahujúcim tento typ nezákonného obsahu, ako sú webové stránky, siete typu peer-to-peer, sociálne siete, diskusné skupiny, IRC (tzn. chat využívajúci decentralizovaný komunikačný protokol), platformy na zdieľanie obsahu a pod.[1044]- pôjde o trestný čin Prechovávania detskej pornografie podľa §370 TZ.

Detskou pornografiou sa na účely TZ rozumie zobrazenie skutočnej alebo predstieranej súlože, iného spôsobu pohlavného styku alebo iného obdobného sexuálneho styku s dieťaťom alebo osobou vyzerajúcou ako dieťa alebo zobrazenie obnažených častí tela dieťaťa alebo osoby vyzerajúcej ako dieťa určené na sexuálne účely resp. za účelom vyvolania vzrušenia a sexuálneho uspokojenia, táto skutočnosť je predmetom dokazovania.[1045] K predmetnému pojmu pozri komentár k § 132 ods. 4 TZ.

Detským pornografickým predstavením sa na účely TZ rozumie živé predstavenie určené publiku, a to aj s využitím informačno-technických prostriedkov, v ktorom je dieťa zapojené do skutočného alebo predstieraného sexuálneho konania alebo v ktorom sú obnažované časti tela dieťaťa určené na sexuálne účely. K predmetnému pojmu pozri komentár k § 132 ods. 5 TZ.

Dieťaťom sa na účely Trestného zákona rozumie osoba mladšia ako osemnásť rokov, pričom skúmanie veku dieťaťa má právny význam pre aplikáciu kvalifikovanej skutkovej podstaty tohto trestného činu podľa § 368 ods. 2 písm. a) TZ.

Jednočinný súbeh trestných činov sexuálneho zneužívania podľa § 201 TZ a výroby detskej pornografie podľa § 368 TZ nie je vylúčený, pretože trestný čin sexuálneho zneužívania postihuje obsah konania páchateľa a trestný čin výroby detskej pornografie postihuje zaznamenávanie obsahu konania páchateľa. Pri trestnom čine výroby detskej pornografie podľa § 368 TZ je bez významu, či boli spáchané dobrovoľne (t. j. so súhlasom maloletého), nakoľko takéto konanie trestnoprávne postihuje, a to bez ohľadu na mienku maloletého poškodeného.

Subjekt je všeobecný, takže páchateľom môže byť ktorákoľvek trestne zodpovedná fyzická osoba, ktorá spĺňa podmienky trestnej zodpovednosti. Tohto trestného činu sa môže

[1044] TURAY, L.; MIHÁLIK, S.; CÁDRA, R.; PETRIČKO, D. a kol. Trestný zákon. Komentár. 1. vydanie. Bratislava: C. H. Beck, 2025, s. 1380 - 1381.
[1045] Napr. KS TT 6T0/45/2019

dopustiť aj právnická osoba v zmysle § 3 TZPO. Za páchateľa zločinu výroby detskej pornografie je nevyhnutné považovať aj výrobcu detskej pornografie " v súkromí" a pre vlastné účely, t. j. bez podmienky jej ďalšieho šírenia[1046]

Subjektívna stránka spočíva v úmyselnom zavinení páchateľa vzhľadom na § 17 TZ, a teda páchateľ musí mať nielen vedomosť o tom, že jeho konanie je protiprávne, ale minimálne musí byť uzrozumený s tým, že svojím konaním spôsobuje následok predpokladaný predmetnou skutkovou podstatou.

Založenie, podpora a propagácia hnutia smerujúceho k potláčaniu základných práv a slobôd (§421 TZ)[1047], Prejav sympatie k hnutiu smerujúcemu k potláčaniu základných práv a slobôd (§422 TZ)[1048], Výroba, rozširovanie a prechovávanie extrémistického materiálu (§422a až 422c TZ), [1049]Popieranie a schvaľovanie holokaustu, zločinov

[1046] NSSR 2 Tdo 8/2015

[1047]Ustanovenie §421 TZ znie:

(1) Kto založí, podporuje alebo propaguje skupinu, hnutie alebo ideológiu, ktorá smeruje k potlačeniu základných práv a slobôd osôb, alebo ktoré hlása rasovú, etnickú, národnostnú alebo náboženskú nenávisť alebo kto propaguje skupinu, hnutie alebo ideológiu, ktorá v minulosti smerovala k potlačeniu základných práv a slobôd osôb, potrestá sa odňatím slobody na jeden rok až päť rokov.

(2) Odňatím slobody na štyri roky až osem rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1

a. verejne alebo na mieste verejnosti prístupnom,
b. závažnejším spôsobom konania, alebo
c. za krízovej situácie.

[1048] Ustanovenie §422 TZ znie:

(1) Kto verejne alebo na mieste verejnosti prístupnom, najmä používaním zástav, odznakov, rovnošiat alebo hesiel, prejavuje sympatie k skupine, hnutiu alebo ideológii, ktorá smeruje alebo v minulosti smerovala k potlačeniu základných práv a slobôd osôb, alebo ktorá hlása rasovú, etnickú, národnostnú, náboženskú nenávisť, potrestá sa odňatím slobody na šesť mesiacov až tri roky.

(2) Rovnako ako v odseku 1 sa potrestá, kto pri čine uvedenom v odseku 1 používa pozmenené zástavy, odznaky, rovnošaty alebo heslá, ktoré vyvolávajú zdanie pravých.

[1049] § 422a Výroba extrémistického materiálu

(1)Kto vyrába extrémistický materiál alebo sa podieľa na takejto výrobe, potrestá sa odňatím slobody na tri roky až šesť rokov.

(2) Odňatím slobody na štyri roky až osem rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1

a) závažnejším spôsobom konania, alebo
b) ako člen extrémistickej skupiny.

§ 422b Rozširovanie extrémistického materiálu

(1)Kto rozmnožuje, prepravuje, zadovažuje, sprístupňuje, uvádza do obehu, dováža, vyváža, ponúka, predáva, zasiela alebo rozširuje extrémistický materiál, potrestá sa odňatím slobody na jeden rok až päť rokov.

(2) Odňatím slobody na tri roky až osem rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1

a) závažnejším spôsobom konania,
b) verejne, alebo
c) ako člen extrémistickej skupiny.

§ 422c
Prechovávanie extrémistického materiálu

politických režimov a zločinov proti ľudskosti (§422d TZ)[1050], Hanobenie národa, rasy a presvedčenia (§423 TZ)[1051], Podnecovanie k národnostnej, rasovej a etnickej nenávisti (§424 TZ)[1052]

Špecifikom trestných činov extrémizmu podľa §140a TZ, je že zároveň uvedené trestné činy, ako jediné z 12 hlavy osobitnej časti podliehajú premlčaniu trestného stíhania v zmysle § 88 TZ a premlčaniu výkonu trestu podľa §91 TZ.

Nenávisť je dlhodobá, hlboká, intenzívna negatívna emócia vyjadrujúca zaujatosť, nepriateľstvo a odpor voči inej osobe, skupine alebo objektu. Nenávisť sa spája s potrebou škodiť a spôsobovať bolesť. Spája sa tiež s pocitom radosti, keď k naplneniu tejto potreby dôjde. **Nenávistný prejav (hate speech)** je možné chápať ako verejný písomný, verbálny, grafický, zvukový alebo audiovizuálny prejav, ktorý podnecuje, rozširuje, propaguje,

---

Kto prechováva extrémistický materiál, potrestá sa odňatím slobody až na dva rok

[1050] Ustanovenie §422d TZ znie:
(1) Kto verejne popiera, spochybňuje, schvaľuje alebo sa snaží ospravedlniť holokaust, zločiny režimu založeného na fašistickej ideológii, zločiny režimu založeného na komunistickej ideológii alebo zločiny iného podobného hnutia, ktoré násilím, hrozbou násilia alebo hrozbou inej ťažkej ujmy smeruje k potlačeniu základných práv a slobôd osôb, potrestá sa odňatím slobody na šesť mesiacov až tri roky.
(2) Rovnako ako v odseku 1 sa potrestá, kto verejne popiera, schvaľuje, spochybňuje, hrubo zľahčuje alebo sa snaží ospravedlniť genocídium, zločiny proti mieru, zločiny proti ľudskosti alebo vojnové zločiny spôsobom, ktorý môže podnecovať násilie alebo nenávisť voči skupine osôb alebo jej členovi, ak bol páchateľ alebo účastník tohto činu odsúdený právoplatným rozsudkom medzinárodného súdu zriadeného na základe medzinárodného práva verejného, ktorého právomoc uznala Slovenská republika, alebo právoplatným rozsudkom súdu Slovenskej republiky.
[1051] Ustanovenie §423 TZ znie:
(1) Kto verejne hanobí
a. niektorý národ, jeho jazyk, niektorú rasu alebo etnickú skupinu, alebo
b. skupinu osôb alebo jednotlivca pre ich skutočnú alebo domnelú príslušnosť k niektorej rase, národu, národnosti, etnickej skupine, pre ich skutočný alebo domnelý pôvod, farbu pleti, náboženské vyznanie alebo preto, že sú bez vyznania,
potrestá sa odňatím slobody na jeden rok až tri roky.
(2) Odňatím slobody na dva roky až päť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a. ako člen extrémistickej skupiny,
b. ako verejný činiteľ, alebo
c. z osobitného motívu.
[1052]Ustanovenie §424 TZ znie:
(1) Kto verejne podnecuje k násiliu alebo nenávisti voči skupine osôb alebo jednotlivcovi pre ich skutočnú alebo domnelú príslušnosť k niektorej rase, národu, národnosti, etnickej skupine, pre ich skutočný alebo domnelý pôvod, farbu pleti, sexuálnu orientáciu, náboženské vyznanie alebo preto, že sú bez vyznania, alebo verejne podnecuje k obmedzovaniu ich práv a slobôd, potrestá sa odňatím slobody až na tri roky.
(2) Rovnako ako v odseku 1 sa potrestá, kto sa spolčí alebo zhromaždí na spáchanie činu uvedeného v odseku 1.
(3) Odňatím slobody na dva roky až šesť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 alebo 2
a. z osobitného motívu,
b. ako verejný činiteľ,
c. ako člen extrémistickej skupiny, alebo
d. za krízovej situácie.

ospravedlňuje nenávisť voči jednotlivcom alebo skupinám osôb pre ich pohlavie, národnosť, jazyk, náboženstvo, rasu, etnickú príslušnosť, farbu pleti, pôvod, sexuálnu orientáciu. Najčastejšie má formu buď hanobenia – verejným šírením výrokov, obrázkov či videí s urážlivým, hrubo osočujúcim obsahom voči skupine osôb, alebo podnecovania k nenávisti – verejným šírením výrokov, obrázkov, videí, výziev vzbudzujúcich nenávisť a podnecujúcich násilie voči určitým skupinám osôb. Nenávistné prvky takéhoto prejavu sú založené na negatívnych predsudkoch hovorcu voči určitým skupinám alebo jednotlivcom v spoločnosti, ktoré vo svojich vyjadreniach uráža, napáda, ponižuje, vyzýva k obmedzeniu ich práv alebo k násilným činom voči nim či inak pošliapava ich ľudskú dôstojnosť. Samotné podnecovanie k nenávisti preto aj z trestnoprávneho hľadiska nevyhnutne nevyžaduje výzvu na násilie.

Druhovým objektom týchto trestných činov je ochrana základných práv a slobôd, rovnoprávnosť ľudí bez ohľadu na ich národnú, etnickú, rasovú, náboženskú alebo inú príslušnosť, farbu pleti, či sexuálnu orientáciu.

Objektívna stránka trestného činu podnecovania k národnostnej, rasovej a etnickej nenávisti podľa § 424 TZ spočíva z pohľadu kybernetickej kriminality vo verejnom prejave (spravidla na sociálnych sieťach, videách, online platformách[1053]) páchateľa, ktorým buď:
a) podnecuje iné osoby, a to alternatívne alebo súčasne, k násiliu alebo nenávisti vo vzťahu ku skupine osôb alebo jednotlivcovi, a to z dôvodu ich skutočnej, alebo z hľadiska páchateľa domnelej príslušnosti k niektorej rase, národu, národnosti, etnickej skupine, ich skutočného, alebo z hľadiska páchateľa domnelého pôvodu, farby pleti, sexuálnej orientácie, náboženského vyznania alebo preto, že sú bez vyznania, alebo
b) podnecuje (najmä verbálne a neverbálne, video, držaním transparentu) k obmedzovaniu práv a slobôd skupiny osôb alebo jednotlivcov.

Podporou takéhoto hnutia sa ma na mysli jednak podpora materiálna (poskytnutie finančných darov, technických prostriedkov, platforiem apod.) alebo morálnu (získavanie priaznivcov, písanie blogov, uverejňovaním príspevkov, natáčanie videi a letáky apod.)

Propagácia takého hnutia môže byť uskutočňovaná otvorené, ale taktiež skryte.

Pri skúmaní trestností takéhoto hnutia je nutné vždy vychádzať z toho, k čomu smeruje uvedená skupina alebo hnutie, či čo hlása resp. akým spôsob zamýšľa, alebo obmedzuje základné práva a slobody iných, alebo ktoré hlása rasovú, etnickú, národnostnú

[1053] Napr. 4chan alebo 8chan.

alebo náboženskú nenávisť a nie iba z názvu takého hnutia či skupiny. skupiny, hnutia alebo ideológie, ktorá smeruje k potlačeniu. Práve v tomto znaku objektívnej stránky **sa tento trestný čin líši od ustanovenia §424 TZ, pretože vyžaduje podporu a propagáciu existujúcich (už založených) hnutí a skupín,** na rozdiel od ustanovenia §424 TZ, ktorého objektívna stránka spočíva v podpore, propagácií násilia, šírenia násilia voči konkrétnej skupiny osôb (obetí) pre ich etnickú, rasovú, náboženskú, národnú atď. príslušnosť a nepropaguje sa už existujúca skupina alebo hnutie, tak ako je to v ustanovení §421 a §422 TZ. Z pohľadu zameranie publikácie pôjde spravidla o šírenie nenávisti a prejavov neznášanlivosti prostredníctvom sociálnych sietí, aplikácií, blogov, podcastov, či videi voči určitej skupine osôb. Pokiaľ **páchateľ nevyzýva k násiliu na skupine obyvateľstva**, ale **takúto skupinu obyvateľov verejne uráža, ponižuje**[1054], pôjde o trestný čin Hanobenie národa, rasy a presvedčenia podľa §423 TZ.

Podľa §122 ods. 2 písm. a) a b) TZ **je trestný čin je spáchaný verejne, ak je spáchaný**

a. obsahom tlačoviny alebo rozširovaním spisu, filmom, rozhlasom, televíziou, použitím počítačovej siete alebo iným obdobne účinným spôsobom, alebo
b. pred viac ako dvoma súčasne prítomnými osobami.

Podnecovaním (resp. podnecovaním k násiliu) sa rozumie vážne mienený prejav páchateľa určený tretím osobám, ktorým páchateľ zamýšľa vyvolať u týchto osôb náladu, správanie alebo rozhodnutie smerujúce k násiliu, nenávisti alebo obmedzovaniu práva slobôd určitej skupiny osôb alebo jednotlivca, pritom nezáleží na forme tohto prejavu (video, písomná[1055] a pod.), pričom podnecovanie

Trestnosť skutku podľa §422 TZ, ktorý je v pomere špeciality k ustanoveniu §421 TZ, spočíva v špecifickej forme podpory a propagácie používaním tzv. extrémistických symbolov, znakov, kombinácií čísel ako akronymov písmen, pozdravov a rovnošiat apod.

Výrobou extrémistického materiálu v zmysle §422a TZ sa rozumie vytvorenie extrémistického materiálu, najmä natočením videa, spísaním manifestu apod. Je vylúčený jednočinný súbeh s prechovávaním extrémistického materiálu. **Rozširovaním extrémistického materiálu sa rozumie podľa §422b TZ** rozmnožovanie, preprava, sprístupňuje, uvádzanie do obehu, dovoz, vývoz, ponuka, zasielanie, pričom objektívna stránka naznačuje, že môže ísť aj o **rozširovanie za odplatu,** pričom nie je rozhodujúce pre

[1054] Napr., že v určitej európskej krajine vládnu fašisti, že určité etnikum predstavuje „špinavé opice" apod.
[1055] Uznesenie Najvyššieho súdu ČR z 25. júna 2014, sp. zn. 3 Tcu 33/2014.

túto skutkovú podstatu, či sa tak deje verejne alebo nie. Prechovávaním extrémistického materiálu podľa §422c TZ znamená ukladanie, zhromažďovanie takéhoto materiálu, najmä scany textov, manifestov, videi, skladieb., prejavov apod.

PRÍKLAD

Z kriminologického pohľadu možno badať posun u páchateľov extrémistických trestných činov od prvoplánovej podpory, šírenia a propagácie extrémistických hnutí a potláčania práv určitej skupiny osôb do sofistikovanej polohy strážcov slobody prejavu a bojovníkov za slobodné prezentovanie vlastných názorov, čo v spoločnosti prispieva k nebezpečnej normalizácií a zakotveniu týchto „odlišných" názorov ako plnohodnotných spoločenských tém, ktoré vedú k radikalizmami a rozpolteniu danej spoločnosti. V tejto súvislosti ide najmä **o názory prostredníctvom blogov, testamentov, videí, podcastov verejne popierajúce holokaust, zločiny komunizmu (zjednodušene tzv. jáchymovská lož) podľa §422d ods. 1 TZ, alebo genocídu, zločiny proti ľudskosti či vojnové zločiny, ak bol ich páchateľ odsúdený medzinárodným trestným súdom podľa §422d ods. 2 TZ.**

Zo subjektívnej stránky vyžadujú všetky trestné činy úmyselné zavinenie.

Subjektom týchto trestných činov môže byť každá trestne zodpovedná fyzická ale i právnická osoba.

12.5 Procesnoprávne aspekty kybernetickej kriminality

Lacuna intra legem v hmotnoprávnej úprave vyúsťuje nepochybne v prospech páchateľov, avšak následky medzier v trestnom práve procesnom sa prejavujú v porušení ľudských práv a základných slobôd, a to najmä procesných práv ústrednej postavy trestného konania, ktorou je obvinený. Nasledujúce state sú preto venované súčasnej právnej úprave procesnej stránky kybernetickej kriminality, ako aj identifikácii jej nedostatkov, ktoré spolupôsobia ako nežiaduce faktory brániace naplneniu zmyslu a účelu trestného konania.

12.5.1 Vecná a miestna príslušnosť na trestné stíhanie počítačových trestných činov

Vzhľadom na rýchly rozvoj prostriedkov IKT s čoraz rafinovanejšími metódami, ako aj s prihliadnutím na zložitosť kybernetickej kriminality je mimoriadne dôležitý vysoký stupeň špecializácie odborníkov pracujúcich v tejto oblasti. V záverečnej správe týkajúcej sa

vykonávania a uplatňovania európskych politík v oblasti predchádzania počítačovej kriminalite a boja proti nej vypracovanej Pracovnou skupinou pre všeobecné záležitosti vrátane hodnotenia (GENVAL)[1056] ešte z roku 2017 sa uvádza, že úroveň špecializácie je v rámci členských štátov Európskej únie dostatočná alebo uspokojivá, pokiaľ ide o orgány presadzovania, ale priestor na zlepšenie existuje v justičnom sektore, keďže v niekoľkých členských štátoch sa počítačovou kriminalitou zaoberajú všeobecné prokuratúry a všeobecné trestné súdy, čo je napokon i prípad Slovenskej republiky.

Orgány činné v trestnom konaní a súdy sa po začatí trestného stíhania zhosťujú neľahkej úlohy spočívajúcej v preukázaní skutočností uvedených v ustanovení § 119 TP, ktoré povedú najmä k zisteniu osoby, ktorá trestný čin spáchala, čo je v prípadoch kybernetickej kriminality ešte niekoľkonásobne sťažené charakterom tejto trestnej činnosti. Trestné stíhanie možno začať v zmysle ustanovenia § 199 ods. 1 tretia veta TP vykonaním neodkladného, neopakovateľného či zaisťovacieho úkonu. Druhým spôsobom je začatie trestného stíhania na podklade podaného trestného oznámenia, a to za súčasného naplnenia predpokladu, že nie je možné vydať jedno z rozhodnutí podľa ustanovení § 197 ods. 1, ods. 2 TP. Podnety, na podklade ktorých možno začať trestné stíhanie prichádzajú v prípadoch kybernetickej kriminality od rôznych oznamovateľov, napríklad od príslušníkov spravodajských služieb, Národného bezpečnostného úradu až po jednotky pre riešenie kybernetických bezpečnostných incidentov. Oznámenia o skutočnostiach nasvedčujúcich tomu, že bol spáchaný trestný čin však prichádzajú najčastejšie od samotných poškodených fyzických osôb alebo právnických osôb. V zmysle ustanovenia § 196 ods. 1 prvá veta TP je trestné oznámenie povinný prijať každý prokurátor alebo policajt, čo je zdôraznené aj zásadou legality, podľa ktorej je prokurátor povinný stíhať všetky trestné činy, o ktorých sa dozvedel.

PRÍKLAD
S výnimkou Špecializovaného trestného súdu a Úradu boja s organizovanou kriminalitou ako organizačnej zložky Prezídia Policajného zboru Slovenskej republiky neexistuje orgán,

[1056] Jednotná akcia 97/827/SVV prijatá Radou na základe článku K.3 Zmluvy o Európskej únii, ktorou sa stanovuje mechanizmus na hodnotenie uplatňovania a vykonávania medzinárodných záväzkov v boji proti organizovanému zločinu na národnej úrovni (Ú. v. EÚ L 344, 15.12.1997). Dostupné na: LINK

ktorý by na seba atrahoval osobitnú príslušnosť vo vzťahu k stíhaniu a prejednávaniu iných trestných činov ako tých v ustanovení § 14 Trestného poriadku.

Z uvedeného ustanovenia je zrejmé, že do taxatívneho výpočtu trestných činov § 14 TP nepojal ani počítačové trestné činy podľa Trestného zákona, to znamená, že určenie vecnej príslušnosti súdu, ktorý o nich bude konať, sa spravuje ustanoveniami § 15 a nasl. TP. Keďže Trestný poriadok stanovuje pravidlo, že príslušnosť súdu je smerodajná aj pre určenie príslušnosti orgánu činného v trestnom konaní, vyšetrovanie, resp. skrátené vyšetrovanie, prípadne osobitne skrátené vyšetrovanie počítačových trestných činov vykonáva policajt služobne zaradený na okresnom, resp. krajskom riaditeľstve Policajného zboru.

A tu sa dostávame k základnému „kameňu úrazu." Keďže počítačové trestné činy podľa Trestného zákona sú v prvých odsekoch prečinmi, vykoná sa o nich skrátené vyšetrovanie v zmysle ustanovenia § 202 TP. Berúc do úvahy trestnú sadzbu, ktorá ani pri jednom z nich v základnej skutkovej podstate neprevyšuje tri roky, skrátené vyšetrovanie vykonáva policajt podľa ustanovení § 10 ods. 8 písm. d) až h) TP, teda poverený príslušník. S ohľadom na lehotu pripadajúcu na vykonanie skráteného vyšetrovania o počítačových trestných činoch, ktorá je dva mesiace a plynie od momentu vznesenia obvinenia konkrétnej osobe, ako aj s ohľadom na určitú okliešteno sť rozsahu úkonov, ktoré sa v rámci skráteného vyšetrovania majú vykonať, sa domnievame, že v prípadoch tak sofistikovanej a latentnej trestnej činnosti by malo dôjsť zo strany prokurátora k nariadeniu vyšetrovania *en bloc*.

Naznačené riešenie však treba ponímať ako dočasné, z dlhodobého horizontu by stálo za úvahu vytvoriť na každom okresnom a krajskom riaditeľstve Policajného zboru oddelenie vyšetrovania špecializované na počítačovú kriminalitu, resp. zaradiť tento druh trestnej činnosti do výberovej príslušnosti Úradu boja s organizovanou kriminalitou alebo vytvoriť úplne novú inštitúciu, ktorá by sa zameriavala výlučne na boj s kybernetickou kriminalitou. Obdobne tomu bolo napríklad pri zriadení Kriminálneho úradu Finančnej správy Slovenskej republiky, do pôsobnosti ktorého prešlo vyšetrovanie a skrátené vyšetrovanie trestných činov spáchaných v súvislosti s porušením daňových predpisov v oblasti dane z pridanej hodnoty pri dovoze a spotrebných daní alebo colných predpisov.

Zároveň však treba spomenúť, že za ostatné roky smerovali snahy v boji proti tejto trestnej činnosti aspoň k vytvoreniu samostatného špecializovaného odboru počítačovej kriminality v rámci štruktúry Prezídia Policajného zboru v roku 2013, od roku 2022 v rámci

Národnej centrály osobitných druhov kriminality, ktorú však medzičasom zasiahli významné organizačné zmeny.

12.5.2 Zaisťovanie kryptoaktív

Ak sa pri vyšetrovaní trestných činov zistia skutočnosti, ktoré nasvedčujú tomu, že kryptoaktívum je nástrojom trestnej činnosti alebo je výnosom z trestnej činnosti, je nevyhnutné pre úspešné zabezpečenie účelu trestného stíhania pozastaviť právo nakladať s kryptoaktívom tak, aby mohla byť predmetom sankcie postihujúcej majetok, ktorou sa tento výnos odčerpá. Právna úprava zaisťovania kryptoaktív je upravená v § 96d TP.

PRÍKLAD

Keďže je kryptoaktívum počítačovým údajom s objektívnou hospodárskou hodnotou, uvedený príkaz vychádza z § 91 TP, avšak odlišuje sa čo do účelu zaistenia, ktorým je odčerpanie výnosu. Kryptoaktíva sa spájajú s výnosmi z trestnej činnosti postupom tzv. trasovania, ktoré analyzujú samotnú transakciu zapísanú v príslušnom blockchaine, znaky ostatných transakcií zapísaných v peňaženke z pohľadu času, objemu, hodnoty, adresy odosielateľa, adresy prijímateľa atď. Príslušné analytické nástroje na tieto analýzy sú komerčne dostupné, avšak v zmysle posledného vývoja, by takéto stotožnenie peňaženky obsahujúcej výnos malo byť založené na vysvetliteľnom spätnom dohľadaní a reťazení entít (tzv. chain of custody) založenej spravidla. na *cost-spend* analýze[1057] alebo inej heuristickej metóde.[1058]

Zaistenie kryptoaktív neobsahuje základnú lehotu zaistenia, tak ako je to pri väzbe a trvá až do okamihu právoplatného skončenia trestného konania a prípadného rozhodnutia o zaistenej nehnuteľnosti alebo až do okamihu, kedy pominú dôvody zaistenia, najviac však na päť rokov s možnosťou predĺženia o 7 mesiacov, a to aj opakovane.[1059] Kryptoaktívum je

[1057] US District Court of Columbia, US v. Roman Sterlingov, case n. 21-399. Dostupné dňa 19.12.2025 na: LINK
[1058] Spôsob riešenia problémov, resp. vedeckej činnosti nevychádzajúci z hypotéz a nepoužívajúci príslušné algoritmy, ale používajúci skrátený, „objaviteľský" postup, teda spravidla začínajúci hrubým odhadom, ktorý sa postupne spresňuje In: CHALUPA, B. HEURISTICKÉ ŘEŠENÍ PROBLÉMU SE ZŘETELEM KE KOMPLEXNOSTI ODPOVĚDI, Sborník prací Filozofické fakulty brněnské univerzity. I, Řada pedagogicko-psychologická. 1988, vol. 37, iss. I23, pp. [41]-5, dostupné na: LINK
[1059] § 98a ods. 4 TP.

možné zaistiť aj ako **náhradnú hodnotu,**[1060] náležitosti príkazu na zaistenie náhradnej hodnoty vo forme kryptoaktíva sa spravujú ustanovením § 96d TP.

Samotný pojem kryptoaktíva je definovaný **v § 131 ods. 7 TZ ako platobný prostriedok. Komplexnú definíciu** poskytuje Nariadenie MiCA[1061] ako **digitálne vyjadrenie hodnoty alebo práva, ktoré možno prevádzať a elektronicky uchovávať použitím technológie distribuovanej databázy transakcií alebo podobnej technológie.**[1062]

Príkaz na zaistenie virtuálnej meny vydáva predseda senátu alebo prokurátor v prípravnom konaní. Taktiež tieto orgány sú oprávnené vydať príkaz na zrušenie zaistenia.[1063]**Ak sa bude virtuálna mena zaisťovať v rámci inštitútu prehliadok podľa § 99 a nasl. TP, nie je podľa nás potrebné vo veci vydávať samostatný príkaz na zaistenie virtuálnej meny.**[1064] Ak vec neznesie odklad príkaz na zaistenie kryptoaktíva, ktorý vydal prokurátor, musí najneskôr do 48 hodín potvrdiť sudca pre prípravné konanie pod sankciou neplatnosti. Pokiaľ v stanovenej lehote príkaz nebol potvrdený alebo sudca pre prípravné konanie takýto súhlas neudelil, príkaz stráca platnosť.[1065]

Príkaz na zaistenie kryptoaktív okrem všeobecných náležitostí príkazu obsahuje zákaz akejkoľvek dispozície s kryptoaktívom a prikáže sa jeho vydanie vrátane vydania hesla, prístupového kódu alebo podobných údajov umožňujúcich nakladanie s kryptoaktívom, adresa úložiska kryptoaktíva orgánu, ktorý ju bude spravovať po zaistení, označenie kryptoaktíva a počet jednotiek. Príkaz musí byť vydaný písomne a musí byť odôvodnený. Právne úkony urobené v rozpore so zákazom uvedeným v príkaze sú neplatné.[1066]

Príkaz na zaistenie kryptoaktíva sa doručuje vlastníkovi alebo **osobe, o ktorej možno dôvodne predpokladať, že má prístupové údaje ku kryptoaktívu**. [1067]Vzhľadom na skutočnosť, že kryptoaktíva poskytujú vysokú mieru anonymity, v praxi dochádza k zaisťovaniu kryptoaktív u osôb, ktoré nimi v čase zaistenia disponujú, t. j. majú prístupové údaje k tzv. peňaženke.

[1060] § 96f TP.
[1061] Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1114 z 31. mája 2023 o trhoch s kryptoaktívami a o zmene nariadení (EÚ) č. 1093/2010 a (EÚ) č. 1095/2010 a smerníc 2013/36/EÚ a (EÚ) 2019/1937 (Ú. v. L 150/40, 9.6.2023) („*nariadenie MiCA*").
[1062] Čl. 3 bod 5 nariadenia MiCA.
[1063] § 96d ods. 1 TP.
[1064] K tomu pozri napr. R 47/2017.
[1065] § 96d ods. 2 TP.
[1066] § 96d ods. 3, ods. 6 TP.
[1067] § 96d ods. 4 TP.

Uvedený výklad sa rovnako použije na doručovanie príkazu na zrušenie zaistenia alebo príkazu, ktorým sa zaistenie obmedzí.

Vlastník virtuálnej meny má právo kedykoľvek v priebehu trestného konania žiadať o preskúmanie zaistenia, resp. žiadať jeho zrušenie alebo obmedzenie. O žiadosti rozhoduje bezodkladne predseda senátu a v prípravnom konaní prokurátor uznesením, proti ktorému je prípustná sťažnosť.[1068] Pokiaľ bola žiadosť dotknutej osoby zamietnutá a dôvody žiadosti sa nezmenili, svoju žiadosť môže opakovať až po uplynutí 30 dní od nadobudnutia právoplatnosti uznesenia o zamietnutí žiadosti; inak sa o žiadosti nekoná. [1069]**Ustanovenia o zaistení kryptoaktíva sa primerane použijú aj na zabezpečenie nároku poškodeného na náhradu škody,**[1070] čím sa zvýrazňuje jeho postavenie v trestnom konaní, posilňujú sa jeho práva a vytvárajú lepšie predpoklady pre rýchle uspokojenie jeho nárokov.

12.5.3 Elektronické dôkazy

Dokazovanie tvorí kľúčovú a neodmysliteľnú zložku trestného konania, pretože na podklade výsledkov vykonaného dokazovania súd rozhoduje o vine, respektíve nevine osoby obvinenej z trestného činu. Hoci pojem dokazovanie nemá v Trestnom poriadku zakotvenú legálnu definíciu, možno ním rozumieť zákonom upravený postup subjektov trestného konania (orgánov činných v trestnom konaní, súdu, obvineného, poškodeného, zúčastnenej osoby atď.), ktorého účelom je vyhľadať, zabezpečiť, vykonávať a zhodnotiť informácie dôležité pre poznanie skutkových okolností, na základe ktorých sa v trestnom konaní rozhoduje najmä o vine a treste obvineného, ale aj o ďalších právne relevantných skutočnostiach (napr. o nároku poškodeného na náhradu škody).[1071]

Vzhľadom na to, že slovenské trestné právo procesné je vybudované na obžalovacej zásade (bez žalobcu niet sudcu), súd na seba nepreberá úlohu vyšetrovateľa, čo je charakteristické pre inkvizičný princíp. Súd koná výlučne na podklade prokurátorom podanej obžaloby, resp. návrhu na schválenie dohody o vine a treste, ktoré predstavujú sumár výsledkov prípravného konania, a ktoré zároveň dostatočne odôvodňujú skutočnosť, že obvineného treba postaviť pred súd. Dokazovanie je však prítomné počas celého trestného konania, pričom jeho rozsah je determinovaný konkrétnym štádiom trestného konania tak,

[1068] § 96d ods. 7 TP.
[1069] § 96d ods. 7 TP.
[1070] § 96d ods. 8 TP.
[1071] ČENTÉŠ, J. a kol.: Trestné právo procesné. Všeobecná časť. Šamorín : Heuréka, 2016, s. 328.

aby došlo k naplneniu účelu dokazovania, teda k zisteniu skutkového stavu, o ktorom nie sú dôvodné pochybnosti v rozsahu nevyhnutnom na rozhodnutie.

Všeobecná právna úprava dokazovania v trestnom konaní je obsiahnutá v šiestej hlave prvej časti Trestného poriadku v ustanoveniach § 119 a nasl. TP. Osobitná úprava dokazovania na hlavnom pojednávaní upravená v treťom diele tretej hlavy druhej časti Trestného poriadku v ustanoveniach § 258 – 273 TP je k všeobecným ustanoveniam o dokazovaní vo vzťahu špeciality. Hoci Trestný poriadok neobsahuje legálnu definíciu elektronického dôkazu a prístupov k jej vymedzeniu existuje v legislatíve[1072] či odbornej literatúre niekoľko,[1073] pod pojmom elektronický dôkaz možno označovať akúkoľvek informáciu s dôkaznou hodnotou relevantnou pre trestné konanie, ktorá je spracovávaná, uchovávaná alebo prenášaná v digitálnej podobe, a ktorá bola získaná zákonným spôsobom.

Keďže dokazovanie je právny pojem, z technického hľadiska sa zabezpečuje najmä prostredníctvom iných vedných disciplín, ktorými sú napríklad kriminalistika, forenzné vedné disciplíny ako súdne lekárstvo, súdna psychiatria, súdna psychológia a súdne inžinierstvo. Vo vzťahu k dokazovaniu plnia primárnu úlohu najmä poznatky z kriminalistiky, ktorá skúma taktické, technické a metodické otázky s cieľom zistiť, odhaliť, dokumentovať a objasňovať trestné činy, ako aj zistiť, odhaliť a usvedčiť ich páchateľov. Kriminalistika nastupuje až po spáchaní trestného činu, trestný čin nepozoruje, skúma ho iba z jeho pozostatkov v okolitom prostredí, teda zo stôp.[1074]

Tak ako po trestnom čine úkladnej vraždy strelnou zbraňou zostane v tele obete balistická stopa v podobe uviaznutej strely, ak dôjde k spáchaniu trestného činu v kybernetickom priestore, jeho páchateľ za sebou zanechá stopu digitálnu. Vo svete informačno-komunikačných technológií platí pravidlo, že pokiaľ čokoľvek nahráte, prenesiete, sprostredkujete, vložíte do kybernetického priestoru, zostane to tam navždy. Vždy bude existovať kópia vašich dát, ktorá vznikne buď v dôsledku toho, že ju uloží iný používateľ počítačového systému alebo v dôsledku fungovania počítačového systému ako

[1072] Čl. 3 ods. 8 e-Evidence nariadenia charakterizuje elektronické dôkazy ako *„údaje o účastníkovi, prevádzkové údaje alebo obsahové údaje uchovávané poskytovateľom služieb alebo v mene poskytovateľa služieb v elektronickej podobe v čase prijatia osvedčenia o európskom príkaze na predloženie dôkazov (OEPPD) alebo osvedčenia o európskom príkaze na uchovanie dôkazov (OEPUD) týmto poskytovateľom služieb.*"

[1073] K tomu porovnaj napr. KOLOUCH, J.: Cybercrime. 1. vydání. Praha : Edice CZ.NIC, 2016, s. 419. Alebo aj CASEY, E.: Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet. Third Edition. London : Academic Press, 2011, s. 8.

[1074] BLAŽEK, R.: Kriminalistika. Šamorín : Heuréka, 2016, s. 15.

takého. Napriek tomu, že tieto dáta následne odstránite alebo ich odstráni niekto iný, k ich trvalému a nezvratnému odstráneniu v skutočnosti nikdy nedôjde.[1075] Každé technologické zariadenie, ktoré získava, spracúva, prenáša, odovzdáva alebo uchováva dáta za sebou zanecháva záznamy (odrazy) o svojej činnosti. Tieto záznamy sú z kriminalistického hľadiska stopami. Podľa teórie odrazu, človek alebo iný objekt ovláda (spúšťa, modifikuje a pod.) softvérové vybavenie, prípadne jeho nastavenie. Vzájomné pôsobenie objektov spôsobuje odovzdávanie informácií medzi týmito objektmi, ktoré vytvára odraz v materiálnom prostredí. To znamená, že činnosti alebo zmeny (napr. preformátovanie disku) určitého subjektu (napr. páchateľa) sa následne odrážajú do materiálneho prostredia zvonka aj zvnútra danej technológie (napr. hoci na prvý pohľad nie je zjavné, že došlo k preformátovaniu disku, zistíme to použitím špeciálneho softvéru).[1076]

V odbornej literatúre sa môžeme stretnúť s niekoľkými prístupmi autorov, ktorí sa snažia ustáliť vhodnú definíciu digitálnej stopy, avšak so všeobecne akceptovanou definíciou prišla ešte v roku 1999 pracovná skupine SWGDE *(Scientific Working Group on Digital Evidence)*, podľa ktorej je digitálna stopa akákoľvek informácia s výpovednou hodnotou, uložená alebo prenášaná v digitálnej podobe,[1077] teda informácia pochádzajúca z prostriedkov informačno-komunikačných technológií. Pod túto univerzálnu definíciu možno poňať všetky digitálne stopy súvisiace s informačno-komunikačnými technológiami, a to nielen počítačové stopy, ale aj dáta pochádzajúce z kamerových systémov, mobilných telefónov či digitálnej televízie.

V porovnaní s inými druhmi kriminalistických stôp sa digitálne stopy vyznačujú špecifickými vlastnosťami, a to:

- nehmotnosť digitálnych stôp,
- latentnosť digitálnych stôp,
- časová trasovateľnosť digitálnych stôp,
- vysoká obsažnosť digitálnych stôp,
- veľmi nízka životnosť digitálnych stôp,

[1075] KOLOUCH, J.: Cybercrime. 1. vydání. Praha : Edice CZ.NIC, 2016, s. 135.
[1076] PORADA, V., RAK, R.: Digitální stopy v kriminalistice a forenzních vědách. In Soudní inženýrství. 2006, č. 17, s. 3- 23.
[1077] Ibid.

- uchovávanie a kvalita digitálnych stôp je ovplyvnená mnohými subjektívnymi faktormi,
- veľký dátový objem digitálnych stôp,
- dátová hustota digitálnych stôp v čase a s rozvojom nových technológií neustále klesá,
- extrémna dynamika prostredia digitálnych stôp,
- heterogénnosť a komplexnosť prostredia digitálnych stôp,
- veľký geografický rozsah priestoru s digitálnymi stopami,
- vysoký stupeň ochrany dát sťažuje alebo znemožňuje prácu s digitálnymi stopami,
- digitálna stopa je použitím špecializovaných prostriedkov automaticky identifikovateľná a spracovateľná,
- vysoká úroveň zahladzovania digitálnych stôp kvalifikovanými páchateľmi,
- obnoviteľnosť zničených digitálnych stôp,
- originálnosť digitálnych stôp,
- nízka úroveň akceptácie digitálnych stôp zo strany súdov a orgánov činných v trestnom konaní.[1078]

Digitálne stopy môžu mať pritom charakter fyzických stôp (pochádzajúcich zo zariadení, ktoré sú určené na spracovanie, uloženie alebo prenos dát, napríklad pevný disk počítača alebo pamäťová karta, ale v širšom význame aj počítač, tlačiareň a pod.), dátových stôp (pochádzajúce z rôznych databáz, adresátov, súborov) alebo stôp pochádzajúcich z metadát (metadáta sú v podstate dáta o dátach, teda súvisiace informácie týkajúce sa dátumu a času vytvorenia súboru, dátumu jeho modifikácie, vlastníka súboru, veľkosť súboru a pod.)

Fyzické a dátové objekty sa stávajú dôkazom až vtedy, ak sa získali z dôkazných prostriedkov podľa Trestného poriadku alebo osobitného zákona a sú akceptované orgánom činným v trestnom konaní, respektíve súdom. Kľúčovou otázkou je preto otázka preukázateľnosti axiómy, že digitálna stopa sa nachádzala na určitom mieste a že v priebehu procesu od jej zaistenia až do ukončenia znaleckého skúmania nebola žiadnym spôsobom modifikovaná. Preto sa pracuje s duplikátom digitálnej stopy, čo je presná digitálna reprodukcia všetkých dátových objektov nachádzajúcich sa na pôvodnom fyzickom objekte

[1078] Ibid.

vyhotovená na fyzicky rovnaký typ dátového média.[1079] Objem dát a informačný obsah všetkých dátových objektov sú v pomere 1:1 medzi originálom a duplikátom. Duplikáty digitálnych stôp sa vytvárajú pre potreby znaleckého dokazovania, aby mohol byť pôvodný materiál kedykoľvek predložený k opätovnému skúmaniu iným znalcom (pozn. najčastejšie pôjde o prípady, kedy si dá vyhotoviť znalecký posudok obvinený), ak samotný fyzický objekt (napríklad počítač) nemožno z rôznych dôvodov zaistiť. V praxi sa v prípade počítačov bežne vytvára obraz (*image)* disku, ktorý je verným duplikátom obsahu disku, teda zrkadlom jeho pôvodného obsahu uložený v digitálnej podobe.[1080]

Analýzou stôp súvisiacich s informačno-komunikačnými technológiami za účelom ich použitia ako elektronického dôkazu v trestnom konaní sa zaoberá **digitálna forenzná analýza**. Nastupuje po tom, čo orgán činný v trestnom konaní, resp. súd dospel k záveru, že za účelom preukázania skutočností podľa ustanovenia § 119 TP bude potrebné obstarať isté penzum dát, ktoré za splnenia určitých kritérií, môže nadobudnúť povahu elektronického dôkazu.

PRÍKLAD

Elektronický dôkaz by mal preto spĺňať tieto podmienky:

a) zákonnosť (dôkaz musí byť získaný zákonom predpísaným spôsobom),
b) autentickosť (pravosť, musí existovať príčinná súvislosť medzi dôkazom a skutkom),
c) integrita (dôkaz musí byť ucelený a nezmenený),
d) spoľahlivosť (spôsob získania dôkazu a manipulácia s ním nesmie v žiadnom prípade vzbudzovať dôvodné pochybnosti o autentickosti a hodnovernosti dôkazu),
e) hodnovernosť (za hodnoverný dôkaz možno považovať iba taký dôkaz, ktorý bol získaný zákonom predpísaným spôsobom, a zároveň neexistujú dôvodné pochybnosti o jeho pravosti, integrity a spoľahlivosti).

[1079] SMEJKAL, V.: Současné možnosti boje proti počítačové kriminalitě. In Data Security Management. 2016, č. 4, s. 18 – 23.
[1080] PORADA, V., RAK, R.: Digitální stopy v kriminalistice a forenzních vědách. In Soudní inženýrství. 2006, č. 17, s. 3- 23.

12.5.3.1Procesné úkony podľa Trestného poriadku smerujúce k získaniu elektronických dôkazov

Stará známa pravda hovorí, že tam, kde sa stretnú traja právnici, existujú štyri rôzne právne názory. Táto anekdota platí dvojnásobne pre problematiku obstarávania elektronických dôkazov. Pomerne často sa v praxi môžeme stretnúť s rozličnými postojmi vo vzťahu k aplikácii jednotlivých procesných ustanovení, a to nielen vo forme typickej triády sudca, prokurátor, advokát. Napriek tomu, že právna úprava zaisťovania dát ako potenciálnych elektronických dôkazov v Slovenskej republike sa aspoň čiastočne priblížila k medzinárodným štandardom, rozhodovacia prax v tejto oblasti zaostáva, je nekonzistentná a častokrát aj protichodná. K dátam, ktoré môžu za splnenia určitých požiadaviek nadobudnúť dôkaznú hodnotu, sa možno dostať viacerými postupmi podľa Trestného poriadku, ktorých použitie závisí od rôznych faktorov. Bude potrebné skúmať nielen to, kde sa záujmové dáta nachádzajú, ale aj o aké dáta ide z hľadiska ich povahy, teda či ide o dáta uchovávané na technickom nosiči alebo ide o údaje prenášané v reálnom čase, dáta obsahové alebo tie, ktoré majú charakter prevádzkových či lokalizačných údajov.

Za účelom zaistenia dát v elektronickej podobe preto možno využiť nasledovné procesné inštitúty upravené v Trestnom poriadku:[1081]

1) vydanie a odňatie veci podľa § 89 a 90 Trestného poriadku,
2) obhliadka podľa § 154 Trestného poriadku,
3) uchovanie, vydanie a odňatie počítačových údajov podľa § 91 Trestného poriadku,
4) odpočúvanie a záznam telekomunikačnej prevádzky podľa § 115 Trestného poriadku,

[1081] V legislatívnom procese LP/2023/612 je návrh novej právnej úpravy, ktorá bude primerane rozlišovať v § 10 TP vo všeobecných pojmoch definovať pre účely trestného konania počítačové údaje, nosiče, údaje o používateľovi, kto sa rozumie poskytovateľom služieb atď. Novela prináša zásadnú zmenu v získavaní rôznych kategórií počítačových údajov. Stanovuje sa povinnosť (všeobecná edičná) vydať počítačový údaj, nosič, alebo počítačový systém, ak nepostačuje vyhotovenie kópie na výzvu policajta, prokurátora, alebo predsedu senátu (89b TP)- ide o ustanovenie lex specialis k vydaniu veci. Odňatie počítačového údaju, nosiča, alebo počítačového systému bude možné iba na príkaz sudcu pre prípravné konanie, alebo predsedu senátu, ak nebolo vydanie veci úspešné a nepostačuje vyhotovenie kópii (§91 TP). Uložené údaje o používateľoch, kontách sa získavajú na príkaz policajta so súhlasom prokurátora, prokurátora alebo predsedu senátu (§116a, ods. 3, písm. a TP) od poskytovateľa služieb. Uložené prevádzkové a lokalizačné údaje sa získavajú na príkaz sudcu pre PK, alebo predsedu senátu (§116a, ods. 3, písm. b) TP) od poskytovateľa služieb. Uložené obsahové údaje sa získavajú na príkaz sudcu pre prípravné konanie alebo predsedu senátu od poskytovateľa služieb (§116a, ods. 3, písm. b) TP). Sledovanie prevádzkových a lokalizačných údajov je prípustné iba na príkaz sudcu pre PK, alebo predsedom senátu podľa §115a TP. Sledovanie obsahu- odpočúvanie zostáva nezmenené, rozširuje sa okruh trestných činov (§115 TP). Uchovanie údajov, odstránenie údajov alebo znemožnenie prístupu k údajom u poskytovateľa služieb bude prípustné podľa príkazu policajta so súhlasom prokurátora, prokurátora alebo predsedu senátu podľa §116 TP; odstránenie údajov alebo znemožnenie prístupu k údajom (avšak nie ich uchovávanie) u toho, kto má údaje u seba podľa príkazu policajta so súhlasom prokurátora, prokurátora alebo predsedu senátu podľa §89c TP.

5) oznámenie údajov o telekomunikačnej prevádzke podľa § 116 Trestného poriadku.

Vydanie a odňatie veci postup podľa § 89 a 90 Trestného poriadku

Prvý a zároveň v určitom smere ideálny prípad zaisťovania dát zahŕňa procesné situácie, kedy orgány činné v trestnom konaní, respektíve súdy majú vedomosť o tom, že predmetné záujmové dáta by sa mohli nachádzať na určitom dátovom nosiči.

Pod pojmom dátový nosič, ktorý je označovaný aj ako technický nosič či iné obdobné technické zariadenie možno rozumieť akékoľvek elektronické zariadenie schopné ukladať a znova prehrávať uložené informácie. Technickým nosičom sú najmä CD, DVD, LP platňa, magnetofónová kazeta, videokazeta, disketa, USB kľúč, filmový pás, harddisk počítača, harddisk mobilného telefónu.[1082] Z uvedeného preto vyplýva, že dáta zachytené na určitom technickom zariadení možno subsumovať pod ustanovenie § 130 ods. 2 TZ, podľa ktorého sa za vec považuje aj nehmotná informácia, dáta výpočtovej techniky alebo obrazový záznam na technickom nosiči.

Keďže dáta umiestnené na technickom nosiči sú považované za vec, a ak zároveň táto vec spĺňa atribút dôležitosti pre trestné konanie, pretože v zmysle ustanovenia § 89 ods. 1 písm. a) TP môže slúžiť na účely dokazovania,[1083] vzťahuje sa na ňu edičná povinnosť vyjadrená v ustanovení § 89a ods. 1 TP. Subjektom edičnej povinnosti je ktokoľvek, kto má vec, ktorá môže slúžiť na účely dokazovania, pri sebe. Predmetné ustanovenie sa teda vzťahuje nielen na osobu podozrivého či obvineného, ale aj na iné osoby, a to bez ohľadu na ich právny vzťah k veci (vlastníctvo, nájom, pôžička a pod.) Postačuje, ak je vec v danom momente v jeho faktickej moci.[1084] V tomto ohľade je potrebné uviesť, že podozrivý a obvinený majú právo, nie povinnosť vec vydať, vzhľadom na zásadu zákazu sebaobviňovania, ktorá vyplýva z čl. 6 Dohovoru o ľudských právach a základných slobodách.[1085] K vydaniu veci preto podozrivého a obvineného nemožno nijakým spôsobom

[1082] BURDA, E., ČENTÉŠ, J., KOLESÁR, J., ZÁHORA, J. a kol.: Trestný zákon. Všeobecná časť. Komentár. I. diel. 1. vydanie. Praha : C. H. Beck, 2010. s. 958.

[1083] V ustanovení § 89 ods. 2 TP sa explicitne ustanovuje generálne pravidlo, že zaistenie veci na účely dokazovania má prednosť pred inými dôvodmi zaistenia veci, pretože primárnym účelom trestného konania je dokázať vinu páchateľovi a spravodlivo ho potrestať.

[1084] ČENTÉŠ, J. a kol.: Trestné právo procesné. Všeobecná časť. Šamorín : Heuréka, 2016. ISBN 978-80-8173-020-7. s. 264.

[1085] Zákaz sebaobviňovania spočíva v práve podozrivej a obvinenej osoby na to, aby nebola žiadnym spôsobom nútená k priznaniu, respektíve k poskytnutiu dôkazov, ktoré by ju mohli usvedčiť či akýmkoľvek spôsobom spojiť s trestným činom.

donucovať,[1086] a to ani pod hrozbou uloženia poriadkovej pokuty, čo však ale neznamená, že mu za splnenia podmienok v ustanovení § 90 TP nemožno vec odňať.

V aplikačnej praxi nastal prípad, kedy sa osoba v procesnom postavení svedka dostavila v prípravnom konaní pred orgán činný v trestnom konaní na výsluch. Svedok mal počas výsluchu pri sebe mobilný telefón patriaci obvinenému, ktorý mal v oprávnenej držbe, nakoľko mu bol tento zverený do úschovy a zo strany vyšetrovateľa bol vyzvaný na vydanie tohto mobilného telefónu, ktorej vyhovel a zariadenie vydal. Na ilustrovanom prípade je preto zrejmé, že aj napriek tomu, že svedok disponoval vecou vo vlastníctve obvineného, nemohol tento postup namietať odkazujúc na zásadu zákazu sebaobviňovania, nakoľko táto prináleží iba osobe v procesnom postavení podozrivého a obvineného v trestnom konaní.

Ak osoba odmietne vyhovieť výzve na vydanie veci na účely dokazovania, možno pristúpiť k odňatiu veci. Pre prípad nevyhovenia výzve však musí byť táto osoba náležite poučená o možnosti uloženia poriadkovej pokuty v zmysle ustanovenia § 70 ods. 1 TP, ako i na možnosť odňatia veci podľa ustanovenia § 90 TP. Odňatie veci sa realizuje na základe príkazu predsedu senátu alebo na základe príkazu prokurátora alebo policajta v prípravnom konaní. Policajt potrebuje na vydanie takého príkazu predchádzajúci súhlas prokurátora. To však neplatí v prípade, kedy predchádzajúci súhlas prokurátora nemožno dosiahnuť a vec neznesie odklad. K odňatiu veci sa podľa možností priberie nezúčastnená osoba. O vydanej a odňatej veci sa spíše zápisnica, ktorá okrem všeobecných náležitostí obsahuje podrobný opis tejto veci tak, aby ju nebolo možné zameniť s inou. V prípade, ak je vydanou alebo odňatou vecou mobilný telefón, tablet či inteligentné hodinky, je do zápisnice potrebné uviesť IMEI *(International Mobile Equipment Identity)* zariadenia. Ide o unikátny kód zariadenia pridelený výrobcom, ktorý možno pripodobniť k rodnému číslu fyzickej osoby. Tento jedinečný kód slúži aj na identifikáciu konkrétneho zariadenia v sieti, na základe ktorého ho možno lokalizovať aj na diaľku.[1087] Osobe, ktorá vec vydala alebo ktorej bola vec odňatá, vydá orgán, ktorý úkon vykonal ihneď písomné potvrdenie alebo rovnopis zápisnice o tomto úkone.

[1086] V zmysle ustanovenia § 119 ods. 5 TP dôkaz získaný nezákonným donútením alebo hrozbou takého donútenia sa nesmie použiť v konaní okrem prípadu, keď sa použije ako dôkaz proti osobe, ktorá také donútenie alebo hrozbu donútenia použila.

[1087] Treba rozlišovať medzi IMEI a IMSI (*International Mobile Subscriber Identity*), čo je unikátne číslo, ktoré ale prideľuje operátor SIM karte v rámci mobilnej siete.

Trestný poriadok upravuje v ustanovení § 89a ods. 2 výnimku z edičnej povinnosti, ktorá sa nevzťahuje na listinu alebo inú vec, ktorej obsah sa týka okolnosti, o ktorej platí zákaz výsluchu, okrem prípadu, keď došlo k oslobodeniu od povinnosti zachovať vec v tajnosti alebo k oslobodeniu od povinnosti mlčanlivosti. Z doslovného výkladu tohto ustanovenia preto možno dospieť k záveru, že každý, koho zaväzuje zákonom ustanovená či uznaná povinnosť mlčanlivosti vo vzťahu k určitým skutočnostiam, o ktorých sa dozvedel alebo ku ktorým sa dostal najmä v súvislosti s výkonom jeho práce, činnosti, funkcie a podobne, je povinný zabrániť ich ďalšiemu rozširovaniu či sprístupňovaniu, ibaže by bol od tejto povinnosti oslobodený. V praxi pôjde najčastejšie o advokátov, daňových poradcov, účtovníkov, pracovníkov banky či osoby požívajúce procesnoprávnu exempciu.

Obhliadka podľa § 154 Trestného poriadku

Použitím týchto procesných nástrojov sa zaisťujú dáta pochádzajúce z otvorených zdrojov *(open source intelligence, OSINT)* tzv. otvorené vyšetrovanie alebo OSINT analýza. Konkrétne formáty zdieľania OSINT analýzy je potrebné voliť s prihliadnutím na faktory, ako sú technologická gramotnosť príjmateľa, objektívnosť, transparentnosť a bezpečnosť.

Uvedené možno ilustrovať na situácii, kedy bol spáchaný napríklad trestný čin podvodu tým spôsobom, že na základe inzerátu verejne dostupného na inzertnom portáli páchateľ ponúkal na predaj určitý sortiment, ktorý ale v skutočnosti neexistoval, resp. páchateľ už od počiatku nemal v úmysle tento ponúkaný sortiment dodať, na základe čoho došlo k vylákaniu kúpnej ceny (aspoň vo výške malej škody) od poškodeného, ktorá bola poukázaná na bankový účet páchateľa, ktorý ale plnenie z kúpnej zmluvy uzavretej na diaľku nedodal, čím páchateľ uviedol niekoho do omylu, a tak sa obohatil na škodu cudzieho majetku.

Z prípadu je zrejmé, že jeden z potenciálnych kľúčových dôkazov bude mať povahu informácie pochádzajúcej z webu inzertného portálu, ktorý je verejne dostupný používateľom internetu. Na zaistenie údajov pochádzajúcich z tejto web stránky nebude potrebné vydávať osobitný príkaz, pretože bude postačovať použitie dôkazného prostriedku v zmysle ustanovenia § 154 TP, ktoré sa týka obhliadky.[1088] Keďže nejde o nijako obzvlášť

[1088] Podľa ustanovenia § 154 ods. 1 prvá veta TP sa obhliadka vykonáva, ak majú byť priamym pozorovaním objasnené skutočnosti dôležité pre trestné konanie, najmä ak by mohli byť zistené alebo zaistené akékoľvek stopy. Z dikcie predmetného ustanovenia je preto zrejmé, že môže ísť aj o stopy digitálne.

náročný postup, nie je potrebné k tomuto procesnému úkonu priberať znalca, postačuje, ak pôjde i o odborne zdatnejšieho vyšetrovateľa. O obhliadke sa spíše zápisnica, ktorú vyhotovuje orgán vykonávajúci tento procesný úkon, teda buď orgán činný v trestnom konaní alebo v konaní pred súdom súd. Zápisnica by mala okrem všeobecných náležitostí podľa ustanovenia § 58 TP obsahovať aj ďalšie informácie, najmä detailný popis zabezpečovania predmetných informácií po technickej stránke. K zápisnici preto treba pripojiť technický nosič (napr. USB kľúč), na ktorom je zachytený zdrojový kód webovej stránky, z ktorej táto digitálna stopa pochádza. Dôraz by mal byť kladený na to, aby s týmto technickým nosičom už nebolo ďalej manipulované, resp. môžu byť vyhotovené i ďalšie kópie súboru obsahujúceho zdrojový kód stránky, a to napríklad pre prípad, že by si ho spolu so spisovým materiálom vyžiadal napríklad obvinený, avšak pri zachovaní originálneho súboru na účely jeho hodnotenia ako dôkazu súdom.

V tejto súvislosti je potrebné zmieniť sa o predkladaní výtlačkov *(printscreen/screenshot)* ako dôkazov prezentujúcich určitú skutočnosť. Hoci je vhodné zadokumentovať pri obhliadke inkriminovaný obsah webovej stránky v danom čase aj prostredníctvom výtlačku obrazovky a tento pripojiť k zápisnici, treba mať na pamäti, že pôjde o listinný dôkaz,[1089] nie o dôkaz elektronický. Použitie výtlačku ako jediného dôkazu by však mohlo zlyhať, a to namietaním jeho pravosti a hodnovernosti, preto je vhodnejšie zhromaždiť čo možno najväčší objem informácií o tvrdenej skutočnosti (zdrojový kód stránky, metadáta atď.)

Získať dáta, ktoré nepochádzajú z verejne prístupných zdrojov, teda v prípadoch, kedy je nutné prekonať určitú bezpečnostnú prekážku (či už vo forme hesla alebo iných prístupových údajov) za účelom obstarania dôkazu použiteľného v trestnom konaní, je možné i v rámci výsluchu, za predpokladu, že ich osoba dobrovoľne poskytne. Vypočúvaná osoba však musí byť v tomto ohľade náležite poučená na následky nevyhovenia výzvy, ktorej splnenie môže byť vynucované i možnosťou uloženia poriadkovej pokuty podľa ustanovenia § 70 ods. 1 TP. Treba mať však zároveň na pamäti, že vynucovanie splnenia povinnosti pod hrozbou uloženia poriadkovej pokuty absolútne neprichádza do úvahy v prípade výsluchu

[1089] V zmysle ustanovenia § 153 ods. 1 TP sú listinnými dôkazmi listiny, ktoré svojím obsahom dokazujú alebo vyvracajú skutočnosť vzťahujúcu sa na objasňovaný skutok, na obvineného alebo iné osoby, ktoré majú k veci vzťah.

podozrivej osoby či obvinenej osoby, nakoľko by to bolo v rozpore so zásadou *nemo tenetur se ipsum accusare*.

Vzhľadom na absenciu ustanovení o použiteľnosti OSINT analýzy ako dôkazu v trestnom konaní v Trestnom poriadku je potrebné vnímať použitie ustanovenia §154 ako aplikačné riešenie nedostatočnej právnej úpravy, ktorá ale slúži inému účelu. Považujeme preto za vhodné uviesť aspoň minimálne štandardy a postupy, ktoré by OSINT analýza mala spĺňať, aby mohla byť použiteľná ako dôkaz v trestnom konaní.

Otvorené zdroje zahŕňajú širokú škálu údajov pochádzajúcich z internetu, tlače, rozhlasového či televízneho vysielania a s obľubou sú využívané nielen orgánmi činnými v trestnom konaní, ale aj bezpečnostnými analytikmi, penetračnými testermi či investigatívnymi novinármi. Zmyslom a princípom OSINT analýzy je vyhľadávanie a hodnotenie verejne prístupných, neutajovaných informácií, na ktorých poskytnutie sa nevyžaduje osobitný príkaz, resp. súhlas.

Pred rozšírením internetu zahŕňal výskum otvorených zdrojov zbieranie informácií z tradičných médií (napr. novín, televíznych a rozhlasových vysielaní), publikácií (napr. kníh, akademických časopisov) a iných materiálov (napr. interných aktov a brožúr), Základná úroveň spočívala v tom, že platení zamestnanci pravidelne prehľadávali určené noviny a akademické, vládne a obchodné publikácie, identifikovali relevantné informácie a hodnotili ich.[1090] Vo všeobecnosti platilo v týchto dobách a platí to i dnes, že otvorený zdroj nie je a nemusí byť vždy zdroj, ktorý je všeobecne jednoducho verejné dostupný.

PRÍKLAD

Analýza otvorených zdrojov v zásade pracuje s štyrmi rôznymi kategóriami informácií:

- verejne dostupné,
- verejne ťažko dostupné,
- verejne dostupné na požiadanie a
- uzavreté – chránené alebo utajené.

[1090] Open source investigations in the age of Google / editors,Henrietta Wilson, SOAS University of London, UK & King's College London, UK,Olamide Samuel, University of Leicester, UK, Dan Plesch, SOAS University of London, UK.Description: New Jersey : World Scientific, [2024] | Series: Security science and technology,2059-1063 ; Vol. 4, s. 215-216

Najjednoduchšia z týchto kategórií – verejne dostupné – zahŕňa informácie, ktoré sú verejne dostupné a relatívne ľahko získateľné, napríklad noviny, ktoré sú buď bezplatné, alebo relatívne lacné. Tieto zdroje sú nielen dostupné, ale zvyčajne aj jednoduché na dekódovanie, pochopenie a vyhodnotenie. Naopak, verejné ťažko dostupné zdroje – niekedy nazývané „sivá literatúra" – sú verejne dostupné, avšak dostupné ťažko. Hľadanie a získavanie otvorených-ťažko dostupných zdrojov je komplikované tým, že ide zvyčajne o špecializované publikácie; často sa vydávajú len v malom náklade a nie sú široko distribuované, okrem toho sa ľahko prehliadnu, napríklad informácie v poznámke pod čiarou. Verejne dostupné zdroje na požiadanie sú zdroje, ku ktorým majú analytici prístup na základe svojej siete kontaktov a zahŕňajú informácie získané prostredníctvom žiadostí o slobodnom prístupe k informáciám. [1091]

Vskutku bohatým zdrojom sú v súčasnej dobe najmä sociálne siete, v rámci ktorých užívatelia dobrovoľne zdieľajú informácie zo svojho súkromia. Užitočné dáta sa dajú vyextrahovať napríklad aj z hlavičky e-mailu či doménového mena, rôznych verejných registrov, databáz a podobne. Ide teda o využívanie voľne dostupných informačných kanálov, ktoré sú verejnosti prístupné bez obmedzenia alebo môžu byť prístupné za určitú protihodnotu (jednorazový poplatok, mesačné predplatné a pod.) Istou nevýhodou zberu informácií z otvorených zdrojov je časová náročnosť a potreba dôkladného overovania ich vierohodnosti, kvality a výpovednej hodnoty. Pri získavaní elektronických dôkazov metódou OSINT je potrebné rozlišovať, či je účelom využitia tejto metódy získanie priameho usvedčujúceho/oslobodzujúceho dôkazu, alebo ide o otvorené vyšetrovanie a zhromažďovanie informácií o prítomnosti predmetu analýzy vo verejne dostupných zdrojoch a z toho hodnotiace závery. V prípade prvého menovaného pôjde o štandardný postup zaisťovania elektronického dôkazu, tak ako je uvedené v iných častiach. Preto je potrebné pri získavaní digitálnych dôkazov metódou OSINT dodržiavať určité zásady:

a) *identifikácia nevyhnutného (primeraného) rozsahu skúmania.*

Nevyhnutný rozsah môže byť časový (relevantný interval skúmania), alebo osobný (Analýza metódou OSINT by nemala pokrývať získavanie informácií o osobách mimo rámec

[1091] Ibid.

zadania a ak áno, mal by byť tento vzťah jasný a zrozumiteľný- napr. spoločník, osoba žijúca v spoločnej domácnosti atď.);[1092]

b) evidencia a reťazenie (chain of custody), transparentnosť a preskúmateľnosť;

Uvádzanie presných údajov a záznamov o využití zdroja informácie ako i identifikácia osoby, ktorá tento zdroj využila je nevyhnutné pre možnosť spätného preskúmania analýzy metódou OSINT (tzv. OSINT analýzy) a jej použiteľnosti ako dôkazu v trestnom konaní.[1093] Princíp evidencie taktiež vyžaduje uvádzať v analýze metódou OSINT nástroje, ktoré sa použili pre vyhľadávanie informácií. Princíp evidencie taktiež vyžaduje, ak analýzu metódou OSINT vykonáva viacej osôb, aj dokumentáciu rozsahu konania týchto osôb a spôsobu odovzdávania si informácií a zadaní.[1094] Overiteľnosť a hodnotenie OSINT analýzy nie je možné bez základných údajov o období (kedy sa vykonávala analýza), miestach a zdrojoch použitých v analýze a časom zakonzervovaní zistených informácií. Uvedené je potrebné najmä preto, že samotná OSINT analýza sa môže použiť ako dôkaz i s väčším časovým odstupom od jej spracovania, kedy určité nástroje, alebo linky použite v čase spracovania už nie sú funkčné, alebo určitý poskytovateľ (najmä sociálne siete) danú funkcionalitu už nepodporuje.[1095]

c) nestrannosť a nezaujatosť;

Tak ako pri akomkoľvek inom vyhľadávaní dôkazov, osoba vyhľadávajúc a hodnotiaca dôkazy získané metódou OSINT (tzv. OSINT dôkazy), musí k týmto pristupovať bez zaujatosti a objektívne. [1096]OSINT analýza v tejto otázke predstavuje riziko, že osoba pri vyhľadávaní a hodnotení OSINT dôkazov začne preberať kontextové informácie a pramene,

[1092] Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Center and UN Human Rights Office of the High Commissioner; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, s. 13, dostupné dňa 10.03.2026 na: LINK

[1093] Ibid.

[1094] ISO 27037, s.10-11.

[1095] Open source investigations in the age of Google / editors,Henrietta Wilson, SOAS University of London, UK & King's College London, UK,Olamide Samuel, University of Leicester, UK, Dan Plesch, SOAS University of London, UK.Description: New Jersey : World Scientific, [2024] | Series: Security science and technology,2059-1063 ; Vol. 4, s. 47

[1096] Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Center and UN Human Rights Office of the High Commissioner; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, s. 12,15 dostupné dňa 10.03.2026 na: LINK

ktoré podporujú argumentáciu jednej zo strán, alebo zastávajú určitý nie neutrálny postoj.[1097] S poukazom na uvedené je nevyhnutné, aby sa v OSINT analýze objavilo i zdôvodnenie, ak sa určitý zdroj nepoužil alebo sa na neho neprihliadalo. V spojení s evidenciou a chain of custody by požiadavku nestrannosti a nezaujatosti OSINT analýzy mala garantovať, ktorá zodpovedá za celkovú OSINT analýzu.

d) subsidiarita OSINT

OSINT analýza spravidla poskytuje veľmi vhodné a kontextové informácie k predmetu analýzy avšak mala by byť dopĺňaná vždy ďalšími dôkazmi, aby jej hodnota bola čo najvyššia.[1098] OSINT analýza sama osobe spravidla nie je priamym elektronickým dôkazom, oslobodzujúcim alebo usvedčujúcim.[1099]

e) Riziková analýza, taktika a plánovanie[1100]

Za dodržanie bezpečnosti OSINT postupov a dotknutých osôb zodpovedajú všetky dotknuté osoby, nielen OSINT odborne zdatné osoby. Za týmto účelom je potrebné prijať opatrenia týkajúce sa infraštruktúry, vrátane hardvéru, softvéru a sietí zapojených do OSINT analýzy a opatrenia týkajúce sa správania osôb, ktoré sa zúčastňujú v určitej miere tvorby OSINT analýzy vrátane orgánov činných v trestnom konaní, či operatívnych zložiek. Rizikové analýzy k prípadu a použitiu OSINT postupov by sa mali vykonávať na:

- strategickej úrovni (úroveň organizácie, resp. zložky vynucujúcej právo)
- taktickej úrovni (konkrétneho vyšetrovania trestného činu, v ktorom má byť OSINT analýza využitá) a

---

[1097] Open source investigations in the age of Google / editors,Henrietta Wilson, SOAS University of London, UK & King's College London, UK,Olamide Samuel, University of Leicester, UK, Dan Plesch, SOAS University of London, UK.Description: New Jersey : World Scientific, [2024] | Series: Security science and technology,2059-1063 ; Vol. 4, s. 228-229

[1098] Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Center and UN Human Rights Office of the High Commissioner; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, s. 15 dostupné dňa 10.03.2026 na: LINK

[1099] Napr. prípad verejne dostupného diela s detskou pornografiou, teroristickým manifestom, podvodným inzerátom na bežnej platforme elektronického trhoviska, ku ktorým je potrebné pristupovať ako ku ktorýmkoľvek iným elektronickým dôkazov spravidla spojenými ďalšími príkazmi na zamedzenie prístupu alebo odstránenie obsahu.

[1100] Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Center and UN Human Rights Office of the High Commissioner; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, s. 44 dostupné dňa 10.03.2026 na: LINK

- operatívnej úrovní konkrétnych činností a úloh jednotlivých úkonov vo vyšetrovaní a plánovaní OSINT analýzy.

Ochranné opatrenia a plánovanie OSINT analýzy by mali byť navrhnuté tak, aby zmierňovali riziká a hrozby vyplývajúce z vykonania analýzy, alebo vyšetrovania konkrétnej trestnej veci. Riziková analýza, taktika a plánovanie OSINT analýzy by mala zohľadňovať všetky druhy škôd, vrátane digitálnych, finančných, právnych, fyzických, psychosociálnych. Riziková analýza použitia OSINT postupov sa musí vysporiadať najmä so zraniteľnosťami otvoreného vyšetrovania spojených s internetovými pripojeniami/IP adresami, zariadeniami a ich funkciami a správaním používateľov.

Proces otvoreného vyšetrovania pozostáva zo šiestich štádií. Sú to:[1101]

- vykonanie online otvoreného vyšetrovania;
- predbežné posúdenie/hodnotenie dát;
- zhromažďovanie dát;
- uchovávanie dát;
- overovanie otvorených dát a postupov; a
- OSINT analýza.

Ide o cyklus, ktorý sa môže opakovať i viackrát, keďže môžu vyjsť najavo nové informácie. Osoby vykonávajúce otvorené vyšetrovanie sú povinní dokumentovať svoje činnosti počas každej fázy.[1102] Zistenia otvoreného vyšetrovania, ktoré sa týkajú buď zhromaždených údajov, alebo záverov vyvodených z týchto údajov, môžu byť v trestnom stíhaní využité dôkazným prostriedkom:[1103]

- výsluchu osoby (ústne) podľa §133 Tr.por, vrátane výsluchu prostredníctvom videokonferencie podľa §61b Tr.por, pri výsluchu je možné použiť i vizualizácie OSINT analýzy formou poznámok

[1101] Takto uvedené štádia sú v súlade i s technickými normami zaisťovania digitálnych dôkazov ISO 27042, s. 4-11 a ISO 27037 s. 6-18, pokiaľ je možné z dokumentácie otvoreného vyšetrovania dovodiť predpísané štandardy, viď. vyššie.

[1102] Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Center and UN Human Rights Office of the High Commissioner; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, s. 66 dostupné dňa 10.03.2026 na: LINK

[1103] Ibid.

- alebo písomne prostredníctvom odborného vyjadrenia podľa §141 Tr.por. Súčasťou písomného odborného vyjadrenie môžu byť i vizualizácia výsledkov a postupov pri tvorbe OSINT analýzy, doplnený o prípadný výsluch osoby podľa bodu vyššie.

Vydanie, odňatie a uchovanie počítačových údajov § 91 Trestného poriadku

Ako bolo už niekoľkokrát naznačené, právna úprava procesných pravidiel uchovania, vydania a odňatia počítačových údajov v zmysle ustanovenia § 91 TP bola prijatá s poukazom na plnenie záväzkov Slovenskej republiky plynúcich z Budapeštianskeho dohovoru.

Inštitút uchovania, vydania a odňatia počítačových údajov má svoj nenahraditeľný význam najmä v situáciách, kedy zaistenie záujmových dát v elektronickej podobe nie je možné vykonať prostredníctvom ustanovenia § 89 TP, pretože nie sú vecou v zmysle Trestného zákona spĺňajúcou zároveň charakteristiku veci dôležitej pre trestné konanie alebo s ohľadom na zásadu primeranosti a zdržanlivosti ako jednu zo zásad trestného konania tento spôsob nie je nevyhnutný či inak účelný.

V obdobnom duchu je poňaté aj konštatovanie Ústavného súdu Slovenskej republiky v náleze III. ÚS 68/2010, podľa ktorého záujem štátu na ochrane pred zločinnosťou zakladajúci legitímnosť zásahov do práva na súkromie pri realizácii niektorých inštitútov podľa štvrtej hlavy prvej časti Trestného poriadku (pozn. zaistenie osôb a vecí) musí byť uvedený do rovnováhy so závažnosťou zásahu do tohto práva. Znamená to zvoliť si pri realizácii zásahu čo najmiernejší prostriedok, ktorý je súčasne spôsobilý zabezpečiť dosiahnutie sledovaného cieľa, napríklad uprednostniť úkon uchovania a vydania počítačových údajov (pozn. podľa ustanovenia § 91 TP uchovanie, vydanie a odňatie počítačových údajov) pred inštitútom vydania, resp. odňatia veci. V opačnom prípade znamená neproporcionálny postup konajúceho orgánu porušenie garancií práva na súkromie a spravodlivého procesu.[1104]

V praxi pôjde najčastejšie o situácie, kedy je na účely trestného konania potrebné zaistiť dáta, ktoré majú napríklad charakter už uskutočnenej komunikácie prostredníctvom mailu, na sociálnej sieti, internetovej zoznamke, ale rovnako tak aj faktúry uložené na virtuálnom úložisku, v notebooku zamestnanca obvinenej právnickej osoby a pod.

[1104] Nález Ústavného súdu Slovenskej republiky sp. zn. III. ÚS 68/2010 z 25. augusta 2010, II. časť odôvodnenia bod 2. B.

PRÍKLAD

Z uvedeného je zrejmé, že príkazy podľa ustanovenia § 91 TP majú vskutku široký záber a nevzťahujú sa len na dáta obsahové spĺňajúce pojmový znak **počítačové údaje uložené prostredníctvom počítačového systému**, ale aj napríklad údaje týkajúce sa pôvodu, cieľa, trasy, dátumu, objemu či trvania komunikácie, ktoré označujeme súhrnným pojmom **prevádzkové údaje**. Rovnako tak je zjavné, že formulácia **povinnej osoby**, ktorou rozumieme osobu, v ktorej držbe alebo osobu, pod ktorej kontrolou sa také údaje nachádzajú, je zámerne poňatá čo najširšie, aby do seba pojala viaceré subjekty, ktoré môžu byť adresátom príkazu podľa ustanovenia § 91 TP, od poskytovateľa služby, zamestnávateľa, účtovníka až po špecialistu bezpečnosti informačných systémov.

Spôsob zaisťovania dát prostredníctvom jedného z príkazov podľa § 91 TP teda predstavuje menej intenzívny zásah do slobody jednotlivca v porovnaní napríklad s vykonaním domovej prehliadky. To však samozrejme nevylučuje procesnú situáciu, kedy dôjde k vykonaniu príkazu v zmysle ustanovenia § 91 TP v rámci vykonania niektorej z prehliadok podľa Trestného poriadku. V prípadoch, kedy je vydaný príkaz napríklad na domovú prehliadku alebo prehliadku iných priestorov nenapĺňajúcich pojmový znak obydlia, už nie je potrebné vydávanie ďalšieho príkazu na vydanie počítačových údajov, nakoľko je tento konzumovaný príkazom na domovú prehliadku, resp. príkazom na prehliadku iných priestorov. V opačnom prípade by išlo o hromadenie príkazov, ktoré sa javí nadbytočné a nie nevyhnutné.[1105] Treba však osobitne zdôrazniť, aby záujmové dáta, ktoré sa majú vykonanou prehliadkou zaistiť boli v príkaze na domovú prehliadku alebo prehliadku iných priestorov čo možno najviac konkretizované.

V zmysle ustanovenia § 91 TP za účelom zaistenia počítačových údajov vrátane prevádzkových údajov uložených prostredníctvom počítačového systému možno vydať päť druhov príkazov, vrátane ich kombinácií, ktorými pred začatím trestného stíhania alebo v prípravnom konaní prokurátor a v štádiu súdneho konania predseda senátu prikáže, aby:

a) boli takéto údaje uchovávané a udržiavané v celistvosti,
b) bolo umožnené vyhotovenie a ponechanie si kópie takých údajov,
c) bol k týmto údajom znemožnený prístup,

[1105] K tomu pozri napr. ŠAMKO, P.: Daňové podvodné konania a ich dokazovanie. Bratislava : Wolters Kluwer, 2015. s. 362.

d) boli takéto údaje odstránené z počítačového systému,

e) boli takéto údaje vydané na účely dokazovania.

PRÍKLAD
Príkaz sa doručuje povinnej osobe, ktorá tieto údaje vydá tomu, kto príkaz vydal, t. j. predsedovi senátu alebo prokurátorovi. Oprávnenou osobou však môže byť aj iný subjekt, napríklad znalec alebo vyšetrovateľ, pričom pre tento prípad platí, že táto osoba musí byť v príkaze výslovne uvedená. Rovnaké pravidlo ako v prípade inštitútu vydania a odňatia veci sa uplatňuje aj vo vzťahu k počítačovým údajom, teda v situácii, kedy by povinná osoba nereagovala na výzvu vydať počítačové údaje dobrovoľne, možno pristúpiť aj k ich odňatiu proti jej vôli, a to s poukazom na ustanovenie § 91 ods. 6 TP. Z hľadiska formálnych a obsahových náležitostí príkazu, musí byť vyhotovený v písomnej forme a okrem všeobecných obsahových náležitostí v zmysle ustanovenia § 181 TP, musí byť aj odôvodnený konkrétnymi skutkovými okolnosťami, ktoré jeho vydanie odôvodňujú.

Pokiaľ ide o príkaz, ktorým sa nariaďuje uchovanie a udržiavanie dát v celistvosti, ako aj o príkaz, ktorým sa nariaďuje znemožnenie prístupu k takýmto dátam, musí byť v príkaze zároveň uvedený aj čas, najviac po dobu 90 dní, a to s možnosťou opätovného predĺženia tejto lehoty novým príkazom. Zároveň popri príkaze podľa ustanovení § 91 ods. 1, 2, 3 TP sa môže povinnej osobe uložiť povinnosť zachovať v tajnosti opatrenia uvedené v príkaze. Splnenie tejto povinnosti je možné vynucovať aj pod hrozbou uloženia poriadkovej pokuty v zmysle ustanovenia § 70 ods. 1 TP, na čo však musí byť povinná osoba vopred upozornená.

Počas celej doby je potrebné skúmať trvanie dôvodov uchovávania počítačových údajov, vrátane prevádzkových údajov. Preto, ak uchovávanie počítačových údajov, vrátane prevádzkových údajov na účely dokazovania už nie je potrebné, bez meškania vydá predseda senátu, resp. prokurátor pred začatím trestného stíhania alebo v prípravnom konaní príkaz na zrušenie uchovávania týchto údajov. V tomto smere preto prichádza do úvahy aj podanie žiadosti dotknutou osobou (napr. obvineným), ktorou sa môže domáhať vydania dát zo zaistenia.

Obvykle sa k realizácii obsahu tohto príkazu priberá aj znalec z príslušného odboru,[1106] ktorý zastrešuje vykonanie tohto procesného úkonu najmä po odbornej a technickej stránke, pretože zaistené dáta sú v ďalšom postupe predmetom znaleckého skúmania, o ktorom sa vyhotovuje znalecký posudok. Ak sa dáta zaisťujú v rámci niektorej z prehliadok podľa Trestného poriadku, je potrebné o tomto úkone vyhotoviť zápisnicu, v ktorej je zadokumentovaný podrobný priebeh úkonu, najmä aké konkrétne dáta boli zaisťované, akým spôsobom, kto zaisťovanie vykonával, aké nosiče dát boli zaistené a podobne.

Prehliadky podľa § 99 a nasl. Trestného poriadku

Nariadiť domovú prehliadku a prehliadku iných priestorov a pozemkov je oprávnený predseda senátu a pred začatím trestného stíhania alebo v prípravnom konaní na návrh prokurátora sudca pre prípravné konanie. Pokiaľ aj došlo k vydaniu príkazu na domovú prehliadku pred začatím trestného stíhania, vykonaním prehliadky sa začína trestné stíhanie V neodkladných prípadoch môže nariadiť domovú prehliadku namiesto príslušného predsedu senátu a v prípravnom konaní namiesto príslušného sudcu pre prípravné konanie predseda senátu a v prípravnom konaní sudca pre prípravné konanie, v ktorého obvode sa má prehliadka vykonať.[1107] Osobnú prehliadku nariaďuje prokurátor alebo s jeho súhlasom policajt.

Príkazy na domovú prehliadku ale i prehliadku iných priestorov a pozemkov musia byť vydané písomne a musí byť odôvodnený. Príkaz musí spĺňať požiadavky podľa § 181 a nasl. TP inak je neplatný. V príkazoch na prehliadku musia byť okrem iných náležitostí uvedené dôvody, ktoré viedli k vydaniu príkazu, vrátane uvedenia vecí alebo osôb, ktoré by mali byť pri prehliadke nájdené (hľadané). Pokiaľ je dôvodom prehliadky zaistenie elektronického nosiča, telefónu, počítača nie je potrebný ďalší príkaz pre účely prístupu do zariadenia zaisteného počas prehliadky (napr. príkaz podľa §91 TP)[1108] Pokiaľ je dôvodom prehliadky zaisťovanie digitálnych údajov má byť v zmysle zásady proporcionality analógie s opisom veci uvedený reťazec znakov, určených na vyhľadávanie digitálnych údajov (slová, slovné

[1106] Znalci zapísaní v zozname znalcov vedenom Ministerstvom spravodlivosti Slovenskej republiky v odbore kriminalistika (odvetvie kriminalistická informatika), resp. v odbore elektrotechnika.
[1107] STRÉMY, T., ŠAMKO, P., KURILOVSKÁ, L. Trestný poriadok. Praktický komentár. 1. vyd. Praha : Wolters Kluwer ČR, a. s., 2024, s. 318.
[1108] K tomu pozri R 47/2017.

spojenia, číslice atď.), ktoré by mali byť koncipované primerane reštriktívne, alebo ktorých kombinácia by nemala byť neprimeraná.

Pokiaľ v priebehu výkonu prehliadky dôjde nájdeniu iných osôb alebo vecí než tých, ktoré boli v príkaze uvedené, nie je možné tieto veci zaistiť, a to bez vydania nového príkazu, okrem prípadu, že ich zaistenie je nevyhnutné z dôvodu ochrany života a zdravia, ochrany majetku a iného vereného záujmu. Takýmto dôvodom môže byť napríklad potreba zaistenia výbušných či rádioaktívnych látok pri výkone prehliadky, ktorá bola nariadená z dôvodu hľadania osoby podozrivej zo spáchania trestnej činnosti a pod. Súčasťou príkazu by tiež malo byť uvedenie osoby (osôb), ktoré ju vykonajú v prípade, ak výkon tejto prehliadky vykonáva iný orgán než ten, ktorý ju nariadil, teda ak prehliadku vykonáva policajt.[1109] Osobou, u ktorej sa prehliadka vykonáva, je osoba, ktorá obydlie skutočne užíva, napr. vlastník, nájomník, osoby im blízke a pod.

PRÍKLAD

Príkazy súdu a prokurátora sa v trestnom konaní vydajú len v prípade zákonného dôvodu na zásah do základných alebo iných práv a slobôd dotknutých osôb. Domovú prehliadku alebo prehliadku iných priestorov alebo pozemku na účel zabezpečenia veci dôležitej pre trestné konanie nie je potrebné nariadiť, ak je zrejmá dobrovoľná súčinnosť osoby, ktorá je vlastníkom alebo oprávneným užívateľom nehnuteľnosti, v (na) ktorej sa má vec nachádzať. V takom prípade sa použije inštitút vydania alebo odňatia veci (§ 91 Tr. por.) po prípadnom predchádzajúcom, resp. súčasnom vykonaní obhliadky (§ 154 Tr. por.) bez nariadenia prehliadky uvedenej v § 99 ods. 1 alebo ods. 2 Tr. por. Aj v prípade nariadenia domovej prehliadky alebo prehliadky iných priestorov alebo pozemku sa od výkonu prehliadky upustí alebo sa prehliadka ukončí, ak sa dobrovoľné vydanie individuálne určenej veci dosiahlo predchádzajúcou výzvou pri splnení podmienok uvedených v § 104 ods. 1 a ods. 2 Tr. por.[1110]

V prípade použitia trestno-procesného nástroja spôsobilého zasiahnuť do garantovaných práv kohokoľvek, akým je aj prehliadka iných priestorov a pozemkov, sa požiadavka ochrany základných práv musí prejaviť aj v štádiu prípravného konania vo vydaní

[1109] STRÉMY, T., ŠAMKO, P., KURILOVSKÁ, L. Trestný poriadok. Praktický komentár. 1. vyd. Praha : Wolters Kluwer ČR, a. s., 2024, s. 320-321.
[1110] K tomu pozri R 17/2015.

dostatočne odôvodneného príkazu prokurátora alebo príkazu policajta. Tieto orgány činné v trestnom konaní majú teda povinnosť poskytnúť dostatočné záruky zákonnosti a ústavnosti ako pri rozhodovaní o nariadení prehliadky iných priestorov a pozemkov, tak aj pri jej realizácii, inak je ich postup spôsobilý porušiť právo na spravodlivý proces a ďalšie práva súvisiace s ochranou súkromia dotknutých osôb.[1111]

Podľa § 2 ods. 1 TP nikto nemôže byť stíhaný ako obvinený inak než zo zákonných dôvodov a spôsobom, ktorý ustanovuje tento zákon. Je preto porušením tejto základnej zásady trestného konania, ak sa vykoná prehliadka „iného priestoru", napr. osobného motorového vozidla, bez prítomnosti vlastníka vozidla, ktorého totožnosť je známa, je dostupný, nie sú prítomné žiadne dôvody v zmysle § 104 ods. 2 TP a dotknutá osoba sa práva účasti na tomto úkone nevzdala.

Prehliadka „iných priestorov" vykonaná v rozpore so zákonom je úkon neopakovateľný a výstup z takejto prehliadky ako dôkaz je nepoužiteľný pre jeho rozpor s ustanovením § 119 ods. 2 TP prvou vetou, v zmysle ktorej za dôkaz môže slúžiť všetko, čo môže prispieť na náležité objasnenie veci a čo sa získalo z dôkazných prostriedkov podľa tohto zákona alebo podľa osobitného zákona.[1112]

Z ustanovení § 100 ods. 1, ods. 2 a § 199 ods. 1 až ods. 3 Trestného poriadku vyplýva, že domovú prehliadku možno nariadiť a vykonať aj pred vydaním uznesenia o začatí trestného stíhania, a to s účinkami začatia trestného stíhania takým zaisťovacím úkonom. Musí však byť splnená podmienka, že súčasne hrozí nebezpečenstvo z omeškania, teda že vzhľadom na hrozbu zničenia alebo zmarenia vykonania dôkazu, ktorý má byť zaistený, neznesie domová prehliadka odklad na čas do vydania uznesenia o začatí trestného stíhania. Nebezpečenstvo z omeškania je v tomto prípade pojmovým ekvivalentom neodkladnosti úkonu (§ 10 ods. 17 Trestného poriadku).[1113]

Z uvedeného vyplýva, že v zmysle zásady subsidiarity a proporcionality by sa pri prehliadke vždy malo uprednostniť stiahnutie relevantných údajov resp. tvorba tzv. imagov pred faktickým odňatím zariadenia. Z uvedeného vychádza i pripravovaná veľká novela zaisťovania počítačových údajov.[1114] Úplným špecifikom sú prehliadky advokátskych kancelárií a zaisťovanie digitálnych dôkazov z elektronicky vedených spisov na úložiskách

[1111] K tomu pozri III. ÚS 172/2010.
[1112] K tomu pozri R 8/2009.
[1113] K tomu pozri R 8/2017.
[1114] Viď poznámka pod čiarou vyššie.

advokátskych kancelárií[1115], ktorých postup sa spravuje Ministerstva spravodlivosti Slovenskej republiky č. 209/2023 Z. z. o podrobnostiach a postupe zabezpečenia a zaistenia listiny pri domovej prehliadke a prehliadke iných priestorov, v ktorých advokát vykonáva advokáciu. Vzhľadom na citlivosť údajov a povinnosť mlčanlivosti ide o formalizovaný postup za účasti zástupcu SAK, ktorý ak nesúhlasí so zaistením dátového nosiča, rozhoduje o sprístupnení takéhoto zariadenia orgánom činným v trestnom konaní sudca pre prípravné konanie.

Vo vzťahu k elektronickým nosičom ako mobilné telefóny resp. počítače, tablety a ich zaisťovaniu počas využitia inštitútu vstupu do obydlia podľa § 103 TP[1116] platí, že tieto je možné zaistiť **výlučne** v prípade ak tieto zariadenia má osoba počas vstupu do obydlia pri sebe alebo na sebe, na ktoré sa následne vzťahuje postup podľa § 102 ods. 4 TP (výkon osobnej prehliadky bez príkazu), dohľadávanie alebo pátranie po elektronických zariadeniach v obydlí počas výkonu vstupu je v rozpore s Trestným poriadkom.

Odpočúvanie a záznam telekomunikačnej prevádzky podľa § 115 a Oznámenie údajov o telekomunikačnej prevádzke podľa § 116 Trestného poriadku

Procesné inštitúty odpočúvanie a záznam telekomunikačnej prevádzky a oznámenie údajov o telekomunikačnej prevádzke zaraďujeme do množiny informačno-technických prostriedkov v zmysle ustanovenia § 10 ods. 20 TP. Použitie informačno-technických prostriedkov sa vyznačuje pomerne intenzívnym zásahom do základných ľudských práv a slobôd, najmä do práva na súkromie. Z ustálenej judikatúry ESĽP vyplýva, že prípustným je iba taký zásah do súkromia jednotlivca zo strany orgánu verejnej moci ktorý je legálny, legitímny a proporcionálny. Z hľadiska **zásady legality** preto odpočúvanie musí spĺňať zákonné podmienky a dôvody na jeho realizáciu ustanovené v Trestnom poriadku, ktoré sú premietnuté napríklad v stanovení okruhu trestných činov, pre ktoré možno ten ktorý

[1115] Okrem sídla advokáta zapísaného do zoznamu advokátov ide ďalej napr. o pobočku advokátskej kancelárie, kanceláriu advokáta v sídle obchodnej spoločnosti, ktorá poskytuje právne služby, vozidlo advokáta alebo miesta určené na archiváciu či uloženie spisov advokáta. Postup podľa § 85b Tř. ř. sa však uplatní aj vo vzťahu k ostatným, do úvahy prichádzajúcich miest vzťahujúcich sa k výkonu advokácie, v ktorých možno ukladať, spracúvať a využívať informácie o klientoch, na ktoré sa vzťahuje povinnosť mlčanlivosti advokáta. Môžu nimi byť rôzne elektronické úložiská dát, a to či už ide o webové stránky advokáta, vlastné dátové úložiská advokát/a nenachádzajúce sa na miestach bežného výkonu advokátskej praxe alebo úložiská prevádzkované odlišnou osobou od advokáta umožňujúce vzdialený prístup prostredníctvom internetovej siete (napr. rôzne typy tzv. hostingov, cloudov, serverov). NS ČR: R 35/2015.

[1116] S poukazom na §103 ods. 2 TP najmä v prípadoch realizovaného pátrania po hľadanej osobe, voči ktorej je vydaný príkaz na zatknutie alebo príkaz na dodanie do výkonu trestu odňatia slobody.

prostriedok použiť, lehôt ich trvania či postupu, ktorým sa môže dotknutá osoba domáhať preskúmania zákonnosti použitého opatrenia. **Zásada legitimity** zásahu do práva na súkromie znamená, že účel sledovaný použitím týchto prostriedkov je v záujme štátu z dôvodov ochrany bezpečnosti, predchádzania nepokojov a zločinnosti alebo z dôvodu ochrany zdravia a morálky, zabezpečenia hospodárskeho blahobytu krajiny a v záujme jednotlivcov z dôvodu ochrany ich práv a slobôd.[1117] Vo vzťahu k **zásade proporcionality** je potrebné skúmať či sledovaný cieľ nie je možné dosiahnuť aj inými, menej invazívnymi prostriedkami pri dosiahnutí rovnakého výsledku, teda či je použitie toho ktorého prostriedku nevyhnutné. K obmedzeniu súkromia osôb pri používaní informačno-technických prostriedkov v zmysle Trestného poriadku preto môže dôjsť zo strany orgánov verejnej moci len celkom výnimočne a ak je to nevyhnutné, a zároveň účel sledovaný verejným záujmom nemožno dosiahnuť inak. Pri nedodržaní týchto podmienok ide o protiústavný zásah.[1118]

Právna úprava odpočúvania a záznamu telekomunikačnej prevádzky je okrem Trestného poriadku obsiahnutá aj v zákone o ochrane pred odpočúvaním,[1119] ako aj v ZPZ. Predmetné právne predpisy sa odlišujú najmä **účelom** právnej úpravy. Kým v prípade úpravy podľa zákona o Policajnom zbore je týmto účelom získavanie informácií v rámci odhaľovania trestnej činnosti, ktoré nevyhnutne nemusí viesť k začatiu trestného stíhania, tak zákon o ochrane pred odpočúvaním upravuje podmienky používania informačno-technických prostriedkov na účely plnenia úloh v oblasti spravodajských služieb. Právna úprava podľa Trestného poriadku je preto vo vzťahu k nim *lex specialis.* To znamená, že ak sa týmto informačno-technickým prostriedkom sleduje získanie informácií, ktoré majú byť použité ako **dôkaz v trestnom konaní**, je potrebné postupovať podľa ustanovení Trestného poriadku.

V súvislosti s dotknutými procesnými inštitútmi je vhodné uviesť pár poznámok k **adresátom príkazov** podľa ustanovení § 115 a 116 TP, ktorých možno rozdeliť do dvoch skupín. Pre obe skupiny však zhodne platí, že majú k dispozícii dáta, ktoré môžu byť významným zdrojom dôkazov v trestnom konaní. Predmetné dáta sa môžu týkať obsahu alebo môžu mať charakter prevádzkových, lokalizačných či iných súvisiacich údajov. Prvou

[1117] ZÁHORA, J.: Uplatňovanie zásady primeranosti a zdržanlivosti pri využívaní informačno-technických prostriedkov v trestnom konaní v Slovenskej republike. In Časopis pro právní vědu a praxi 2018, č. 1, s. 29 - 39.
[1118] ČENTÉŠ, J.: Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. 1. vydanie. Bratislava : C. H. Beck, 2013, s. 89.
[1119] Zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov.

skupinou adresátov príkazov budú poskytovatelia služieb spĺňajúcich definičné znaky poskytovateľa služby podľa ZEK. Poskytovateľ služieb v zmysle ZEK je podnik poskytujúci elektronické komunikačné siete a služby, teda infraštruktúru, to znamená operátori a poskytovatelia internetu[1120] ako sú spoločnosti Orange, O2, Slovak Telekom, SWAN a podobne.[1121]

Druhou skupinou adresátov príkazov budú poskytovatelia služieb informačnej spoločnosti podľa zákona o elektronickom obchode.[1122] Poskytovateľ služieb informačnej spoločnosti v zmysle ustanovenia § 2 písm. b) zákona o elektronickom obchode je fyzická osoba alebo právnická osoba, ktorá na účely podnikania alebo na iné účely poskytuje služby informačnej spoločnosti prostredníctvom elektronických komunikačných sietí, spravidla za úhradu a na žiadosť príjemcu služby.[1123]

Ustanovenie § 115 TP upravuje postup **odpočúvania a zaznamenávania telekomunikačnej prevádzky**. Napriek tomu, že dotknuté ustanovenie bolo zákonodarcom koncipované primárne pre potreby odpočúvania telekomunikačnej prevádzky (napr. pevné linky, mobilné telefóny), s poukazom na zákonnú dikciu uvedenú v ods. 11 tohto ustanovenia zahŕňa aj postup zachytávania údajov, ktoré sú v reálnom čase prenášané prostredníctvom počítačového systému. V praktickej rovine pôjde napríklad o **zachytávanie obsahu** elektronickej komunikácie,[1124] ktorá v zmysle ustanovenia § 115 ods. 1 ZEK tvorí predmet telekomunikačného tajomstva, realizovanej prostredníctvom elektronickej komunikačnej siete,[1125] ktorá prebieha v reálnom čase smerom do budúcnosti. Odpočúvanie a záznam telekomunikačnej prevádzky vykonáva utajeným spôsobom príslušný útvar Policajného zboru.

[1120] V zahraničnej literatúre sa možno v tejto súvislosti stretnúť s pojmami ISPs (internet service provider) alebo IAPs (internet access provider), teda poskytovatelia internetu, resp. poskytovatelia prístupu na internet.
[1121] K tomu pozri kapitolu 1. Teoretické základy kybernetickej bezpečnosti.
[1122] Zákon č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení zákona č. 284/2002 Z. z.
[1123] K tomu pozri kapitolu 1. Teoretické základy kybernetickej bezpečnosti.
[1124] Poskytovanej prostredníctvom služieb, ako sú napríklad Gmail, Yahoo, Hotmail, ale aj prostredníctvom sociálnych sietí a aplikácií, akú sú napríklad Facebook Messenger, Skype, Viber, WhatsApp, Signal, Threema a podobne.
[1125] Vzhľadom na širokú definíciu elektronickej komunikačnej siete v ustanovení § 2 ods. 1 ZEK, možno konštatovať, že zachytávanie obsahu prenášaných správ je možné realizovať v akomkoľvek type siete, najčastejšie pôjde o internet, ale do úvahy prichádza aj interná sieť LAN či externá sieť WAN.

Odpočúvanie a záznam telekomunikačnej prevádzky môže nariadiť iba súd[1126] písomným a odôvodneným príkazom:

- v trestnom konaní o zločine, korupcii, trestných činoch extrémizmu, trestnom čine zneužívania právomoci verejného činiteľa, trestnom čine legalizácie výnosu z trestnej činnosti alebo pre iný úmyselný trestný čin, o ktorom na konanie zaväzuje medzinárodná zmluva, trestnom čine poškodzovania finančných záujmov Európskej únie podľa § 261 Trestného zákona,
- v trestnom konaní pre iný úmyselný trestný čin, ako je uvedený ustanovení § 115 ods. 1 TP, avšak výhradne so súhlasom užívateľa odpočúvaného alebo zaznamenávaného telekomunikačného zariadenia.

Zásada legitimity sa prejavuje v zákonnej formulácii ustanovenia § 115 ods. 1 prvá veta *„ak je možno dôvodne predpokladať, že budú zistené skutočnosti významné pre trestné konanie.*" V tomto ohľade si všimnime prepojenie citovaného ustanovenia s počítačovými trestnými činmi podľa Trestného zákona, ktoré, napriek tomu, že sú vo svojich základných skutkových podstatách prečinmi, možno zahrnúť do tohto výpočtu, nakoľko ide o úmyselné trestné činy, o ktorých na konanie zaväzuje medzinárodná zmluva.[1127]

Zásada proporcionality je premietnutá do ustanovenia § 115 ods. 1 druhá veta TP, ktorá podmieňuje vydanie príkazu iba v prípadoch ak *„nemožno sledovaný účel dosiahnuť inak alebo ak by bolo jeho dosiahnutie iným spôsobom podstatne sťažené*." Príkaz na odpočúvanie a záznam telekomunikačnej prevádzky možno vydať najviac na šesť mesiacov, s možnosťou opätovného predĺženia vždy o ďalšie dva mesiace. Trestný poriadok explicitne neustanovuje, ktorým subjektom sa príkaz na odpočúvanie a záznam telekomunikačnej prevádzky **doručuje.** Z povahy veci je však zrejmé, že vo väčšine prípadov podnik v zmysle ZEK (t. j. poskytovateľ internetu) nemá k dispozícii obsahové údaje komunikácie prenášanej prostredníctvom elektronických komunikačných sietí. *A contrario*, príkaz je potrebné doručiť tomu subjektu, ktorý má záujmové obsahové dáta k dispozícii, a teda adresátom príkazu bude vo väčšine prípadov poskytovateľ služieb informačnej spoločnosti v zmysle zákona o elektronickom obchode.

[1126] Predseda senátu a pred začatím trestného stíhania alebo v prípravnom konaní sudca pre prípravné konanie na návrh prokurátora.
[1127] Touto medzinárodnou zmluvou je Budapeštiansky dohovor.

Ak sa má záznam telekomunikačnej prevádzky použiť ako **dôkaz v trestnom konaní**, je potrebné k nemu vyhotoviť doslovný prepis a zároveň, ak boli týmto postupom získané údaje prenášané v reálnom čase prostredníctvom počítačového systému, je potrebné vyhotoviť presnú kópiu zaistených dát 1:1 a túto uchovať na vhodnom technickom nosiči, ktorý je súčasťou spisu.

Ustanovenie § 116 TP upravuje postup **oznámenia údajov o telekomunikačnej prevádzke.** Rovnako ako v prípade odpočúvania a záznamu telekomunikačnej prevádzky, je s ohľadom na ustanovenie § 116 ods. 6 TP možné tento postup aplikovať aj na zistenie a oznámenie údajov prenášaných prostredníctvom počítačového systému. Na rozdiel od ustanovenia § 115 TP, v režime podľa ustanovenia § 116 TP sa pôjde vtedy, ak bude potrebné zistiť ostatné údaje tvoriace predmet telekomunikačného tajomstva v zmysle ustanovenia § 117 ods. 1 ZEK, okrem obsahových údajov. To znamená, že pôjde o oznámenie **prevádzkových údajov,** [1128] **lokalizačných údajov**[1129] a **iných súvisiacich údajov komunikujúcich strán**.[1130] Kým príkaz podľa ustanovenia § 115 TP možno z povahy veci vydať iba na odpočúvanie prevádzky, ktorá sa ešte len má uskutočniť, príkaz na oznámenie údajov o telekomunikačnej prevádzke možno vydať tak do budúcna, ako aj do minulosti, čo vyplýva z dikcie ustanovenia § 116 ods. 2 štvrtá veta TP *„Ak nejde o zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke…*"

Oznámenie údajov o telekomunikačnej prevádzke môže nariadiť iba súd[1131] písomným a odôvodneným príkazom v trestnom konaní pre úmyselný trestný čin, za ktorý zákon ustanovuje trest odňatia slobody, ktorého horná hranica je najmenej tri roky, pre trestný čin ochrany súkromia v obydlí podľa § 194a, podvodu podľa § 221, nebezpečného vyhrážania podľa § 360, nebezpečného prenasledovania podľa § 360a, šírenia poplašnej

[1128] Podľa ustanovenia § 109 ods. 2 ZEK prevádzkové údaje sú údaje vzťahujúce sa na užívateľa a na konkrétny prenos informácií v sieti a vznikajúce pri tomto prenose, ktoré sa spracúvajú na účely prenosu správy v sieti alebo na účely fakturácie. Pozn.: prevádzkové údaje teda identifikujú komunikujúce strany (kto s kým napríklad telefonoval, teda zdroj a adresát komunikácie), typ komunikácie, dátum a čas, kedy sa komunikácia uskutočnila a informáciu o tom, ako dlho komunikácia trvala.

[1129] V zmysle § 109 ods. 3 ZEK lokalizačné údaje sú údaje spracúvané v sieti alebo prostredníctvom služby, ktoré označujú geografickú polohu koncového zariadenia užívateľa verejnej služby. Pozn.: lokalizačné údaje sú teda identifikátorom konkrétneho miesta, na ktorom sa zariadenie v čase uskutočnenej prevádzky nachádzalo.

[1130] Súvisiace údaje komunikujúcich strán sú s ohľadom na ustanovenie § 117 ods. 1 písm. b) ZEK telefónne číslo, obchodné meno a sídlo právnickej osoby, alebo obchodné meno a miesto podnikania fyzickej osoby – podnikateľa alebo osobné údaje fyzickej osoby, ktorými sú meno, priezvisko, titul a adresa trvalého pobytu, predmetom telekomunikačného tajomstva nie sú údaje, ktoré sú zverejnené v telefónnom zozname.

[1131] Predseda senátu a pred začatím trestného stíhania alebo v prípravnom konaní sudca pre prípravné konanie na návrh prokurátora.

správy podľa § 361, podnecovania podľa § 337, schvaľovania trestného činu podľa § 338, pre trestný čin, ktorým bola spôsobená ťažká ujma na zdraví alebo smrť alebo pre iný úmyselný trestný čin, pri ktorom na konanie zaväzuje medzinárodná zmluva. Zásada legitimity sa prejavuje v zákonnej formulácii ustanovenia § 116 TP *„...ktoré sú nevyhnutné na objasnenie skutočností dôležitých pre trestné konanie.*"

Zásada proporcionality je premietnutá do ustanovenia § 116 druhá veta TP, ktorá podmieňuje vydanie príkazu iba v prípadoch *„ak nemožno sledovaný účel dosiahnuť inak alebo ak by bolo jeho dosiahnutie iným spôsobom podstatne sťažené.*" Príkaz na oznámenie údajov o telekomunikačnej prevádzke možno vydať najviac na šesť mesiacov, s možnosťou opätovného predĺženia vždy o ďalšie dva mesiace. Príkaz sa **doručuje** podniku poskytujúcemu verejné siete alebo služby, to znamená poskytovateľovi služieb v zmysle ZEK. V súvislosti s časovým ohraničením príkazu, ktorý možno vydať za účelom získania údajov o už uskutočnenej prevádzke by sme chceli upriamiť pozornosť na nález Ústavného súdu Slovenskej republiky sp. zn. PL. ÚS 10/2014.[1132] Podľa právnej úpravy účinnej do dátumu uverejnenia predmetného nálezu bola podnikom poskytujúcim elektronické siete a služby (pozn.: poskytovateľom služieb v zmysle ZEK) uložená povinnosť uchovávať prevádzkové údaje, lokalizačné údaje a súvisiace údaje komunikujúcich strán počas šiestich mesiacov odo dňa uskutočnenia komunikácie, ak išlo o pripojenie k internetu, elektronickú poštu a telefonovanie prostredníctvom internetu, a počas dvanástich mesiacov, ak išlo o ostatné druhy komunikácie. Ústavný súd Slovenskej republiky však po vzore rozsudku *Digital Rights Ireland*[1133] vyslovil nesúlad vybraných ustanovení TP, ZPZ a ZEK s Ústavou SR a Dohovorom o ochrane ľudských práv a základných slobôd.

Postup, ktorým sa môže dotknutá osoba domáhať **preskúmania zákonnosti použitého opatrenia** či už sa týkalo odpočúvania a záznamu telekomunikačnej prevádzky podľa ustanovenia § 115 TP alebo oznámenia údajov o telekomunikačnej prevádzke podľa

[1132] Nález Ústavného súdu Slovenskej republiky sp. zn. PL. ÚS 10/2014 z 29. apríla 2015. Dostupné na: https://www.ustavnysud.sk/documents/10182/992035/PL_+%C3%9AS+10_2014.pdf (navštívené dňa 22. októbra 2020).

[1133] Vo výroku rozsudku Súdneho dvora Európskej únie (veľká komora) z 8. apríla 2014, Digital Rights Ireland a Seitlinger a i. (spojené veci C-293/12 a C-594/12) Súdny dvor vyhlásil smernicu Európskeho parlamentu a Rady 2006/24/ES z 15. marca 2006 o uchovávaní údajov vytvorených alebo spracovaných v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb alebo verejných komunikačných sietí a o zmene a doplnení smernice 2002/58/ES za neplatnú z dôvodu, že zásah do základných práv na rešpektovanie súkromného života a ochranu osobných údajov, ktorý spôsobuje všeobecná povinnosť uchovávať údaje o prenose dát a polohe, sa neobmedzoval na to, čo je prísne nevyhnutné.

ustanovenia § 116 TP je rovnaký. Po právoplatnom skončení trestnej veci dotknutú osobu informuje orgán činný v trestnom konaní alebo súd, v závislosti od toho, ktorý subjekt právoplatné meritórne rozhodnutie vydal, pričom táto osoba má právo podať v lehote dvoch mesiacov od doručenia návrh na preskúmanie zákonnosti príkazu na odpočúvanie a záznam telekomunikačnej prevádzky, respektíve návrh na preskúmanie zákonnosti príkazu na zistenie a oznámenie údajov o telekomunikačnej prevádzke na Najvyšší súd Slovenskej republiky. Najvyšší súd Slovenskej republiky v konaní podľa ustanovení § 362f a 362g TP uznesením vysloví buď porušenie zákona alebo že k porušeniu zákona nedošlo. Proti tomuto rozhodnutiu nie je prípustný opravný prostriedok.

Porovnanie údajov v informačných systémoch podľa §118 Trestného poriadku

Podstatou inštitútu je elektronické porovnávanie údajov o osobách, ktoré v informačných systémoch **vytvárajú a spravujú štátne orgány, neštátne inštitúcie a významné podnikateľské subjekty (poisťovacie spoločnosti, bankové inštitúcie, subjekty poskytujúce služby veľkému množstvu užívateľov v oblasti telekomunikácií, sieťových odvetví**), **ktorých povaha, alebo citlivosť neumožňuje ich poskytnutie prostredníctvom súčinnosti v zmysle §3 (biometrické údaje, DNA profily, rizikové profily, psychologické profily, kreditové a platobné profily osôb).** Inštitút vyjadruje zákonný zásah do práva na ochranu osobných údajov podľa článku 19 ods. 3 Ústavy SR a do práva na súkromný život podľa článku 8 ods. 1 EDĽP. **Zákonnými podmienkami pre uplatnenie tohto procesného postupu podľa §118 ods. 1 TP sú:**

a) existencia trestného konania – konania podľa TP (pozri § 10 ods. 15),

b) existencia taxatívneho trestného činu ako predmetu trestného konania – ide o úmyselný trestný čin, na ktorý TZ ustanovuje trest odňatia slobody s hornou hranicou trestnej sadzby prevyšujúcou tri roky alebo o iný úmyselný trestný čin, o ktorom na konanie zaväzuje medzinárodná zmluva[1134].; a

c) nevyhnutnosť postupu pre objasnenie trestného činu.

V zmysle §118 ods. 1 TP **predmetom porovnávania** sú údaje o osobách alebo o veciach dôležitých pre trestné konanie- o ich znakoch charakterizujúcich alebo vylučujúcich konkrétnu osobu alebo vec v informačných systémoch.

[1134] Napríklad články 34, 35 a 37 Dohovoru o právach dieťaťa prijatého 20. novembra 1989 v New Yorku – oznámenie ministerstva zahraničných vecí č. 104/1991 Zb.

Porovnávanie údajov vedených v rôznych informačných systémoch sa vykonáva na základe príkazu predsedu senátu v konaní pred súdom alebo prokurátora pred začatím trestného stíhania a v prípravnom konaní. Príkaz musí mať písomnú formu.

Ďalšími obligatórnymi náležitosťami príkazu v zmysle §118 ods. 3 TP sú:

a) označenie prevádzkovateľa informačného systému jeho zákonným, úradným alebo evidenčným názvom (obchodným menom), sídlom a inými identifikačnými znakmi a údajmi,

b) vymedzenie údajov a skúšobných znakov o osobe alebo o veci – ide o údaje a znaky týkajúce sa osobného, rodinného, sociálneho, pracovného, finančného stavu osoby a technických parametrov veci, účelu jej použitia, formy, obsahových náležitostí.

V zmysle §118 ods. 4 TP prevádzkovateľ informačného systému je povinný v zmysle príkazu poskytnúť údaje a skúšobné znaky o osobe alebo o veci podľa príkazu, a to v rozsahu potrebnom na ich porovnanie v inom informačnom systéme a to vrátane údajov a znakov, ktoré sú neoddeliteľné od požadovaných údajov v príkaze. Tzv. neoddeliteľné údaje a znaky sa smú použiť na porovnávanie s údajmi a znakmi v inom informačnom systéme, avšak v zmysle §118 ods. 4 TP nemožno ich použiť ako dôkaz v trestnom konaní.

V zmysle §118 ods. 5 TP údaje sa poskytujú na nosiči informácií alebo vo forme ich elektronického prenosu na iný nosič údajov. Po skončení porovnávania sa nosiče bezodkladne vrátia tento nosič prevádzkovateľovi informačného systému alebo sa údaje vymažú, ak boli zaslané

V zmysle §118 ods. ods. 6, ods. 7 s poukazom na ustanovenie §115 ods. 6 ak sa má záznam o výsledku porovnávania údajov a skúšobných znakov o osobe alebo o veci v informačných systémoch **použiť ako dôkaz** v trestnom konaní, **pripojí sa k nemu doslovný prepis podstatnej časti výsledkov vyhotovený orgánom činným v trestnom konaní, súdom alebo príslušníkom PZ vykonávajúcimi porovnávanie**. Prepis musí obsahovať údaje o mieste, čase a zákonnosti vykonávania porovnávania a podpis osoby, ktorá ho vyhotovila.

Prepis sa zakladá do spisu. Prepis sa spravidla neutajuje. Prepis môže byť použiteľný v inej trestnej veci ako dôkaz za kumulatívneho splnenia podmienky existencie iného trestného konania a súčasne toto trestné konanie sa musí viesť pre niektorý z trestných činov uvedených v §118 ods. 1 TP.

V zmysle §118 ods. 8 TP v prípade negatívneho výsledku porovnávania sa musia údaje i znaky bezodkladne zničiť.

Využitie systémov profilovania osôb, biometrickej kategorizácie a biometrickej identifikácie[1135]

Novú formu informačno-technického prostriedku[1136] predstavuje využitie systémov umelej inteligencie na profilovanie osôb, biometrickú kategorizáciu a biometrickú identifikáciu s cieľom vykonávať:

- profilovania osoby, že sa stane páchateľom trestného činu[1137]
- biometrickú kategorizáciu osôb,[1138] alebo
- biometrickú identifikáciu osôb reálnom čase[1139]

Ostatné formy využitia systémov umelej inteligencie v zásade možno zaradiť pod pojmy technického sledovania podľa ustanovení §113 TP, alebo vyhotovenia obrazových, zvukových, alebo obrazovo zvukových záznamov podľa §114 TP, či *packet sniffing* podľa §116 TP, alebo §91 TP, ak netvoria predmet telekomunikačného tajomstva[1140] a v zásade ich bude možné zaradiť pod existujúce právne nástroje, ktorých zákonné použitie je ustálené dlhodobou aplikačnou praxou.[1141]

Použitie systému umelej inteligencie *pre účely profilovania fyzickej osoby, že spácha trestný čin* je všeobecne zakázané. Zákaz sa vzťahuje na predvídania rizika, že osoba spácha trestný čin na základe informácií o jej štátnej príslušnosti, miesta narodenia, miesta bydliska, počtu detí, výšky dlhu alebo typu vozidla. I keď pojem profilovanie a predpovedania rizika, že osoba sa stane páchateľom trestného činu nie je nikde definované[1142] -vo všeobecnosti ide o rôzne pokročilé technológie a analytické metódy aplikované na veľký počet často

[1135] VOJTUŠ, F., KORDÍK, M.: K možnostiam a problémom získania dôkazov z asistenčných systémov vozidiel a automatizovaných vozidiel. In Právny obzor, 109, 2026, v tlači.
[1136] Porovnaj §10 ods. 20 TP.
[1137] Čl. 5 ods.1, písm.d) Aktu o umelej inteligencii.
[1138] Čl. 5 ods.1, písm.g) Aktu o umelej inteligencii.
[1139] Čl. 5 ods. 1, písm. h) Aktu o umelej inteligencii upravuje iba tzv. *live facial recognition* (LFR), identifikáciu v reálnom čase a nie identifikáciu osôb po spáchaní skutku tzv. *post event / after facial recognition* (AFR), čo predstavuje bežný postup orgánov presadzovania práva porovnávania tvárí napr. z bezpečnostných kamier po spáchaní skutku počas pátrania po horúcej stope. Porovnaj AI and Policing, EUROPOL, s. 24, dostupné dňa 21.10.2025 na: LINK
[1140] §117 ods.1 zákona č. 452/2021 Z. z. o elektronických komunikáciách v znení neskorších predpisov.
[1141] STRÉMY, T., ŠAMKO, P., KURILOVSKÁ, L. Trestný poriadok. Praktický komentár. 1. vyd. Praha : Wolters Kluwer ČR, a. s., 2024, s. 40.
[1142] Čl. 3 bode 4 smernice EÚ 2016/6801 o presadzovaní práva v oblasti ochrany údajov s poukazom na čl. 5 ods. 1 písm. d) Aktu o umelej inteligencii, profilovanie (všeobecne) vymedzuje použitím čl. 4 bode 4 Nariadenia 697/2016- všeobecného nariadenia o ochrane osobných údajov ako akúkoľvek formu automatizovaného spracúvania osobných údajov, ktoré pozostáva z použitia osobných údajov na vyhodnotenie určitých osobných aspektov týkajúcich sa fyzickej osoby, predovšetkým analýzy alebo predvídania aspektov dotknutej fyzickej osoby súvisiacich s výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom".

historických ukazovateľov (vrátane sociálno ekonomických údajov, záznamov očtk a zložiek presadzujúcich právo atď.), ktoré sa v kombinácii s kriminologickými teóriami a štatistickými metódami používajú na strategické plánovanie síl a prostriedkov orgánov presadzovania práva a prevenciu kriminality.[1143] Z uvedenej zakázanej praktiky je všeobecne vyňatá vylúčená riziková analýza páchania trestnej činnosti na základe polohy, geopriestorových informácií o spáchaní trestného činu (tzv. hot spoty) za podmienky, že rozhodnutie sa musí uskutočniť vždy individuálnym ľudským posúdením.[1144]

Biometrická kategorizácia fyzických osôb je všeobecne zakázaná, ak je cieľom odvodiť alebo vyvodiť obmedzený počet citlivých charakteristík: rasu, politické názory, členstvo v odboroch, náboženské alebo filozofické presvedčenie, sexuálny život alebo sexuálnu orientáciu.[1145] Možno však uviesť, že Akt o umelej inteligencii považuje za výnimku z uvedených zakázaných praktík biometrickej kategorizácie, tie ktoré sú právom dovolené využívať najmä zložkami presadzujúcimi právo pri plnení ich úloh, ako je tvorba rizikových analýz a predikcie páchania trestnej činnosti. resp. viktimizácie osôb najmä v spojení s terorizmom a obchodovaním s ľuďmi vo vzťahu k mladým ľuďom a deťom[1146], škálovanie osôb podľa všeobecných charakteristík pre účely rôznych identikitov, databáz častí tvare, očí, vlasov, pier apod.[1147] Selekcia a mapovanie dát biometrických údajov by mali vykonávať systémy biometrickej kategorizácie práve pre to, aby bolo zaručené, že v sume zbieraných údajov budú zastúpené všetky demografické skupiny a zber sa nebude zameriavať na jednu konkrétnu skupinu. Opäť aj v tomto prípade platí všeobecná požiadavka finálneho ľudského posúdenia.[1148]

Používanie autonómnych vozidiel so systémom umelej inteligencie s diaľkovou *biometrickou identifikáciou v reálnom čase (LFR)* vo verejne prístupných priestoroch je všeobecnosti zakázané, pretože predstavuje významný zásah do súkromia osôb. [1149] Akt o umelej inteligencii sa však neaplikuje na systémy biometrickej identifikácie nasadené v

[1143] AI and Policing, EUROPOL, s. 15, dostupné 21.10.2025 na: https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing#:~:text=With%20the%20AI%20and%20policing%20report%2C%20produced%20through,more%20efficient%2C%20responsive%20and%20effective%20law%20enforcement%20model

[1144] Rozsudok Súdneho dvora z 21. júna 2022, Ligue des droits humains, C-817/19, ECLI:EU:C:2022:491

[1145] Usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu stanovených v nariadení (EÚ) 2024/1689 z 29.7.2025, s. 100. Dostupné na LINK

[1146] AI and Policing, EUROPOL, s. 52, dostupné 21.10.2025 na: LINK

[1147] Recitál 30 Aktu o umelej inteligencii.

[1148] Poznámka pod čiarou č. 50.

[1149] Recitál 33 Aktu o umelej inteligencii.

oblasti národnej bezpečnosti, a to bez ohľadu na typ subjektu[1150] a pri predchádzaní trestnej činnosti. Ide o porovnávanie rozpoznávacích znakov osôb bez výrazného časového oneskorenia proti referenčnej databáze[1151] na verejne prístupných miestach.[1152]

Pod národnú bezpečnosť možno zahrnúť záujem na ochrane základných funkcií štátu a základných záujmov spoločnosti, taktiež zahŕňa prevenciu a represiu aktivít, ktoré smerujú proti základným politickým, ústavným alebo spoločenským štruktúram krajiny a najmä priamo ohroziť spoločnosť, obyvateľstvo alebo samotný štát, akými sú napríklad teroristické aktivity.[1153] Národná bezpečnosť nezahŕňa napríklad činnosti súvisiace s bezpečnosťou cestnej premávky[1154] alebo organizáciou či výkonom spravodlivosti.[1155]

Vo vzťahu k biometrickej identifikácií v reálnom čase v zmysle uvedeného platí, že táto je možná ak ide o:[1156]

- cielené pátranie po konkrétnych obetiach únosov, obchodovania s ľuďmi alebo sexuálneho vykorisťovania ľudí, ako aj pátranie po nezvestných osobách;
- predchádzanie konkrétnemu, závažnému a bezprostrednému ohrozeniu života alebo fyzickej bezpečnosti fyzických osôb alebo skutočnej a existujúcej alebo skutočnej a predvídateľnej hrozbe teroristického útoku;
- lokalizáciu alebo identifikáciu osoby podozrivej zo spáchania trestného činu na účel vedenia vyšetrovania alebo stíhania trestného činu alebo výkonu trestnej sankcie za trestné činy uvedené v prílohe II, za ktoré možno v dotknutom členskom štáte uložiť trest odňatia slobody alebo ochranné opatrenie obmedzujúce slobodu s hornou hranicou trestnej sadzby najmenej štyri

[1150] Rozsudok Súdneho dvora zo 6. októbra 2020, La Quadrature du Net a i., C-511/18, C-512/18 a C-520/18, EU:C:2020:791, bod 13.
[1151] Usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu stanovených v nariadení (EÚ) 2024/1689 z 29.7.2025, s. 106-107. Dostupné na LINK
[1152] Prístupnosť pre vopred nie stanovený počet osôb, nezávisle od kapacitných alebo bezpečnostných obmedzení, ako sú kúpa vstupenky alebo cestovného lístka, predchádzajúca registrácia alebo určitá veková hranica. Možnosť prístupu do priestoru, že priestor je verejne prístupný, ak existujú znaky alebo oznámenia, ktoré naznačujú opak (napríklad označenie obmedzujúce prístup) In: Usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu stanovených v nariadení (EÚ) 2024/1689 z 29.7.2025, s. 108. Dostupné na LINK
[1153] Rozsudok Súdneho dvora zo 6. októbra 2020, La Quadrature du Net a i., C-511/18, C-512/18 a C-520/18, EU:C:2020:791, bod 13.
[1154] Rozsudok Súdneho dvora z 22. júna 2021, Latvijas Republikas Saeima, C-439/19, EU:C:2021:504, bod 68.
[1155] Rozsudok Súdneho dvora z 5. júna 2023, Komisia/Poľsko, C-204/21, EU:C:2023:442, bod 319.
[1156] Čl. 5 ods.1, písm. h) body I až III Aktu o umelej inteligencii.

roky.[1157] Pričom tento postup je aplikovateľný aj v konaní o európskom zatýkacom rozkaze ako i medzinárodnom zatýkacom rozkaze.[1158]

Tieto výnimky netvoria právny základ týchto systémov. Právnym základom je vnútroštátny predpis upravujúci podmienky využívania tohto biometrického systému. Ak takýto predpis neexistuje, je používanie systému na diaľkovú identifikáciu od 1.2. 2025 zakázané.[1159]

Cielené pátranie zahŕňa lokalizáciu a identifikáciu obetí troch kategórií trestných činov:

a. *únosov*
b. *obchodovanie s ľuďmi a v*
c. *sexuálneho vykorisťovania*[1160] a
d. *pátrania po nezvestných osobách*-pri nezvestných osobách je možné zdôrazniť, že tento postup nie je postupom v rámci trestného konania, ale osobitného správneho konania, ktoré sa preto nepovažujú za postupy pri vyšetrovaní trestnej činnosti. V podmienkach SR je takýto postup upravený v §2 ods. 1, písm. l) v spojení s §69b a 81b zákona č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov a na ktoré použitie sa nevzťahuje biometrická identifikácia podľa Aktu o umelej inteligencii ale nasadenie biometrickej identifikácie podľa Všeobecného nariadenia o ochrane osobných údajov.[1161]

Konkrétne, závažné a bezprostredné ohrozenie života alebo fyzickej bezpečnosti fyzických osôb bezprostredné ohrozenie života alebo fyzickej bezpečnosti fyzických osôb ako druhý dôvod môže zahŕňať aj bezprostredné ohrozenie kritickej infraštruktúry, ak by

[1157] Terorizmus, obchodovanie s ľuďmi, sexuálne vykorisťovanie detí a detská pornografia, nedovolené obchodovanie s omamnými alebo psychotropnými látkami, nedovolené obchodovanie so zbraňami, strelivom alebo s výbušninami, vražda, ťažká ujma na zdraví, nedovolené obchodovanie s ľudskými orgánmi alebo tkanivami, nedovolené obchodovanie s jadrovými alebo rádioaktívnymi materiálmi, únos, obmedzovanie osobnej slobody alebo branie rukojemníka, trestné činy podliehajúce právomoci Medzinárodného trestného súdu, nezákonné ovládnutie lietadla alebo plavidla, znásilnenie, trestné činy proti životnému prostrediu, organizovaná alebo ozbrojená lúpež, sabotáž, účasť v zločineckej organizácii zapojenej do jedného alebo viacerých vyššie uvedených trestných činov.

[1158] Usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu stanovených v nariadení (EÚ) 2024/1689 z 29.7.2025, s. 117. Ods. 354. Dostupné na LINK

[1159] Čl. 5 ods. 5 Aktu o umelej inteligencii.

[1160] V podmienkach SR ide o trestný čin obchodovania s ľuďmi podľa § 179 TZ, trestný čin vydierania podľa § 189 TZ, trestný čin sexuálneho násilia podľa § 200, trestný čin sexuálneho zneužívania podľa § 201 TZ alebo trestný čin kupliarstva podľa § 367 TZ.

[1161] Čl. 9 Všeobecného nariadenia o ochrane osobných údajov.

narušenie alebo zničenie takejto kritickej infraštruktúry viedlo k bezprostrednému ohrozeniu života alebo fyzickej bezpečnosti osoby, a to aj v dôsledku vážnej ujmy na poskytovaní základných dodávok pre obyvateľstvo alebo výkone základných funkcií štátu."[1162] Bezprostredné ohrozenie života alebo fyzickej bezpečnosti je ohrozenie, ktorá môže nastať v ktoromkoľvek okamihu a vyžaduje si „prijatie okamžitých opatrení"[1163] Konkrétne ohrozenie znamená, že ohrozenie je jasne vymedzené, individualizované a špecifické, teda že by nemalo byť hypotetické.[1164]

Pojem *skutočná a existujúca alebo skutočná a predvídateľná hrozba teroristického útoku*, ako sa používa v článku 5 ods. 1 písm. h) bode ii) autonómnym pojmom práva Únie, a preto by sa mal v zásade posudzovať nezávisle od vnútroštátneho vymedzenia.[1165] Musí ísť o skutočnú a reálnu hrozbu.[1166]

Lokalizáciu alebo identifikáciu osoby podozrivej zo spáchania vybraných trestných činov na účel vedenia vyšetrovania alebo stíhania trestného činu alebo výkonu trestnej sankcie za vybrané trestné činy aby sa zistila/ potvrdila totožnosť špecificky zacieleného jednotlivca.[1167]

Z uvedeného vyplýva, že nemusí ísť iba o známu osobu, ale i jednotlivca, ktorého totožnosť je potrebné zistiť, ak je vyšpecifikovaný inak napr. kamerovým záznamom z bezpečnostnej kamery z miesta činu apod.

Podmienky používania systémov diaľkovej biometrickej identifikácie v reálnom čase na účely presadzovania práva vo verejne prístupných priestoroch, musia byť:[1168]

a. určité,
b. taxatívne a
c. primerané ak existuje *„nevyhnutná potreba*" dosiahnuť *„významný verejný záujem*", ktorý *„prevažuje nad rizikami*", ktoré to predstavuje pre základné práva.

[1162] Usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu stanovených v nariadení (EÚ) 2024/1689 z 29.7.2025, s. 114. Dostupné na LINK
[1163] Odôvodnenie 37 e-Evidence nariadenia.
[1164] Usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu stanovených v nariadení (EÚ) 2024/1689 z 29.7.2025, s. 115. Dostupné na LINK
[1165] Usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu stanovených v nariadení (EÚ) 2024/1689 z 29.7.2025, s. 115. Dostupné na LINK
[1166] Rozsudok Súdneho dvora z 20. septembra 2022, SpaceNet, C-793/19 (spojené veci C-793/19, C794/19), ECLI:EU:C:2022:702, bod 93.
[1167] Usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu stanovených v nariadení (EÚ) 2024/1689 z 29.7.2025, s. 120. Dostupné na LINK
[1168] Usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu stanovených v nariadení (EÚ) 2024/1689 z 29.7.2025, s. 117. Dostupné na LINK

Akékoľvek iné používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva, ktoré nie je uvedené v článku 5 ods. 1 písm. h) bodoch i) až iii) aktu o AI, je zakázané.

Vo vzťahu k prvému a tretiemu bodu výnimiek je zrejmé, že ide o identifikáciu známej osoby resp. určiteľnej osoby, ktorej totožnosť sa má zistiť [1169]a ktorej údaje sa porovnávajú voči údajom napr. z bezpečnostných kamier s použitím diaľkovej biometrickej identifikácie, s jasným cieľom stotožniť túto osobu a to i pre potreby vyšetrovania. Súčasne ide o reaktívny prístup na skutočnosť predpokladanú v danom ustanovení.

Výnimka formulovaná v bode 2 je vágnejšia, avšak v zmysle výkladu Súdneho dvora musí ísť o konkrétne skutočnosti a nie všeobecnú prevenciu pred určitou hrozbou z dôvodu „zhoršenia bezpečnostnej situácie"[1170]. Avšak aj tu platí, že je možné týmto spôsobom zisťovať totožnosť, vrátane lokalizácie.[1171]

Aplikácie umelej inteligencie v oblasti presadzovania sú taktiež vysoko rizikové vzhľadom na ich významný potenciál ovplyvniť individuálne práva a slobody.[1172] Medzi aplikácie považované za vysoko rizikové patria biometrické systémy používané na jedinečnú identifikáciu jednotlivcov, ako sú nástroje na rozpoznávanie emócií. Medzi ďalšie vysoko rizikové aplikácie patria niektoré kategorizačné systémy, ako aj systémy určené na hodnotenie rizika viktimizácie alebo páchania trestných činov prostredníctvom analýzy pravdepodobnosti, že sa jednotlivci stanú obeťami alebo páchateľmi trestných činov, vrátane obchodovania s ľuďmi, domáceho násilia alebo počítačovej kriminality, či systémy biometrickej identifikácie[1173]

Uplatnenie uvedeného systému biometrickej identifikácie v reálnom čase navyše okrem obsahuje ďalšie poistky, ktoré by mali brániť jeho zneužitiu vo forme primeranosti nebezpečnej vzniknutej situácie a primeranosti následkov pre dotknutých jednotlivcov.[1174]

Súčasne je v zmysle čl. 5 ods. 3 Aktu o umelej inteligencii pre použitie tejto výnimky potrebný súhlas nezávislej justičnej autority alebo nezávislého správneho regulačného

[1169] Čl. 2 ods. 3 Aktu o umelej inteligencii.
[1170] Rozsudok Súdneho Dvora EÚ vo veci C-203/15, Tele 2 Sverige, bod 117-119; Rozsudok Súdneho Dvora EÚ vo veci C-511/18, C-512/18, 520/18 La Quadrature, bod 150.
[1171] Usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu stanovených v nariadení (EÚ) 2024/1689 z 29.7.2025, s. 120. Dostupné na LINK
[1171] Čl. 2 ods. 3 Aktu o umelej inteligencii.
[1172] AI and Policing, EUROPOL, s. 42. Dostupné dňa 21.10.2025 na: LINK
[1173] AI and Policing, EUROPOL, s. 43, dostupné 21.10.2025 na: LINK
[1174] Čl. 5, ods. 2 Aktu o umelej inteligencii.

orgánu a to len po nevyhnutnú dobu, tento súhlas resp. príkaz je navyše možné vydať len po vykonaní rizikovej analýzy podľa čl. 27, ibaže vec neznesie odklad.[1175] Vo vzťahu k slovenským právnym reáliám, by nasadenie tohto prostriedku malo podliehať príkazu sudcu pre prípravné konanie alebo súhlasu sudcu krajského súdu analogicky podľa zákona č. 166/2003 Z. z. pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) v znení neskorších predpisov.

Posúdenie vplyvu podľa čl. 27 Aktu o umelej inteligencii, ktoré je povinné v zmysle čl. 5 ods. 2 je odlišné od posúdenia vplyvu na jednotlivca pri spracovaní osobných údajov.[1176]. Posúdenie vplyvu musí obsahovať:[1177]

- Opis používania diaľkovej biometrickej identifikácie a procesov nasadzujúceho subjektu v súvislosti s týmto používaním, spolu s jeho zamýšľaným účelom a referenčnou databázou a opisu technológie s právnym základom použitia systému
- časový úsek, frekvencia a spôsob používania vrátane súhlasu justičnej autority alebo správneho orgánu;
- kategórie osôb a skupín, ktoré sú systémom dotknuté. je potrebné rozlišovať medzi zacielenou osobou, ktorá môže byť obeťou trestného činu, páchateľom alebo podozrivou osobou, osobami, ktorých biometrické údaje sú zahrnuté v referenčnej databáze, a kategóriami osôb, ktoré sa nachádzajú v okolitých oblastiach, kde bude systém diaľkovej biometrickej identifikácie nasadený.. Dotknuté budú aj práva iných osôb, ktorých biometrické údaje sa používajú na účely porovnania, okoloidúcich a osôb, ktoré sa náhodne nachádzajú v oblasti pátrania. Opis geografického rozsahu oblasti pátrania, na ktorú sa vzťahuje systém diaľkovej biometrickej identifikácie v reálnom čase, ovplyvní aj počet osôb, ktoré sú systémom dotknuté. ;
- opatrenia na zabezpečenie ľudského dohľadu počas prevádzky systému, a spôsob interpretácie výstupov v kontexte rozhodovacieho procesu a objasniť úlohu človeka pri overovaní a interpretácii výstupov

[1175] Čl. 5 ods. 3 Aktu o umelej inteligencii.

[1176] Podľa článku 27 Smernice EÚ 2016/6801 o presadzovaní práva, článku 35 všeobecného nariadenia o ochrane osobných údajov alebo článku 39 nariadenia EÚ 2018/1725, ktorým sa stanovujú pravidlá ochrany údajov pre inštitúcie, orgány, úrady a agentúry EÚ.

[1177] Čl. 27 Aktu o umelej inteligencii a Usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu stanovených v nariadení (EÚ) 2024/1689 z 29.7.2025, s. 124-126. Dostupné na LINK

- opatrenia na zmiernenie rizika a vysvetlenie nápravných opatrení v prípade, že sa riziko naplní, vrátane postupov riešenia sťažností

12.5.4 Medzinárodná justičná spolupráca v trestných veciach

Pri bližšom skúmaní našich inteligentných mobilných telefónov zistíme, že ide o zariadenia zložené z prvkov a komponentov, ktoré pochádzajú z rôznych krajín. V súčasnosti nie je ničím výnimočným, že čip telefónu bol vyrobený v Číne, dizajnér, ktorý zariadenie doviedol do estetickej dokonalosti pôsobí v USA, vývojár, ktorý aplikáciu navrhol pracuje v technologickom laboratóriu v Južnej Kórei. Aby bola situácia o poznanie komplikovanejšia, predstavme si, že z tohto zariadenia, ktoré sa v inkriminovanom čase nachádzalo na území Slovenskej republiky bol vedený útok prostredníctvom služby, ktorej poskytovateľ má sídlo v Nemecku, pričom dáta sú reálne uchovávané na serveri, ktorý beží v Indii a následok útoku sa prejavil v Taliansku. Na načrtnutom prípade vidíme, že kľúčovým prvkom pre efektívnejšie stíhanie kybernetickej kriminality a cezhraničného zaisťovania a vykonávania dôkazov je dobre fungujúca medzinárodná spolupráca. Napriek tomu, že v mnohých prípadoch funguje medzinárodná policajná spolupráca, napríklad prostredníctvom Interpolu alebo Europolu, o niečo lepšie v porovnaní so spoluprácou justičných orgánov (súdov a prokuratúr), nakoľko je nepochybne menej byrokraticky zaťažená, je v rámci nej možné realizovať iba niektoré kategórie úkonov operatívnej povahy, ktoré nie sú primárne určené k obstarávaniu dôkazov na účely trestného konania spĺňajúcich požiadavku zákonnosti a procesnej použiteľnosti. Trestný poriadok totiž vychádza z absolútne jednoznačnej zásady, že všetky dôkazy, ktoré majú byť použité v rámci trestného stíhania vedeného v Slovenskej republike, je potrebné zaobstarať cestou právnej pomoci.[1178] Aby tieto dôkazy boli aj použiteľné, musia byť získané v súlade s právnymi predpismi vykonávajúceho, respektíve dožiadaného štátu a zároveň nesmú byť v rozpore s princípmi, na ktorých je Slovenská republika budovaná, a na ktorých dodržiavaní je potrebné bezvýhradne trvať.

Na účely tejto podkapitoly bude preto výklad vedený v zmysle medzinárodnej justičnej spolupráce v trestných veciach. Tá sa osobitne vo vzťahu k zaisťovaniu dát ako potenciálnych elektronických dôkazov realizuje vo viacerých režimoch, a to v závislosti od

[1178] KORDÍK, M.: Právny styk s cudzinou. Bratislava : C. H. Beck SK, 2017, s. 104.

toho či ide o medzinárodnú spoluprácu členských štátov Európskej únie alebo ide o medzinárodnú spoluprácu vo vzťahu k tretím krajinám.

a) medzinárodná justičná spolupráca členských štátov Európskej únie

PRÍKLAD

Základným pilierom justičnej spolupráce v trestných veciach v rámci Európskej únie je **článok 82 odsek 1 Zmluvy o fungovaní Európskej únie**, podľa ktorého má byť justičná spolupráca v trestných veciach medzi členskými štátmi založená na **zásade vzájomného uznávania** rozsudkov a iných justičných rozhodnutí, na rozdiel od medzinárodnej spolupráce s tretími krajinami, pre ktorú je príznačné používanie mechanizmov **vzájomnej právnej pomoci.**[1179] Čl. 2 odsek 1 Zmluvy o fungovaní Európskej únie poskytuje zákonodarcovi Európskej únie možnosť prijímať nariadenia a smernice. Súčasný právny rámec spolupráce členských štátov Európskej únie v trestných veciach pozostáva najmä z nasledujúcich aktov sekundárneho práva:

- **smernica 2014/41/EÚ,** [1180]
- **Dohovor o vzájomnej pomoci v trestných veciach medzi členskými štátmi Európskej únie,**[1181]
- **nariadenie (EÚ) 2018/1727,**[1182]
- **nariadenie (EÚ) 2016/794.**[1183]

Treba však mať na zreteli, že medzinárodná spolupráca členských štátov Európskej únie v trestnej oblasti sa vykonáva nielen na základe prameňov sekundárneho práva Európskej únie, ale aj na podklade rámcových rozhodnutí, napríklad **rámcové rozhodnutie**

[1179] V zahraničnej literatúre sa možno v tejto súvislosti stretnúť s pojmom MLA (*mutual legal assistance*), od ktorého je odvodený aj termín *MLAT (mutual legal assistance treaty)*, ktorým sa označuje medzinárodná zmluva uzavretá medzi dvomi alebo viacerými štátmi za účelom cezhraničnej spolupráce v trestných veciach.

[1180] Smernica Európskeho parlamentu a Rady 2014/41/EÚ z 3. apríla 2014 o európskom vyšetrovacom príkaze v trestných veciach (Ú. v. EÚ L 130, 1.5.2014).

[1181] Akt Rady z 29. mája 2000 potvrdzujúci v súlade s článkom 34 Zmluvy o Európskej únii Dohovor o vzájomnej pomoci v trestných veciach medzi členskými štátmi Európskej únie. (Ú. v. EÚ C 197, 12.7.2000).

[1182] Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1727 zo 14. novembra 2018 o Agentúre Európskej únie pre justičnú spoluprácu v trestných veciach (Eurojust) a o nahradení a zrušení rozhodnutia Rady 2002/187/SVV (Ú. v. EÚ L 295, 21.11.2018).

[1183] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/794 z 11. mája 2016 o Agentúre Európskej únie pre spoluprácu v oblasti presadzovania práva (Europol), ktorým sa nahrádzajú a zrušujú rozhodnutia Rady 2009/371/SVV, 2009/934/SVV, 2009/935/SVV, 2009/936/SVV a 2009/968/SVV (Ú. v. EÚ L 135, 24.5.2016).

Rady 2002/465/SVV,[1184] ktorým je priznaný *de facto* rovnocenný status ako aktom sekundárneho práva Európskej únie, prijatých pred nadobudnutím platnosti Lisabonskej zmluvy, keď mala policajná a justičná spolupráca v trestných veciach osobitné postavenie. Vo vzťahu k obstarávaniu dôkazov na účely trestného konania sú dôležité najmä **rámcové rozhodnutie Rady 2003/577/SVV**[1185] a **rámcové rozhodnutie Rady 2008/978/SVV**.[1186] Vzhľadom na dobu prijatia však tieto rámcové rozhodnutia trpia určitými nedostatkami, ktoré proces zaistenia dôkazov vo vykonávajúcom štáte a ich následného odovzdania vydávajúcemu štátu neúmerne predlžujú, čo má značný negatívny dopad na efektivitu.

Európsky vyšetrovací príkaz

Z toho dôvodu bola na pôde Európskej únie prijatá **smernica 2014/41/EÚ,**[1187] ktorá proces súvisiaci s obstarávaním dôkazov čiastočne zjednodušila, a to najmä s prihliadnutím na to, že umožňuje priamy styk justičných orgánov členských štátov. Z hľadiska rozsahu tzv. vyšetrovacích opatrení sa týka všetkých procesných úkonov, ktorých cieľom je zabezpečiť dôkaz na účely trestného konania. Prostredníctvom európskeho vyšetrovacieho príkazu možno realizovať nielen úkony vedúce k zaisteniu dát ako potenciálnych elektronických dôkazov, ale aj žiadať orgán iného členského štátu napríklad o vykonanie výsluchu (podozrivého, obvineného, poškodeného, svedka a znalca) prostredníctvom videokonferencie, odpočúvanie telekomunikačnej prevádzky (vrátane zachytávania obsahu elektronickej komunikácie), oznámenie údajov o telekomunikačnej prevádzke či požiadať o informácie nachádzajúce sa v databázach justičných orgánov členských štátov. Smernica 2014/41/EÚ stanovuje konkrétne podmienky, za ktorých možno vydať a zaslať európsky vyšetrovací príkaz, vrátane lehôt pripadajúcich na proces jeho uznania a vykonania. V tomto ohľade vymedzuje aj dôvody, pre ktoré možno európsky vyšetrovací príkaz neuznať a nevykonať.

[1184] Rámcové rozhodnutie Rady 2002/465/SVV z 13. júna 2002 o spoločných vyšetrovacích tímoch (Ú. v. EÚ L 162, 20.6.2002).
[1185] Rámcové rozhodnutie Rady 2003/577/SVV z 22. júla 2003 o vykonaní príkazu na zaistenie majetku alebo dôkazov v Európskej únii (Ú. v. EÚ L 196, 2.8.2003).
[1186] Rámcové rozhodnutie Rady 2008/978/SVV z 18. decembra 2008 o európskom príkaze na zabezpečenie dôkazov na účely získavania predmetov, dokumentov a údajov na použitie v konaniach v trestných veciach (Ú. v. EÚ L 350, 30.12.2008).
[1187] Smernica 2014/41/EÚ bola do právneho poriadku Slovenskej republiky transponovaná samostatným zákonom č. 236/2017 Z. z. o európskom vyšetrovacom príkaze v trestných veciach a o zmene a doplnení niektorých zákonov.

Vo vzťahu k európskemu vyšetrovaciemu príkazu je možné uviesť, že táto kapitola tvorí akúsi nadstavbu všeobecných prameňov venovaných justičnej spolupráci v trestných veciach[1188] a zameriava sa len na digitálne dôkazy.

V zmysle § 5 ZEVP, ak je potrebné vykonať vyšetrovací úkon v inom členskom štáte s cieľom získať dôkaz na účel trestného konania, **vydá predseda senátu alebo sudca európsky vyšetrovací príkaz.[1189] V prípravnom konaní vydá európsky vyšetrovací príkaz prokurátor, okrem vyšetrovacieho úkonu na ktorý sa vyžaduje súhlas súdu[1190]** a dočasného odovzdania osoby do iného členského štátu na účely vykonania vyšetrovacieho úkonu. Európsky vyšetrovací príkaz možno vydať aj na základe žiadosti obvineného, jeho zákonného zástupcu alebo jeho obhajcu. Európsky vyšetrovací príkaz možno vydať aj na účel získania dôkazu, ktorý už má vykonávajúci orgán k dispozícii.[1191] Európsky vyšetrovací príkaz možno vydať, ak

a) je to nevyhnutné a primerané na účely trestného konania a
b) vyšetrovací úkon uvedený v európskom vyšetrovacom príkaze by bolo možné za obdobných podmienok vykonať na území Slovenskej republiky.

Podľa § 7 ZEVP na zabezpečenie vybavenia európskeho vyšetrovacieho príkazu je príslušná krajská prokuratúra, v ktorej obvode sa má požadovaný vyšetrovací úkon vykonať. Ak sa na vykonanie vyšetrovacieho úkonu uvedeného v európskom vyšetrovacom príkaze vyžaduje podľa právneho poriadku Slovenskej republiky príkaz súdu, na jeho vydanie je podľa

[1188] ČENTÉŠ, J. a kol. Trestné právo procesné - Osobitná časť, 3. vydanie, Šamorín, Heuréka, 2025, 12. kapitola, s. 465-551.

[1189] S poukazom na § 2 ods. 3 TP. Smernica 2014/41 v spojení s článkom 47 Charty základných práv Európskej únie a článkom 4 ods. 3 ZEÚ sa má vykladať v tom zmysle, že bráni tomu, aby príslušný orgán členského štátu vydal európsky vyšetrovací príkaz na vykonanie prehliadok a zaistení, ako aj na výsluch svedka prostredníctvom videokonferencie, ak právna úprava tohto členského štátu neupravuje nijaký opravný prostriedok proti vydaniu takéhoto európskeho vyšetrovacieho príkazu. In: Súdny dvor EÚ, vo veci C-852/19, Gavanozov II.

[1190] Prokurátor nemá právomoc vydať v prípravnej fáze trestného konania európsky vyšetrovací príkaz v zmysle tejto smernice na získanie údajov o prenose dát a polohe, týkajúcich sa telekomunikačnej prevádzky, ak v rámci podobného vnútroštátneho konania prijatie vyšetrovacieho opatrenia na účely prístupu k takýmto údajom patrí do výlučnej právomoci sudcu. In: Súdny dvor EU, vo veci C-724/19, Specializirana prokuratura.
Pozn.: Oznámenie identifikačných údajov užívateľov účastníckych staníc a IP adries nie je predmetom telekomunikačného tajomstva, ale vyšetrovacím úkonom, na ktorý je prokurátor oprávnený. In: Súdny dvor EU, vo veci C-724/19, Specializirana prokuratura, bod 31-38, pozri aj čl. 3, bod 9 a 10 e-Evidence nariadenia.

[1191] Smernica 2014/41 sa má vykladať v tom zmysle, že nebráni tomu, aby prokurátor vydal európsky vyšetrovací príkaz, ktorého cieľom je poskytnutie (digitálnych) dôkazov, ktoré už majú v držbe príslušné orgány vykonávajúceho štátu, ak boli tieto dôkazy získané týmito orgánmi na území vydávajúceho štátu po odpočúvaní telekomunikačnej prevádzky všetkých používateľov mobilných telefónov, ktoré vďaka špeciálnemu softvéru a pozmenenému vybaveniu umožňujú šifrovanú komunikáciu po celej dĺžke spojenia, pokiaľ takéto rozhodnutie spĺňa všetky podmienky stanovené prípadne právom vydávajúceho štátu na poskytnutie takýchto dôkazov v čisto vnútornej situácii tohto štátu. In: Súdny dvor EÚ, vo veci C-670/22 Encrochat, bod 2.

§7 ods. 4 ZEVP príslušný okresný súd podľa § 16 ods. 1 Trestného poriadku v obvode krajskej prokuratúry, ktorá zabezpečuje vybavenie európskeho vyšetrovacieho príkazu. Proti európskemu vyšetrovaciemu príkazu, ktorým sa vykonáva alebo zabezpečuje určitý dôkaz, nie je prípustný opravný prostriedok.

Ak vydávajúci orgán v európskom vyšetrovacom príkaze požiada o vykonanie vyšetrovacieho úkonu súdom z dôvodu použiteľnosti vyšetrovacieho úkonu v trestnom konaní v štáte pôvodu, predloží prokurátor v tejto časti európsky vyšetrovací príkaz na vybavenie súdu podľa §16 ods. 1 TP, v ktorého obvode sa má vyšetrovací úkon vykonať. Ak predmetom európskeho vyšetrovacieho príkazu je výlučne vyšetrovací úkon, ktorý má vykonať súd z dôvodu použiteľnosti vyšetrovacieho úkonu v trestnom konaní v štáte pôvodu, na vybavenie európskeho vyšetrovacieho príkazu je príslušný súd podľa §16 ods. 1 TP, v ktorého obvode sa má vyšetrovací úkon vykonať. Ak sa na vykonanie vyšetrovacieho úkonu uvedeného v európskom vyšetrovacom príkaze vyžaduje podľa právneho poriadku Slovenskej republiky príkaz súdu, na jeho vydanie je príslušný súd podľa §16 ods. 1 TP,[1192] v obvode krajskej prokuratúry, ktorá zabezpečuje vybavenie európskeho vyšetrovacieho príkazu.

V zmysle § 11 ZEVP platia aj pre vykonanie a zabezpečenie digitálnych dôkazov všeobecné ustanovenia, kedy vykonávajúci justičný orgán odmietne vykonať európsky vyšetrovací príkaz, ak ide o prípad ne bis in idem, procesnopráv nej exempcie, nemožnosť vydať obdobný príkaz v slovenskom trestnom stíhaní, je daná príslušnosť slovenských justičných orgánov, ohrozenie bezpečnostných záujmov Slovenskej republiky, ohroziť zdroj informácií, alebo by mohol ohroziť alebo narušiť činnosť spravodajských služieb, medzinárodný záväzok, alebo iný dôvod pre ktorý nie je možné EVP vykonať.

Vykonávajúci justičný orgán rozhoduje v zmysle § 11 ods. 5 ZEVP o odmietnutí európskeho vyšetrovacieho príkazu opatrením, ktoré zašle vydávajúcemu orgánu spolu s uvedením dôvodu takého postupu. Proti opatreniu nie je prípustný opravný prostriedok. V zmysle § 13 ZEVP pri výkone európskeho vyšetrovacieho príkazu je potrebné dodržiavať formálne náležitosti a postupy v ňom uvedené, pokiaľ nie sú v rozpore so základnými zásadami právneho poriadku Slovenskej republiky; ak nie je možné v danom prípade tieto náležitosti alebo postupy dodržať, vykonávajúci justičný orgán o tom bezodkladne vyrozumie

[1192] S účinnosťou od 1.1.2023 „okresný súd podľa § 16 ods. 1 TP".

vydávajúci orgán. Inak sa pri výkone európskeho vyšetrovacieho príkazu postupuje podľa právneho poriadku Slovenskej republiky.

V zmysle § 14 ZEVP na posilnenie zásady proporcionality vykonávajúci justičný orgán môže použiť iný vyšetrovací úkon ako je vyšetrovací úkon uvedený v európskom vyšetrovacom príkaze, ak by sa takým úkonom dosiahol rovnaký výsledok, a tento úkon by v menšej miere zasahoval do práv dotknutej osoby ako vyšetrovací úkon uvedený v európskom vyšetrovacom príkaze, **čo môže byť významne aj pri získavaní digitálnych dôkazov.**

V zmysle § 15 ZEVP európsky vyšetrovací príkaz nemožno vykonať, ak vyšetrovací úkon uvedený v európskom vyšetrovacom príkaze nie je v právnom poriadku Slovenskej republiky upravený, alebo by ho nebolo možné vykonať v obdobnom vnútroštátnom prípade v trestnom konaní vedenom v Slovenskej republike, a zároveň nemožno použiť iný vyšetrovací úkon, ktorým by sa dosiahol rovnaký výsledok, a ktorý by nezasahoval do práv dotknutej osoby vo väčšej miere ako vyšetrovací úkon uvedený v európskom vyšetrovacom príkaze. Toto neplatí, ak bol európsky vyšetrovací príkaz vydaný na

- **získanie informácie alebo dôkazu, ktorý má vykonávajúci justičný orgán už k dispozícii, ak ho možno podľa právneho poriadku Slovenskej republiky na účely iného konania poskytnúť,**[1193]
- **získanie údajov z evidencií a informačných systémov policajných orgánov alebo justičných orgánov, do ktorých má vykonávajúci justičný orgán priamy prístup,**
- **vykonanie výsluchu osoby,**
- **zistenie totožnosti používateľa určitého telefónneho čísla alebo IP adresy,**
- **vykonanie vyšetrovacieho úkonu podľa právneho poriadku Slovenskej republiky, ktorý nevyžaduje vydanie rozhodnutia justičného orgánu a nezasahuje do základných ľudských práv a slobôd.**[1194]

[1193] Prípad medzi nemeckými justičnými orgánmi a francúzskymi justičnými orgánmi v prípade veci Súdny dvor EÚ, vo veci C-670/22 ENCROCHAT.

[1194] Napr. Doručovanie písomností, previerky pobytu, miesta, previerky v katastri nehnuteľností, obchodnom registri, nedoplatkoch na daňových a odvodových povinnostiach. Okruh týchto postupov úzko súvisí napr. s rozsahom informácií podľa čl. 6 ods. 2 Smernice EÚ 2024/1260 o vymáhaní majetku a konfiškácii, o ktoré je možné žiadať aj podľa úpravy Smernice EÚ 2024/1260 o konfiškáciách, prostredníctvom útvaru ARO, avšak v kratších lehotách.

Informácie o bankových a iných finančných operáciách v inom členskom štáte/ Informácie o bankových a iných finančných operáciách a účtoch v banke alebo finančnej inštitúcii na území Slovenskej republiky

I keď informácie o bankových a finančných operáciách nie sú samé o sebe digitálnym dôkazom, majú však veľký význam pre účely boja proti podvodom, resp. prepojení krypto aktív s FIAT[1195] menami. V zmysle § 27 ZEVP vydávajúci orgán môže vydať európsky vyšetrovací príkaz aj na účely zistenia informácií

- **o majiteľovi účtu v banke alebo finančnej inštitúcii so sídlom na území iného členského štátu, alebo o osobe, ktorá má dispozičné právo k účtu, a o ďalších skutočnostiach o tomto účte, alebo**
- **o transakciách na účte vedenom v banke alebo finančnej inštitúcii počas určitého časového obdobia vrátane informácií o účtoch, z ktorých alebo na ktoré boli tieto transakcie vykonané.**

Vydávajúci orgán v európskom vyšetrovacom príkaze uvedie dôvod, pre ktorý má za to, že informácia o majiteľovi účtu a transakciách je dôležitá pre trestné konanie, dôvod, pre ktorý má za to, že účet je vedený v banke alebo finančnej inštitúcii v inom členskom štáte, a súčasne všetky dostupné informácie, ktoré môžu vykonanie európskeho vyšetrovacieho príkazu uľahčiť.

Vykonávajúci justičný orgán (Slovenskej republiky) v zmysle § 28 ZEVP poskytne na základe európskeho vyšetrovacieho príkazu vydávajúcemu orgánu informácie (vyššie) v rozsahu,
v akom sú tieto informácie banke alebo finančnej inštitúcii nachádzajúcej sa na území Slovenskej republiky známe, pričom, ak banka takýmito informáciami nedisponuje, vykonávajúci justičný orgán odmietne vykonať európsky vyšetrovací príkaz.

Odpočúvanie a záznam telekomunikačnej prevádzky s technickou pomocou iného členského štátu/ Odpočúvanie a záznam telekomunikačnej prevádzky s technickou pomocou Slovenskej republiky

[1195] Pojem označujúci vládami štátov vydávané meny, ktoré sú všeobecne akceptovateľné vyjadrenia hodnoty (USD, EURO, Yen, Libra, Juan, Koruna, Líra atď.) **bez krytia zlatom.** Latinský pôvod slova „nech sa stane", „nech bude" znamená prísľub stanovenej hodnoty pri peňažných transakciách.

Vydávajúci orgán môže vydať európsky vyšetrovací príkaz v zmysle § 34 ZEVP aj na účely odpočúvania a záznamu telekomunikačnej prevádzky v inom členskom štáte, ak sa vyžaduje technická pomoc tohto členského štátu. **Ak technickú pomoc na odpočúvanie a záznam telekomunikačnej prevádzky môže poskytnúť viac členských štátov, vydávajúci orgán zašle európsky vyšetrovací príkaz len jednému z nich a uprednostní členský štát, v ktorom sa odpočúvaná osoba nachádza alebo má nachádzať.** Vydávajúci orgán v európskom vyšetrovacom príkaze uvedie údaje nevyhnutné na zistenie totožnosti odpočúvanej osoby, dobu, počas ktorej má byť odpočúvanie vykonávané, a potrebné technické údaje. Odpočúvanie možno vykonať:

- priamym prístupom k telekomunikačnej prevádzke vo vykonávajúcom štáte zo Slovenskej republiky, alebo
- odpočúvaním a záznamom telekomunikačnej prevádzky vo vykonávajúcom štáte.

Ak to **vyžadujú okolnosti prípadu, vydávajúci orgán môže požiadať vykonávajúci justičný orgán o prepis, dekódovanie alebo dešifrovanie** záznamu telekomunikačnej prevádzky.

Ak sú splnené podmienky v zmysle § 34 ZEVP na výkon európskeho vyšetrovacieho príkazu na účely odpočúvania a záznamu telekomunikačnej prevádzky v Slovenskej republike s technickou pomocou Slovenskej republiky a podmienky podľa § 115 Trestného poriadku, vykonávajúci justičný orgán predloží návrh na vydanie príkazu na odpočúvanie a záznam telekomunikačnej prevádzky na území Slovenskej republiky súdu, v územnom obvode ktorého zabezpečuje prokurátor krajskej prokuratúry vybavenie európskeho vyšetrovacieho príkazu; pritom sa primerane postupuje podľa § 115 Trestného poriadku.[1196]

Vykonávajúci justičný orgán odmietne vykonať európsky vyšetrovací príkaz vydaný na účely odpočúvania a záznamu telekomunikačnej prevádzky v Slovenskej republike, možno okrem všeobecných dôvodov podľa §11 ZEVP aj vtedý okrem všeobecných dôvodov uvedených v § 11 **aj vtedy, ak príkaz nebolo možné vydať na účely trestného konania vedeného v Slovenskej republike v obdobnom vnútroštátnom prípade.**

[1196] Opatrenie súvisiace s infiltráciou koncových zariadení, ktorého cieľom je získať údaje o prenose dát, polohe a komunikácii internetovej komunikačnej služby predstavuje „odpočúvanie telekomunikačnej prevádzky, In: Súdny dvor EÚ, vo veci C-670/22 EncroChat, bod 3. rozsudku.

Vykonávajúci justičný orgán dohodne s vydávajúcim orgánom, či sa európsky vyšetrovací príkaz vykoná priamym prístupom k telekomunikačnej prevádzke v Slovenskej republike zo štátu pôvodu, alebo odpočúvaním a záznamom telekomunikačnej prevádzky v Slovenskej republike.

Ak o to požiada vydávajúci orgán a je to technicky možné, záznam telekomunikačnej prevádzky sa prepíše, dekóduje alebo dešifruje; to neplatí, ak s tým vykonávajúci justičný orgán nesúhlasí. Náklady podľa prvej vety znáša štát pôvodu.

Cezhraničné odpočúvanie bez technickej pomoci iného členského štátu/ Cezhraničné odpočúvanie bez technickej pomoci Slovenskej republiky

Ak bol v zmysle § 35 ZEVP vydaný príkaz na odpočúvanie a záznam telekomunikačnej prevádzky, ktorý sa má vykonať zo Slovenskej republiky na území iného členského štátu bez jeho technickej pomoci **(ďalej len „cezhraničné odpočúvanie"),** prokurátor a po podaní obžaloby súd informuje orgán tohto členského štátu o takom odpočúvaní **bez zbytočného odkladu po tom, ako sa dozvie, že sa odpočúvaná osoba počas odpočúvania nachádza, bude nachádzať alebo sa nachádzala na území tohto členského štátu**. Na tento účel sa použije formulár, ktorého vzor je uvedený v prílohe č. 4 ZEVP preložený do úradného jazyka alebo jedného z úradných jazykov členského štátu, do ktorého sa má zaslať, alebo do jazyka, v ktorom ho tento štát podľa svojho vyhlásenia prijíma. V tomto prípade nie je potrebné vydávať na účely odpočúvania a záznamu telekomunikačnej prevádzky európsky vyšetrovací príkaz.

Odpočúvanie musí byť ukončené najneskôr do 96 hodín po tom, ako orgán iného členského štátu oznámi príslušnému prokurátorovi alebo súdu, že s jeho vykonaním na svojom území nesúhlasí.

Jedná sa o prípady, kedy je odpočúvanie technicky vykonávané bez akéhokoľvek zapojenia v vykonávajúceho štátu **napr. ide o odpočúvanie aplikácií, mailov apod.**

Podľa § 36 ZEVP na rozhodovanie o udelení súhlasu s odpočúvaním a záznamom telekomunikačnej prevádzky, ktorý je, bol alebo má byť vykonaný z iného členského štátu na území Slovenskej republiky bez technickej pomoci Slovenskej republiky, alebo s jeho pokračovaním a na súvisiace úkony, je príslušný Mestský súd Bratislava I.**Súhlas s vykonaním odpočúvania alebo s jeho pokračovaním je možné udeliť len pri splnení podmienok uvedených v § 115 Trestného poriadku.**

Príslušný súd o udelení súhlasu vyrozumie orgán iného členského štátu do 96 hodín od prijatia oznámenia o odpočúvaní. Ak súhlas s odpočúvaním nebol udelený, príslušný súd oznámi orgánu iného členského štátu, že informácie získané prostredníctvom cezhraničného odpočúvania nemôžu byť použité na účely trestného konania vedeného v tomto členskom štáte, alebo že môžu byť použité len pri splnení podmienok, ktoré príslušný súd určí; v oznámení sa uvedie dôvod, pre ktorý je potrebné také podmienky splniť.

Zaistenie veci v inom členskom štáte na vykonanie dokazovania v Slovenskej republike/Zaistenie veci v Slovenskej republike na vykonanie dokazovania v inom členskom štáte

Vydávajúci orgán môže vydať európsky vyšetrovací príkaz podľa § 37 ZEVP aj na účely zaistenia veci nachádzajúcej sa vo vykonávajúcom štáte, ktorá má byť použitá ako dôkaz[1197] na území Slovenskej republiky; v európskom vyšetrovacom príkaze sa uvedie, či má byť vec odovzdaná Slovenskej republike, alebo má byť zaistená vo vykonávajúcom štáte počas doby uvedenej v európskom vyšetrovacom príkaze, avšak na získanie vecisa neplikujte

Ak vec, ktorá bola zaistená vo vykonávajúcom štáte na základe európskeho vyšetrovacieho príkazu, nie je na ďalšie konanie potrebná, a ak neprichádza do úvahy jej prepadnutie alebo zhabanie, vydávajúci orgán o tejto skutočnosti bezodkladne informuje vykonávajúci justičný orgán.

Vykonávajúci justičný orgán spravidla do 24 hodín od doručenia európskeho vyšetrovacieho príkazu na účely zaistenia veci nachádzajúcej sa na území Slovenskej republiky, ktorá má byť použitá ako dôkaz v štáte pôvodu, posúdi, či sú splnené podmienky na jeho výkon, a informuje o tom vydávajúci orgán.

V súčasnosti sa teda medzinárodná spolupráca členských štátov Európskej únie vo vzťahu k zaisťovaniu dát ako potenciálnych elektronických dôkazov[1198] realizuje v drvivej väčšine prípadov prostredníctvom európskeho vyšetrovacieho príkazu, čo však nevylučuje použitie existujúcich bilaterálnych medzinárodných zmlúv o právnej pomoci v trestných

[1197]Mobilný telefón, PC, notebook, tablet a pod.

[1198] Hoci smernica 2014/41/EÚ neobsahuje legálnu definíciu pojmu elektronický dôkaz, v recitáli 30 smernice 2014/41/EÚ sa uvádza, že možnosti spolupráce pri odpočúvaní telekomunikačnej prevádzky by sa nemali obmedzovať na obsah telekomunikačnej prevádzky, ale mohli by sa vzťahovať aj na zhromažďovanie prevádzkových údajov a lokalizačných údajov spojených s takouto telekomunikačnou prevádzkou, a to vrátane prevádzkových údajov a lokalizačných údajov týkajúcich sa minulej, teda už uskutočnenej, telekomunikačnej prevádzky.

veciach, ktoré môžu upravovať proces zaisťovania dát odchylne a z časového aspektu efektívnejšie.[1199]

V uplynulých rokoch na pôde Európskej únie však osobitne vyvstala otázka súvisiaca so zjednodušením procesu obstarávania elektronických dôkazov v trestnom konaní, pretože existujúce mechanizmy nie sú dostatočne efektívne. Európska únia preto prijala dva akty v rámci tzv. e-evidence balíka, a to smernicu[1200] a nariadenie.[1201]

Dominantným prvkom nariadenia je prijatie dvoch nových nástrojov, a to európskeho príkaz na predloženie dôkazov a európskeho príkazu na uchovanie dôkazov, ktoré majú byť doplnkom k európskemu vyšetrovaciemu príkazu v trestných veciach. V zmysle právnej úpravy by mal **európsky príkaz na predloženie dôkazov** umožňovať vydávajúcemu justičnému orgánu členského štátu získať dáta ako potenciálny elektronický dôkaz v trestnom konaní (napríklad e-maily, obsah komunikácie realizovane prostredníctvom aplikácií, ako aj iné dôležité údaje napomáhajúce identifikácii páchateľa) priamo od poskytovateľa služieb[1202] alebo od jeho právneho zástupcu v inom členskom štáte Európskej únie, ktorý bude povinný záujmové dáta vydať do desiatich dní alebo v núdzových prípadoch do šiestich hodín. Účelom prijatia **európskeho príkazu na uchovanie dôkazov** je to, aby bolo vykonávajúcemu justičnému orgánu členského štátu umožnené žiadať o uchovanie dát ako potenciálnych elektronických dôkazov v trestnom konaní priamo poskytovateľa služieb alebo jeho právneho zástupcu, a to za účelom ich možného následného predloženia na základe európskeho príkazu na predloženie dôkazov, európskeho vyšetrovacieho príkazu alebo cestou právnej pomoci.

[1199] Vzhľadom na osobitné postavenie Spojeného kráľovstva, Írska a Dánska v rámci Európskej únie, tieto štáty oznámili, že sa na prijatí smernice 2014/41/EÚ nebudú zúčastňovať, a tak ňou nie sú viazané ani nepodliehajú jej uplatňovaniu. To znamená, že medzinárodná spolupráca Slovenskej republiky s týmito krajinami vo vzťahu k obstarávaniu dôkazov na účely trestného konania ide v obdobnom režime ako keby boli v postavení tretích krajín, to znamená, že treba skúmať či existuje medzinárodná zmluva o právnej pomoci medzi týmito štátmi na jednej strane a Slovenskou republikou na druhej strane.

[1200] Smernica Európskeho parlamentu a Rady (EÚ) 2023/1544 z 12. júla 2023, ktorou sa stanovujú harmonizované pravidlá určovania určených prevádzkarní a vymenúvania právnych zástupcov na účely zhromažďovania dôkazov v trestnom konaní, Ú. v. EÚ L 191, , s. 181–190

[1201] Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1543 z 12. júla 2023 o európskych príkazoch na predloženie elektronických dôkazov a európskych príkazoch na uchovanie elektronických dôkazov v trestnom konaní a na výkon trestu odňatia slobody v nadväznosti na trestné konanie, Ú. v. EÚ L 191, , s. 118 - 180.

[1202] Nariadenie v čl. 3 ods. 3 vymedzuje aj definičné kritériá poskytovateľa služieb, ktorým je akákoľvek právnická osoba alebo fyzická osoba poskytujúca elektronické komunikačné služby, služby informačnej spoločnosti (vrátane sociálnych sietí, online trhov, hostingových služieb) a služby týkajúce sa názvov internetových domén a čísel IP adries (najmä poskytovatelia IP adries a registrátori domén).

Hlavným cieľom smernice je určiť adresátov príkazov na predloženie a uchovanie dôkazov, ktoré majú v držbe poskytovatelia služieb prostredníctvom splnomocnených právnych zástupcov, ktorí budú zodpovední za prijímanie, dodržiavanie a vykonávanie obsahu týchto príkazov v mene poskytovateľov služieb. Povinnosť určiť právneho zástupcu sa bude týkať tých poskytovateľov služieb, ktorí nie sú usadení v Európskej únii, ale ponúkajú v jej priestore svoje služby. Smernicu možno ponímať aj ako reakciu Európskej únie na prijatie kontroverzného zákona CLOUD *(The Clarifying Lawful Overseas Use of Data Act)* Spojenými štátmi americkými s extra-teritoriálnou pôsobnosťou, na základe ktorého je možné, aby americké orgány činné v trestnom konaní žiadali americké súdy o sprístupnenie údajov od poskytovateľov elektronických komunikačných služieb, a to bez ohľadu na to či sa záujmové údaje fyzicky nachádzajú na území USA.

b) medzinárodná spolupráca s tretími krajinami

Medzinárodná spolupráca Slovenskej republiky v trestných veciach s tretími krajinami, teda krajinami, ktoré nie sú členskými štátmi Európskej únie je realizovaná v dvoch režimoch, a to v závislosti od existencie, respektíve neexistencie bilaterálnej, prípadne multilaterálnej medzinárodnej zmluvy o vzájomnej právnej pomoci v trestných veciach, ktorá zaväzuje zmluvné strany kooperovať. Z pohľadu prameňov práva je justičná spolupráca v trestných veciach upravená jednak v **multilaterálnych** a **bilaterálnych medzinárodných zmluvách**, ktorými je Slovenská republika viazaná a taktiež normami **piatej časti Trestného poriadku**, ktoré sa použijú subsidiárne. Charakteristickým znakom justičnej spolupráce s tretími krajinami je, že príslušné justičné orgány štátov nekomunikujú priamo, ale formou diplomatického, konzulárneho styku cez zastupiteľské úrady či prostredníctvom ústredných orgánov štátnej správy (Ministerstvo spravodlivosti Slovenskej republiky) alebo prostredníctvom iných orgánov verejnej moci (Generálna prokuratúra Slovenskej republiky).

Prvý režim zahŕňa situácie, kedy medzi Slovenskou republikou a tretím štátom existuje uzavretá medzinárodná zmluva o právnej pomoci v trestných veciach. Môže ísť pritom buď o dvojstrannú alebo viacstrannú medzinárodnú zmluvu o vzájomnej pomoci v trestných veciach. Vhodným príkladom multilaterálneho nástroja je **Dohovor o počítačovej kriminalite**, ktorý v tretej kapitole obsahuje osobitné ustanovenia týkajúce sa

medzinárodnej spolupráce.[1203] Tento dokument, ktorý vzišiel z iniciatívy Rady Európy bol uznaný aj Európskou úniou ako hlavný viacstranný rámec na boj proti kybernetickej kriminalite v rámci stratégie kybernetickej bezpečnosti z roku 2013.[1204] V súvislosti s posilnením spolupráce zmluvných strán v oblasti zaisťovania dát ako potenciálnych elektronických dôkazov v trestnom konaní bol v roku 2021 prijatý Druhý dodatkový protokol k Budapeštianskemu dohovoru.[1205]

Vzhľadom na to, že poskytovatelia služieb ako Facebook, X či Google majú sídlo v USA, osobitne dôležitým inštrumentom je tiež bilaterálna **Dohoda o vzájomnej právnej pomoci s USA,**[1206] ako aj **Dohoda o vzájomnej právnej pomoci s Japonskom**[1207] uzavretá medzi Európskou úniou na jednej strane a USA, respektíve Japonskom na strane druhej. Obe zmluvy však predstavujú komplementárny nástroj vo vzťahu k existujúcim dvojstranným zmluvám členských štátov Európskej únie s týmito krajinami.

V prípadoch, kedy Slovenská republika nemá uzatvorenú medzinárodnú zmluvu o právnej pomoci v trestných veciach s tretím štátom, je plne na mieste postup podľa ustanovení **piatej časti Trestného poriadku** upravujúcej problematiku právneho styku s cudzinou.[1208] Zároveň však, rešpektujúc princíp prednosti a priamej použiteľnosti medzinárodných zmlúv, táto časť Trestného poriadku slúži aj na vykonávanie medzinárodných zmlúv v rozsahu, v ktorom zákonná úprava nie je v rozpore s ustanoveniami medzinárodnej zmluvy. Význam tejto úpravy vo vzťahu k medzinárodným zmluvám je predovšetkým pri tých zmluvách, ktoré upravujú len rámcovú povinnosť spolupracovať, avšak neobsahujú potrebnú úpravu vykonávania jednotlivých inštitútov.[1209] Vo vzťahu k obstarávaniu a vykonávaniu dôkazov na účely trestného konania (čo v intenciách

[1203] K tomu pozri bližšie podkapitolu 12.5.4 Kybernetická kriminalita v medzinárodnoprávnych dokumentoch a právnych aktoch Európskej únie.
[1204] Spoločné oznámenie Komisie a vysokej predstaviteľky Únie pre zahraničné veci a bezpečnostnú politiku o stratégii kybernetickej bezpečnosti Európskej únie: Otvorený, bezpečný a chránený kybernetický priestor, JOIN (2013) 1 final.
[1205] K dátumu vydania tejto učebnice sa Slovenská republika stále nestala signatárom Druhého dodatkového protokolu k Budapeštianskemu dohovoru.
[1206] Rozhodnutie Rady 2009/820/SZBP z 23. októbra 2009 o uzavretí v mene Európskej únie Dohody o extradícii medzi Európskou úniou a Spojenými štátmi americkými a Dohody o vzájomnej právnej pomoci medzi Európskou úniou a Spojenými štátmi americkými (Ú. v. EÚ L 291, 7. november 2009, s. 40).
[1207] Rozhodnutie Rady 2010/616/EÚ zo 7. októbra 2010 o uzavretí Dohody medzi Európskou úniou a Japonskom o vzájomnej právnej pomoci v trestných veciach (Ú. v. EÚ L 271, 15. október 2010, s. 3).
[1208] Vyplýva to aj z ustanovenia § 478 TP, podľa ktorého sa ustanovenia tejto časti Trestného poriadku použijú, ak medzinárodná zmluva neustanovuje inak.
[1209] KORDÍK, M.: Právny styk s cudzinou. Bratislava : C. H. Beck SK, 2017, s. 18.

ustanovenia § 531 TP[1210] možno subsumovať pod pojem právna pomoc vo vzťahu k cudzine) sa aplikujú ustanovenia piatej hlavy piatej časti Trestného poriadku, ktorá upravuje postup pri vykonávaní úkonov právnej pomoci na základe **princípu vzájomnosti (reciprocita).** Vzájomnosť možno definovať ako záväzok Slovenskej republiky vyhovieť žiadosti cudzieho štátu alebo uistenie Slovenskej republiky, že žiadosti Slovenskej republiky bude vyhovené v cudzom štáte, ak by Slovenská republika alebo cudzí štát v obdobnom prípade postupoval rovnako. Podobnosť prípadu je potrebné posudzovať najmú s prihliadnutím na skutkové okolnosti prípadu a konkrétnu formu a obsah spolupráce, o ktorú sa v minulosti žiadalo a ktorá bola poskytnutá a prijatá.[1211] Keďže Trestný poriadok vychádza zo zásady, že priamy styk orgánov Slovenskej republiky žiadajúcich právnu pomoc v cudzine je možný len na základe medzinárodnej zmluvy, tak vo všetkých ostatných prípadoch je potrebné dožiadanie zasielať sprostredkovane cez Generálnu prokuratúru Slovenskej republiky alebo cestou Ministerstva spravodlivosti Slovenskej republiky, a to v závislosti od štádia trestného konania.

[1210] V zmysle ustanovenia § 531 TP sa právnou pomocou rozumejú úkony po začatí trestného konania v Slovenskej republike, vykonávané v cudzine na základe dožiadania slovenských orgánov alebo takéto úkony vykonávané na území Slovenskej republiky na základe dožiadania cudzích orgánov, najmä doručovanie písomností, výsluch osôb a vykonávanie ďalších dôkazov.
[1211] KORDÍK, M.: Právny styk s cudzinou. Bratislava : C. H. Beck SK, 2017, s. 28.

13. KYBERNETICKÁ BEZPEČNOSŤ OPERAČNÝCH TECHNOLÓGIÍ (OT)

Operačné technológie (Operational Technology, OT) predstavujú programovateľné systémy alebo zariadenia, ktoré priamo interagujú s fyzickým prostredím alebo riadia zariadenia, ktoré s fyzickým prostredím interagujú. Ich základnou funkciou je zisťovanie, monitorovanie a vyvolávanie priamych zmien v zariadeniach, procesoch a udalostiach. Do tejto kategórie patria najmä priemyselné riadiace systémy, systémy správy budov, protipožiarne systémy či mechanizmy fyzickej kontroly prístupu.[1212] Na rozdiel od klasických informačných technológií, ktorých primárnym cieľom je spracovanie, uchovávanie a prenos dát, OT systémy zabezpečujú kontinuitu fyzických procesov, a preto ich narušenie môže mať bezprostredné dôsledky na bezpečnosť osôb, prevádzku podnikov aj fungovanie kritickej infraštruktúry.

Pojem OT sa často používa zameniteľne s pojmom priemyselné riadiace systémy (Industrial Control Systems, ICS), avšak ICS predstavujú iba podmnožinu OT. ICS zahŕňajú siete informačných systémov určených na riadenie priemyselných procesov, ako sú výroba, manipulácia s produktmi, produkcia či distribúcia. Ide o všeobecný pojem, ktorý zahŕňa viaceré typy riadiacich systémov, najmä systémy SCADA (Supervisory Control and Data Acquisition), distribuované riadiace systémy (Distributed Control Systems, DCS) a ďalšie konfigurácie riadenia, medzi ktoré patria aj programovateľné logické automaty (Programmable Logic Controllers, PLC). Priemyselný riadiaci systém je tvorený kombináciou elektrických, mechanických, hydraulických alebo pneumatických komponentov, ktoré spoločne zabezpečujú dosiahnutie konkrétneho priemyselného cieľa, napríklad výroby, dopravy materiálu alebo distribúcie energie.[1213]

Kybernetická bezpečnosť OT sa v posledných rokoch stala jednou z kľúčových tém bezpečnostnej praxe aj regulácie. Dôvodom je predovšetkým rastúca prepojenosť OT a IT

[1212] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. NIST Special Publication 800-37 Rev. 2 [online]. Gaithersburg, MD: National Institute of Standards and Technology, 2018. Dostupné na: DOI: 10.6028/NIST.SP.800-37r2 .

[1213] STOUFFER, Keith; PEASE, Michael; TANG, CheeYee; ZIMMERMAN, Timothy; PILLITTERI, Victoria; LIGHTMAN, Suzanne; HAHN, Adam; SARAVIA, Stephanie; SHERULE, Aslam and THOMPSON, Michael. Guide to Operational Technology (OT) Security. NIST Special Publication 800-82 Rev. 3 [online]. Gaithersburg, MD: National Institute of Standards and Technology, 2023 Dostupné na: DOI: 10.6028/NIST.SP.800-82r3.

prostredí, ktorá síce prináša vyššiu efektivitu, lepšiu správu procesov a nové obchodné možnosti, no zároveň významne rozširuje priestor pre útoky. Tradične boli OT systémy navrhované s dôrazom na spoľahlivosť, dostupnosť a bezpečnú prevádzku, nie však s dôrazom na odolnosť voči moderným kybernetickým hrozbám. Ich architektúra preto často vychádza zo zastaraných technológií, uzavretých protokolov a dlhých životných cyklov zariadení, čo sťažuje zavádzanie bezpečnostných opatrení porovnateľných s tými, ktoré sa uplatňujú v IT prostredí.

Prostredie hrozieb OT je dynamické a rýchlo sa vyvíja. Jedným z hlavných faktorov tohto vývoja sú technologické zmeny. Podniky čoraz intenzívnejšie prepájajú OT siete s IT infraštruktúrou, pričom tento trend je podporovaný viacerými faktormi. Medzi najvýznamnejšie patrí široká dostupnosť zariadení s podporou IP komunikácie, nižšie náklady na komerčne dostupný softvér (commercial off-the-shelf), potreba dosahovať prevádzkové úspory a synergické efekty s podnikovými procesmi, ako aj rastúca požiadavka na vzdialený prístup a vzdialenú podporu.[1214] Tieto technologické posuny zásadne transformovali priemyselnú prevádzku, no súčasne vytvorili nové zraniteľnosti, ktoré bezpečnostné rámce často nestíhajú reflektovať.

Problémom je najmä to, že zavádzanie nových technológií v OT prostredí často prebieha rýchlejšie než budovanie primeraných bezpečnostných mechanizmov. V dôsledku toho vzniká prostredie, v ktorom sú osvedčené bezpečnostné postupy buď nedostatočne rozvinuté, alebo sa uplatňujú nekonzistentne. Osobitne rizikový je rastúci počet zariadení podobných ICS, ktoré sú priamo dostupné z internetu.[1215] Takáto dostupnosť zvyšuje pravdepodobnosť prieskumu, zneužitia nesprávnej konfigurácie, útokov na zraniteľnosti a neoprávneného prístupu zo strany škodlivých aktérov.

Významným zdrojom rizika je aj rozširovanie zmluvných vzťahov s dodávateľmi, najmä ak tieto vzťahy zahŕňajú ustanovenia o vzdialenom prístupe do OT prostredia. Hoci vzdialená správa a údržba prinášajú prevádzkové výhody, zároveň vytvárajú nové vektory útokov. Útočníci môžu zneužiť slabé miesto v bezpečnosti tretej strany a prostredníctvom dodávateľského reťazca preniknúť do interných systémov organizácie. Nedostatok

[1214] ISA: https://gca.isa.org/blog/it-ot-convergence-managing-the-cybersecurity-risks

[1215] KOPŘIVA, Jan. It appears that the number of industrial devices accessible from the internet has risen by 30 thousand over the past three years [online]. SANS Internet Storm Center, 22 April 2024 Dostupné na: https://isc.sans.edu/diary/It+appears+that+the+number+of+industrial+devices+accessible+from+the+internet+has+risen+by+30+thousand+over+the+past+three+years/30860.

štandardizovaných bezpečnostných protokolov medzi jednotlivými dodávateľmi navyše sťažuje udržanie jednotnej úrovne ochrany v celom OT ekosystéme. Z tohto dôvodu je nevyhnutné posilniť procesy preverovania dodávateľov, zmluvného nastavenia bezpečnostných požiadaviek a priebežného monitorovania prístupov tretích strán.

Osobitnú pozornosť si vyžaduje rozvoj kyberneticko-fyzických útočných schopností. Na rozdiel od tradičných kybernetických útokov, ktoré sa zameriavajú predovšetkým na dáta, informačné systémy a digitálne služby, kyberneticko-fyzické útoky smerujú priamo proti fyzickej prevádzke technologických systémov. Ich následkom môže byť poškodenie zariadení, prerušenie výroby, ohrozenie zdravia a života osôb, environmentálne škody alebo narušenie dodávok strategických komodít. Tento trend je úzko spätý s fenoménom hybridných foriem konfliktu, pri ktorých sa kybernetické a fyzické prostriedky kombinujú s cieľom maximalizovať narušenie alebo oslabiť protivníka.

Štátni aj neštátni aktéri preto čoraz intenzívnejšie investujú do vývoja špecializovaných nástrojov určených na kompromitáciu OT a ICS systémov. Ide najmä o sofistikovaný malvér navrhnutý tak, aby dokázal manipulovať priemyselné procesy alebo meniť správanie riadiacich komponentov. FrostyGoop je deviaty malvér špecifický pre priemyselné riadiace systémy objavený v roku 2024.[1216] Takéto útoky už nemožno vnímať ako izolované incidenty. Naopak, často ide o výsledok dlhodobej prípravy, mapovania zraniteľností a vytvárania prístupových bodov do systémov, ktoré môžu byť aktivované v čase geopoliticky priaznivom pre útočníka. Tento vývoj naznačuje posun smerom k deštruktívnejším a koordinovanejším formám kybernetických operácií s potenciálne ďalekosiahlymi dôsledkami pre priemysel aj štát.

Prostredie hrozieb OT je zároveň významne formované geopolitickým kontextom a regulačným rámcom. Rastúci význam kritickej infraštruktúry a priemyselných systémov vedie štáty a regulačné orgány k prijímaniu nových pravidiel, štandardov a požiadaviek na súlad.[1217]

[1216] DRAGOS. Impact of FrostyGoop ICS Malware on Connected OT Systems [online]. Intelligence Brief. Dragos, July 2024 Dostupné na: https://hub.dragos.com/report/frostygoop-ics-malware-impacting-operational-technology.

[1217] Možno spomenúť najmä činnosť americkej agentúry CISA, ktorá vydala napr. Základy kybernetickej bezpečnosti OT: Inventarizácia aktív Pokyny pre vlastníkov a prevádzkovateľov zo dňa 13. augusta 2025 (dostupné na: https://www.cisa.gov/resources-tools/resources/foundations-ot-cybersecurity-asset-inventory-guidance-owners-and-operators) alebo príručku, ktorá má pomôcť vlastníkom a prevádzkovateľom prevádzkových technológií (OT) implementovať bezpečnú komunikáciu a poradiť výrobcom OT pri znižovaní bariér a zlepšovaní použiteľnosti, s názvom Bariéry zabezpečenej komunikácie OT: Prečo sa Johnny nemôže

Ochrana OT vyžaduje odlišný prístup než ochrana IT systémov. V OT prostredí je prioritou dostupnosť a bezpečnosť prevádzky, pričom zásahy do systémov musia byť starostlivo plánované, aby neohrozili fyzické procesy. Bezpečnostné opatrenia preto musia byť prispôsobené prevádzkovej realite priemyselných systémov. Kľúčové sú najmä segmentácia sietí, obmedzenie a kontrola vzdialeného prístupu, dôsledná správa identít a prístupových práv, monitorovanie anomálií, riadenie zraniteľností, bezpečnostné požiadavky na dodávateľov a pravidelné testovanie pripravenosti organizácie reagovať na incidenty.

13.1 Komponenty OT systémov, IIoT a architektúry

Typický systém OT pozostáva z viacerých vzájomne prepojených prvkov, ktorých spoločným cieľom je monitorovanie, riadenie a udržiavanie fyzických procesov v požadovanom stave. Takýto systém spravidla zahŕňa viacero riadiacich slučiek (control loop), rozhrania človek – stroj (Human-Machine Interface, HMI), ako aj nástroje vzdialenej diagnostiky a údržby. Technologicky je budovaný na súbore sieťových protokolov využívaných vo vrstvových architektúrach a pri kritických procesoch býva doplnený aj o bezpečnostné systémy, ktorých úlohou je zabrániť havarijným alebo nebezpečným stavom. Konkrétna podoba OT systému závisí od viacerých faktorov, najmä od toho, či ide o architektúru založenú na SCADA, DCS alebo PLC topológii.

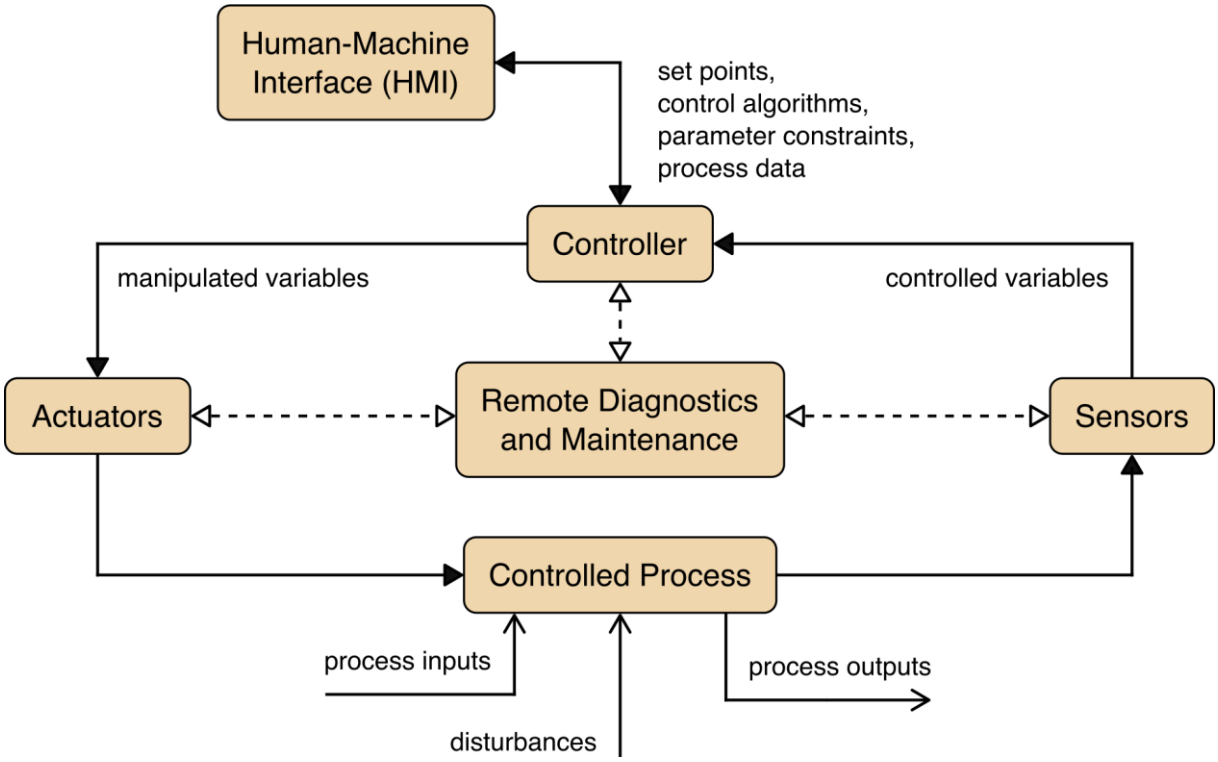
Základným funkčným prvkom OT prostredia je riadiaca slučka. Tá využíva senzory, akčné členy a riadiace jednotky na ovládanie sledovaného procesu. Senzor predstavuje zariadenie, ktoré meria určitú fyzikálnu veličinu a získané údaje odovzdáva riadiacej jednotke ako riadené premenné. Riadiaca jednotka tieto údaje interpretuje, vyhodnocuje ich podľa nastaveného algoritmu riadenia a cieľových hodnôt a následne vytvára manipulačné premenné, ktoré odosiela akčným členom. Akčné členy, medzi ktoré patria napríklad regulačné ventily, ističe, prepínače alebo motory, potom priamo zasahujú do riadeného procesu. Práve táto priama väzba medzi digitálnym riadením a fyzickým účinkom odlišuje OT od bežných informačných systémov.

Nie všetky OT systémy však fungujú v plne automatizovanom režime. V monitorovacích systémoch sa spravidla nevyskytuje priame spojenie medzi senzormi a

autentifikovať zo dňa 10. februára 2026 (dostupné na: https://www.cisa.gov/resources-tools/resources/barriers-secure-ot-communication-why-johnny-cant-authenticate)

akčnými členmi. Namerané hodnoty sú prenášané do monitorovacieho centra, kde ich vyhodnocuje človek. Aj tieto systémy však možno považovať za súčasť OT, pretože ich účelom je identifikovať a následne zmierniť určitý stav alebo udalosť vo fyzickom prostredí. Príkladom môže byť signalizácia násilného otvorenia dverí, ktorá vedie k vyslaniu bezpečnostnej služby, alebo environmentálny senzor detegujúci zvýšenú teplotu v serverovni, na základe čoho operátor aktivuje záložnú klimatizačnú jednotku. V takýchto prípadoch síce zostáva „človek v slučke", no systém naďalej plní funkciu operačnej technológie, keďže je navrhnutý na reakciu voči fyzickým udalostiam.

Významnú úlohu v OT prostredí zohrávajú rozhrania človek – stroj (HMI). Operátori a inžinieri ich využívajú na monitorovanie procesu, nastavovanie cieľových hodnôt, konfiguráciu algoritmov riadenia a úpravu parametrov riadiacich jednotiek. HMI zároveň poskytujú informácie o aktuálnom stave procesu aj historické údaje potrebné na analýzu prevádzky a rozhodovanie. Popri tom sú neoddeliteľnou súčasťou OT prostredia aj nástroje diagnostiky a údržby, ktorých cieľom je predchádzať abnormálnym stavom, identifikovať poruchy a podporovať obnovu systému po zlyhaní alebo incidente. Práve tieto nástroje, najmä ak umožňujú vzdialený prístup, však predstavujú aj významný bezpečnostný rizikový faktor.



Obrázok č. 15: Základné fungovanie OT systému.[1218]

S rozvojom digitalizácie priemyslu nadobudol osobitný význam priemyselný internet vecí (Industrial Internet of Things, IIoT). IIoT zahŕňa senzory, prístroje, stroje a ďalšie zariadenia, ktoré sú navzájom prepojené a využívajú internetovú konektivitu na podporu priemyselných a výrobných procesov. Zavedenie IIoT do OT prostredia zásadne zvyšuje mieru konektivity a objem výmeny informácií s podnikovými systémami a cloudovými platformami. To síce prináša významné výhody v podobe lepšej analytiky, prediktívnej údržby, vzdialenej správy či optimalizácie procesov, no zároveň si vyžaduje nové úvahy o bezpečnostnej architektúre. Zavedenie IIoT môže totiž znamenať zmenu sieťových hraníc, otvorenie nových rozhraní a vystavenie väčšieho počtu služieb vonkajšiemu prostrediu.

Z pohľadu bezpečnosti priemyselných sietí je pritom dôležité uvedomiť si, že pri IIoT nemožno sústrediť pozornosť výlučne na samotný internet ako komunikačné médium. Podstatou bezpečnostného problému je predovšetkým sieťová prepojenosť zariadení, tok dát a možnosť vzdialeného ovládania alebo zásahu do prevádzky.[1219] IIoT architektúra má spravidla plne distribuovaný charakter a umožňuje široké spektrum komunikačných modelov. Môže ísť o peer-to-peer komunikáciu medzi zariadeniami, spoluprácu edge zariadení v odľahlých lokalitách, distribuované dotazy nad údajmi uloženými v zariadeniach alebo v cloude, ako aj distribuovanú správu dát, ktorá určuje, kde sa majú údaje uchovávať, v akom rozsahu a ako dlho. Neoddeliteľnou súčasťou IIoT je aj správa dát z pohľadu ich kvality, dostupnosti, použiteľnosti, súkromia a bezpečnosti.[1220]

Architektúra IIoT spravidla počíta s viacerými sieťovými vrstvami. Edge sieť prepája okrajové uzly, ako sú senzory, akčné členy, zariadenia a ďalšie OT aktíva, s príslušnou platformou. Zvyčajne ide o prepojenie jedného alebo viacerých klastrov zariadení s bránou,

[1218] Prevzaté z STOUFFER, Keith; PEASE, Michael; TANG, CheeYee; ZIMMERMAN, Timothy; PILLITTERI, Victoria; LIGHTMAN, Suzanne; HAHN, Adam; SARAVIA, Stephanie; SHERULE, Aslam and THOMPSON, Michael. Guide to Operational Technology (OT) Security. NIST Special Publication 800-82 Rev. 3 [online]. Gaithersburg, MD: National Institute of Standards and Technology, 2023 Dostupné na: DOI: 10.6028/NIST.SP.800-82r3.

[1219] KNAPP, Eric D. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. 3rd ed. Cambridge, MA: Syngress, 2024. ISBN 9780443137372. Dostupné na: DOI: 10.1016/B978-0-443-13737-2.00016-6.

[1220] STOUFFER, Keith; PEASE, Michael; TANG, CheeYee; ZIMMERMAN, Timothy; PILLITTERI, Victoria; LIGHTMAN, Suzanne; HAHN, Adam; SARAVIA, Stephanie; SHERULE, Aslam and THOMPSON, Michael. Guide to Operational Technology (OT) Security. NIST Special Publication 800-82 Rev. 3 [online]. Gaithersburg, MD: National Institute of Standards and Technology, 2023 Dostupné na: DOI: 10.6028/NIST.SP.800-82r3.

ktorá zabezpečuje komunikáciu s ostatnými sieťami. Prístupová sieť následne umožňuje tok dát a riadiacich signálov medzi okrajovou a platformovou vrstvou. Takéto spojenie môže byť realizované prostredníctvom podnikovej siete, súkromnej siete nad verejným internetom alebo prostredníctvom mobilných sietí 4G a 5G. Práve využívanie moderných komunikačných technológií a nových edge zariadení však môže viesť k situácii, v ktorej sa jednotlivým systémom alebo poskytovateľom služieb udeľuje prístup priamo do OT prostredia bez dostatočnej autentifikácie, autorizácie alebo prevádzkových povolení, a to najmä s cieľom zjednodušiť procesy a znížiť administratívnu záťaž. Hoci to môže zvyšovať efektivitu, súčasne to vytvára priestor pre nežiaduce zásahy a zneužitie zo strany škodlivých aktérov.[1221]

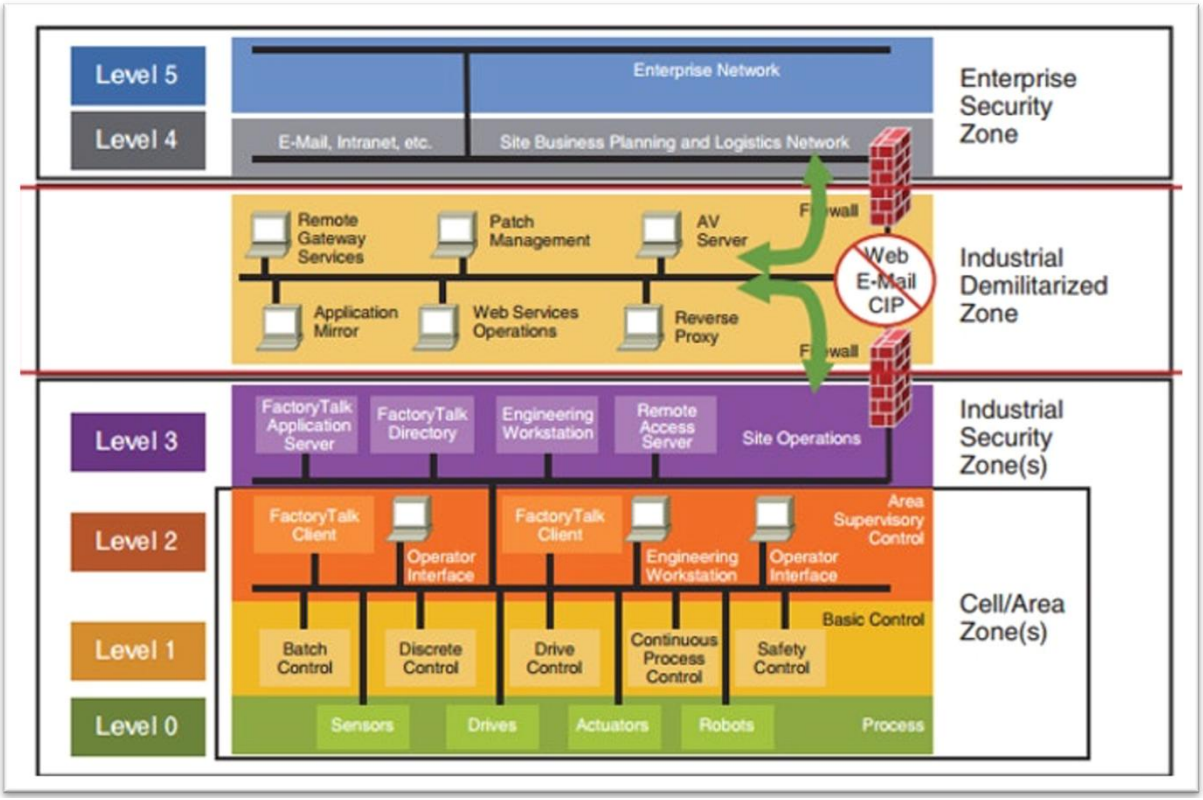
Základným predpokladom bezpečnej OT architektúry je preto identifikácia, segmentácia a izolácia IT a OT zariadení. Zoskupovanie komponentov do úrovní, vrstiev alebo zón predstavuje nevyhnutný predstupeň k nasadeniu technických prostriedkov, ktoré umožňujú chrániť a monitorovať komunikáciu medzi jednotlivými časťami siete. V praxi sa na tento účel často využívajú priemyselne uznávané referenčné modely, predovšetkým model Purdue, resp. ISA-95.[1222] Tento model predstavuje hierarchickú schému výrobných systémov a slúži na zachytenie vzťahov medzi rôznymi systémami a procesmi vo výrobnom prostredí. Jeho cieľom je podporovať koordinovanú a efektívnu spoluprácu medzi jednotlivými vrstvami automatizácie a riadenia a zabezpečiť riadený tok informácií medzi nimi.

Tradičný Purdue model vychádza z jasne oddelených úrovní – od fyzických procesov na najnižšej úrovni až po podnikové informačné systémy na najvyššej úrovni. S rastúcou integráciou IIoT technológií sa však ukazuje, že zaradenie nových zariadení a platforiem do tejto klasickej hierarchie nie je vždy jednoznačné. IIoT technológie často komunikujú naprieč úrovňami, obchádzajú tradičné hranice a vytvárajú nové logické väzby medzi zariadeniami, platformami a cloudovými službami. Aj z tohto dôvodu sa objavujú snahy modifikovať tradičný Purdue model tak, aby lepšie zohľadňoval realitu modernej priemyselnej konektivity. V tomto smere možno spomenúť prístup agentúry ENISA, ktorá navrhla upravenú verziu modelu uznávajúcu existenciu IIoT platformy na úrovni 3, komunikujúcej

[1221]ONSHUS, Tor et al. ICT Security and Independence. Report 2021:01387 – Open, Version 2 [online]. SINTEF, 17 December 2021 Dostupné na: https://www.havtil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/sintef---report---ict-security-and-independence.pdf.

[1222] ISA-95 je medzinárodný štandard pre integráciu podnikových (IT) a riadiacich (OT) systémov v priemysle, vyvíjaný organizáciou ISA. Definuje rozhrania medzi podnikovými informačnými systémami a riadením výroby.

priamo so zariadeniami IIoT na úrovni 1.[1223] Takáto koncepcia reflektuje skutočnosť, že moderné OT architektúry už nemožno vnímať ako striktne lineárne a vertikálne usporiadané.



Obrázok č. 16: Purdue model. Prevzaté z NIST.

Dochádza aj k čoraz intenzívnejšej integrácii cloudových architektúr do prostredia OT. Cloudovo hostované aplikácie sa v OT využívajú najmä prostredníctvom IoT a IIoT riešení, ktoré sa spoliehajú na cloudové backend systémy. Tento vývoj umožňuje nasadzovanie OT aplikácií formou služby (Software-as-a-Service, SaaS), čo prináša vyššiu škálovateľnosť, flexibilitu a často aj nákladovú efektívnosť. V posledných rokoch navyše integrácia OT s cloudom smeruje k využívaniu tzv. hyperscale architektúr veľkých poskytovateľov, ako sú Microsoft, Amazon alebo Google. Hlavným dôvodom je elasticita zdrojov, možnosť rýchleho škálovania a schopnosť promptne nasadzovať a sprístupňovať nové služby. Výsledkom je stav, v ktorom zmenu OT prostredia už neudávajú výlučne tradiční dodávatelia

[1223] EUROPEAN UNION AGENCY FOR CYBERSECURITY. Good Practices for Security of Internet of Things in the Context of Smart Manufacturing [online]. ENISA, 19 November 2018 [Dostupné na: https://www.enisa.europa.eu/sites/default/files/publications/WP2018%20O-1-1-1%201%20Good%20practices%20for%20security%20of%20IoT.pdf.

automatizačných riešení alebo telekomunikační operátori, ale čoraz viac práve veľkí cloudoví poskytovatelia v spolupráci s podnikovým IT.[1224]

Takýto vývoj však prináša aj závažné otázky kybernetickej bezpečnosti. Jedným z kľúčových problémov je obmedzená viditeľnosť organizácie do riadenia identít a prístupových oprávnení u poskytovateľov služieb. To vyvoláva obavy z delegovania oprávnení, z nekontrolovaného šírenia privilégií a z nedostatočného prehľadu o tom, kto má faktický prístup k dátam, systémom a riadiacim funkciám v cloudovom prostredí. Situáciu ďalej komplikuje fenomén „internetu cloudov", teda prostredia, v ktorom medzi sebou interaguje viacero cloudových služieb a poskytovateľov. Organizácie majú v takom prípade len obmedzený prehľad o tom, ako sú naprieč týmito službami nastavené prístupové opatrenia a kontrolné opatrenia. Táto netransparentnosť môže vytvárať podmienky pre neoprávnený prístup, eskaláciu privilégií alebo pretrvávanie zraniteľností, ktoré zostanú nepovšimnuté.

Ďalším problémom je, že pre cloudové OT architektúry zatiaľ nie sú ustálené všeobecne prijaté osvedčené postupy, pokiaľ ide o ich implementáciu, bezpečnostné požiadavky, bezpečnostné preskúmania či audity. Organizácie sa tak často pohybujú v prostredí, kde technologické možnosti napredujú rýchlejšie než regulačné, štandardizačné a metodické rámce.

13.2 Nová regulácia kybernetickej bezpečnosti OT

Nová právna úprava kybernetickej bezpečnosti predstavuje vo vzťahu k operačným technológiám významný kvalitatívny posun. Jedným z hlavných cieľov smernice NIS2 je totiž posilnenie ochrany kritickej infraštruktúry a tých sektorov, ktorých fungovanie je existenčne závislé od bezpečnej a nepretržitej prevádzky OT systémov. To sa odráža aj v rozšírení okruhu regulovaných subjektov, keďže medzi nové alebo osobitne akcentované sektory patria práve oblasti typicky založené na operačných technológiách, najmä energetika, doprava, výrobný priemysel, chemický priemysel, vodné hospodárstvo, odpadové hospodárstvo a výroba potravín. Vo všetkých týchto sektoroch OT systémy zabezpečujú riadenie fyzických

[1224] PERDUCAT, Cyril; MAZUR, David C.; MUKAI, William; SANDLER, Samuel N.; ANTHONY, Michael J. and MILLS, Joseph A. Evolution and Trends of Cloud on Industrial OT Networks. IEEE Open Journal of Industry Applications. 2023, vol. 4, pp. 291–303. Dostupné na: DOI: 10.1109/OJIA.2023.3309669.

procesov, automatizáciu, monitorovanie prevádzky a ochranu kontinuity služieb, a preto sú prirodzeným predmetom zvýšeného regulačného záujmu.

ZoKB na túto zmenu nadväzuje tým, že v § 20 výslovne uvádza, že bezpečnostné opatrenia sa vzťahujú nielen na siete a informačné systémy, ale aj na operačné technológie. Podľa zákona ide o úlohy, procesy, roly a technológie v organizačnej, personálnej, fyzickej a technologickej oblasti, ktorých cieľom je dosiahnutie, zaručenie a udržanie kybernetickej bezpečnosti počas celého životného cyklu sietí, informačných systémov a operačných technológií. Z hľadiska normatívnej techniky možno poznamenať, že samotný zákon ani vykonávacia vyhláška pojem „operačné technológie" výslovne nedefinujú. Tento pojem sa objavuje v systematike právnej úpravy, absentuje však jeho legálne vymedzenie. Istú interpretačnú oporu preto poskytuje až dôvodová správa, ktorá pod pojmom výrobné a produkčné technológie rozumie technické, softvérové a organizačné prostriedky slúžiace na riadenie, automatizáciu, monitorovanie a vykonávanie procesov výroby, spracovania alebo distribúcie fyzických produktov, energií, surovín alebo služieb, pričom výslovne uvádza systémy OT, ako sú PLC, SCADA, HMI, senzorika, akčné členy a súvisiaca infraštruktúra. Z pohľadu právnej istoty ide o určitý deficit, ktorý je však čiastočne kompenzovaný materiálnym obsahom prílohy č. 1 vyhlášky NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach (ďalej len „vyhláška").

Práve príloha č. 1 vyhlášky predstavuje z pohľadu regulácie OT osobitne inovatívny prvok. Na rozdiel od staršieho, prevažne všeobecného prístupu vytvára štandardizovaný, praktický a kontrolovateľný katalóg bezpečnostných opatrení, pri ktorých sa výslovne rozlišuje relevancia pre IKT a pre OT, a zároveň osobitne pre prevádzkovateľa základnej služby a prevádzkovateľa kritickej základnej služby. Zároveň ustanovenie § 4 vyhlášky, výslovne uvádza, že bezpečnostná dokumentácia obsahuje určenie sietí a informačných systémov a operačných technológií do príslušnej kategórie informačných a komunikačných technológií alebo operačných technológií, kde v prípade nejednoznačnosti rozhodne o určení kategórie prevádzkovateľ základnej služby. Vo vyhláške sa výslovne vyžaduje zahrnúť do dokumentácie aj topológiu a infraštruktúru operačných technológií. Normatívny význam tohto riešenia je značný. Hoci prevádzkovateľ po analýze rizík určuje rozsah a spôsob implementácie bezpečnostných opatrení, kombinácia prílohy, dokumentačných povinností podľa § 4 vyhlášky a požiadavky viesť zoznam prijatých a neprijatých opatrení v praxi

znamená, že prevádzkovateľ bude musieť neimplementovanie opatrenia presvedčivo odôvodniť.

Z analýzy tabuľky v prílohe č. 1 vyplýva, že zákonodarca pri OT neostal pri mechanickom rozšírení všeobecných IKT požiadaviek, ale zaviedol viacero skutočne OT-špecifických opatrení. Prvú skupinu tvoria opatrenia zamerané na kontinuitu prevádzky, odolnosť a obnovu systémov. Položka 30 vyžaduje, aby komponenty operačných technológií boli schopné prepínať sa na núdzové napájanie a z núdzového napájania bez vplyvu na aktuálny stav zabezpečenia alebo na vopred definovaný obmedzený režim. Ide o typicky OT požiadavku, ktorá reflektuje, že priemyselné a prevádzkové systémy nemôžu byť posudzované iba z pohľadu dôvernosti dát, ale predovšetkým z pohľadu bezpečnej a riadenej kontinuity fyzického procesu. Na tento prístup nadväzujú položky 33 a 34, ktoré pri kritických OT výslovne vyžadujú oddelený zálohovací systém pre OT a každoročné testovanie funkčnosti záloh aspoň dvoch rôznych systémov. Tým sa do regulácie premieta zásada, že obnova OT nemôže byť iba teoretická, ale musí byť prakticky overovaná vzhľadom na potenciálne závažné dôsledky neobnoviteľnosti konfigurácií, historických dát alebo riadiacich parametrov.

Druhá významná skupina opatrení sa týka bezpečnej konfigurácie a životného cyklu OT komponentov. Položky 40 až 42 výslovne vyžadujú určenie a aplikovanie základných parametrov bezpečných konfigurácií, konfiguráciu OT komponentov podľa bezpečnostných odporúčaní dodávateľa a zabezpečenie rozhrania na prístup k aktuálne nasadeným bezpečnostným konfiguračným nastaveniam. Tieto požiadavky sú z právno-regulačného hľadiska dôležité, pretože reflektujú tradičný problém OT prostredí: prevádzku zariadení s dlhou životnosťou, proprietárnymi nastaveniami a obmedzenou možnosťou štandardného hardeningu. Vyhláška tu fakticky prenáša do roviny opatrenia požiadavku konfiguračnej transparentnosti a bezpečnostnej správy aktív, čo sa približuje princípom známych z medzinárodných priemyselných štandardov. Osobitný význam má aj položka 46, ktorá pre vrstvy 3 a vyššie vyžaduje uzamknutie relácie po konfigurovateľnom čase nečinnosti alebo manuálnym uzamknutím. Táto formulácia ukazuje, že regulátor si uvedomuje rozdielnu technickú realitu jednotlivých vrstiev OT a neukladá identické požiadavky plošne aj na zariadenia nižších vrstiev, pri ktorých by to bolo technicky neprimerané alebo prevádzkovo problematické.

Treťou kľúčovou oblasťou sú identity, prístupy a kontrola externých zásahov. Osobitne významné sú položky 74, 75 a 77. Položka 74 zavádza požiadavku identifikácie oprávnenosti pristupujúceho technického prostriedku a následne aj používateľa pri komponentoch zaradených do vrstiev 3 a vyššie. Ide o dôležitý odklon od historickej OT praxe, v ktorej sa dôvera často viazala na samotnú sieť alebo pracovisko, nie na overenú identitu zariadenia a osoby. Položka 75 ide ešte ďalej a v prípade prístupu na inžinierske prostredia v OT vyžaduje pri kritických základných službách použitie technológie na záznam a archiváciu úkonov externej organizácie. Táto požiadavka reaguje na jedno z najvýznamnejších reálnych rizík OT prostredia, teda na servisný a dodávateľský vzdialený prístup. Položka 77 následne pri kritických OT vyžaduje samostatnú, oddelenú technológiu na riadenie prístupov v operačných technológiách. Z hľadiska systematiky regulácie ide o potvrdenie, že riadenie prístupov v OT nemá byť iba derivátom podnikových IT nástrojov na riadenie identít a prístupov, ale má reflektovať osobitosti prevádzkových rolí, inžinierskych pracovísk a vyššiu citlivosť zásahov do technologického procesu.

Osobitne silná je štvrtá skupina opatrení, a to opatrenia sieťovej architektúry a komunikačnej bezpečnosti. Položka 107 vyžaduje systémy detekcie narušenia zohľadňujúce proprietárne protokoly a dátové toky, čím vyhláška správne reflektuje, že bežné IT detekčné nástroje často nedokážu spoľahlivo analyzovať špecifiká priemyselnej komunikácie. Položka 108 ustanovuje automatické ukončenie vzdialenej relácie po dobe nečinnosti, čo priamo reaguje na vysoké riziko vzdialeného prístupu v OT. Položky 110 až 115 vyžadujú mechanizmy smerovania a filtrácie prevádzky cez sieťový firewall, logickú segmentáciu medzi OT, sieťami a informačnými systémami, pri kritických základných službách dokonca aj fyzickú segmentáciu, segmentáciu vybraných sietí riadiaceho systému od ostatných OT sietí, nezávislý firewall pre OT a blokovanie odosielania a prijímania správ medzi používateľmi v OT sieťach. Tieto opatrenia sú zjavne inšpirované architektonickými princípmi zón, vrstiev a hraníc dôvery typických pre priemyselné referenčné modely. Ich význam spočíva v tom, že bezpečnostné opatrenia prvýkrát pomerne explicitne transformujú architektonické zásady priemyselnej kybernetickej bezpečnosti do opatrení.

Piata oblasť OT-špecifických opatrení smeruje k detekcii, monitorovaniu a správe koncových zariadení. Položky 133 až 135 zas upravujú reguláciu alebo zákaz používania prenosných zariadení v kritických oblastiach OT, automatické presadzovanie obmedzení používania mobilných a prenosných zariadení a overovanie súladu takýchto zariadení s

požiadavkami bezpečnostnej zóny. Aj tieto ustanovenia sú mimoriadne významné, keďže prenosné médiá, servisné notebooky a mobilné zariadenia patria dlhodobo medzi najčastejšie vektory zavlečenia škodlivého kódu do priemyselných prostredí.

Za osobitnú pozornosť stojí aj to, že vyhláška pracuje s vlastným vrstvením OT prostredia od vrstvy 5 po vrstvu 0. Toto vrstvenie sa zjavne približuje logike Purdue modelu, hoci používa vlastnú legislatívnu terminológiu. Vrstva 5 predstavuje celkové prostredie organizácie, vrstva 4 prostredie centrálnej správy OT, vrstva 3 prostredie prevádzky a riadenia výrobného procesu (najmä zálohovací server (historian), riadiace servery), vrstva 2 prostredie riadenia a automatizácie procesov (najmä rozhranie HMI, SCADA), vrstva 1 prostredie priameho riadenia (najmä PLC) a vrstva 0 fyzické prostredie senzorov a akčných členov. Z hľadiska regulácie je dôležité, že viacero opatrení sa viaže iba na vrstvy 3 a vyššie. To možno hodnotiť pozitívne, pretože ide o realistický a technicky citlivý prístup. Regulátor tým implicitne uznáva, že nie všetky bezpečnostné mechanizmy sú vhodné alebo uskutočniteľné na úrovni PLC, senzorov a akčných členov, a že vyššie vrstvy predstavujú prirodzené miesto pre zavedenie prístupovej kontroly, šifrovania, riadenia relácií či záznamu činností externých subjektov.

Nová slovenská úprava kybernetickej bezpečnosti OT už nestavia iba na všeobecnej požiadavke primeraných bezpečnostných opatrení, ale vytvára osobitný regulačný režim pre OT prostredia. Tento režim je charakteristický štyrmi znakmi. Po prvé, diferencuje medzi IKT a OT. Po druhé, rozlišuje medzi prevádzkovateľom základnej služby a prevádzkovateľom kritickej základnej služby. Po tretie, zohľadňuje vrstvovú architektúru OT. Po štvrté, zavádza viaceré explicitne OT-špecifické opatrenia, ktoré nemožno redukovať na obyčajnú aplikáciu IT bezpečnosti v priemyselnom prostredí. Práve v tomto spočíva najväčší význam novej právnej úpravy.

Vyhláška a jej príloha č. 1 predstavuje jeden z normatívne najzaujímavejších prvkov novej právnej úpravy. Napriek absencii presnej zákonnej definície OT vytvára materiálne pomerne jasný obraz o tom, čo regulátor považuje za jadro bezpečnej prevádzky operačných technológií. Osobitné požiadavky na núdzové napájanie, oddelené zálohovanie, bezpečné konfigurácie, riadenie externých zásahov, samostatnú správu prístupov, segmentáciu, detekciu, reguláciu prenosných zariadení a klasifikáciu dátových tokov medzi bezpečnostnými zónami ukazujú, že slovenská právna úprava sa posúva smerom k zrelšiemu a technicky informovanejšiemu modelu regulácie priemyselnej kybernetickej bezpečnosti.

POUŽITÁ LITERATÚRA A ZDROJE

Monografie, periodiká a zborníky

ADAMKOVIČ, M. Šírenie poplašnej správy a aplikačné problémy v kontexte súčasného smerovania spoločnosti In: MARKOVÁ, V.; PAULÍČKOVÁ, N. (zost.) Aktuálne otázky trestného práva v teórii a praxi. Zborník príspevkov z 12. roč. interdisciplinárnej celoštátnej vedeckej konferencie s medzinárodnou účasťou. Bratislava: Akadémia Policajného zboru v Bratislave. 2024, s. 26. ISBN 978-80-8293-020-0. Dostupné na: LINK;

AGO, Roberto: L'occupazione bellica di Roma e il Trattato lateranense. In: Comunicazioni e Studi. Milan: Giuffrè, 1945, vol. II.

AI HLEG - Assessment List for Trustworthy Artificial Intelligence (ALTAI) . Dostupné na: https://futurium.ec.europa.eu/en/european-ai-alliance/document/ai-hleg-assessment-list-trustworthy-artificial-intelligence-altai?language=sk.

ALAFUA, Princess. Data Privacy and Data Protection: The Right of User's and the Responsibility of Companies in the Digital World. 7 January 2022. Dostupné na: https://ssrn.com/abstract=4005750 alebo http://dx.doi.org/10.2139/ssrn.4005750.

ANDRAŠKO, J a kol.:. Zákon o kybernetickej bezpečnosti. Bratislava : Wolters Kluwer, 2018.

ANDRAŠKO, J.; MESARČÍK, M.; SOKOL, P. Právo kybernetickej bezpečnosti. 1. vyd. – Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2022.

ARADAU, Claudia. Governing Terrorism Through Risk: Taking Precautions, (Un)Knowing the Future. European Journal of International Relations, 2007, roč. 28, č. 1, s. 89.

ARONSSON-STORRIER, Marie: Article 8 bis (2). Lexsitus – CILRAP, aktualizované 20. 5. 2019. Dostupné na: https://cilrap-lexsitus.org/en/clicc/8-bis/8-bis-2.

BAKER, W., FISHER W., SCARFONE K., SOUPPAYA, M.: NISTIR 8374 - Ransomware Risk Management: A Cybersecurity Framework Profile, [online] [21.3.2022]. Dostupné na: https://csrc.nist.gov/publications/detail/nistir/8374/final.

BARBOU DES PLACES, Ségolène. Introduction: Public order and public security in EU law. Time for Reappraisal. European Papers, 2024, roč. 9, č. 3, s. 1316 – 1328.
BEDI, Suneal. The Myth of the Chilling Effect. Harvard Journal of Law & Technology, 2021, roč. 35, č. 1.

BARLOW, John Perry: A Declaration of the Independence of Cyberspace. Electronic Frontier Foundation, 8. 2. 1996. Dostupné na: https://www.eff.org/cyberspace-independence.

BASSIOUNI, M.; CHERIF, M. Introduction to International Criminal Law, Transnational publishers, New York, ISBN: 1-57105-286-0, 2003.

BEDNÁR, Daniel: K niektorým aspektom ozbrojených konfliktov 21. storočia v kontexte medzinárodného práva. In: VALUCH, Jozef – OZORÁKOVÁ, Lilla (eds.): Aktuálne bezpečnostné výzvy a medzinárodné právo. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2021.

BENYUSZ, Márta – RAISZ, Anikó (eds.): International Children's Rights. Miskolc – Budapest: Central European Academic Publishing, 2024. ISBN 978-615-6474-70-4 (pdf).

BÍLKOVÁ V. Úprava vnitrostátních ozbrojených konfliktů v mezinárodním humanitárním právu. Univerzita Karlova v Praze, Právnická fakulta, Praha, 2007, ISBN: 80-85889-82-6;

BLAŽEK, R.: Kriminalistika. Šamorín : Heuréka, 2016;

BRAYNE, Sarah. Big Data Surveillance: The Case of Policing. American Sociological Review, 2017, roč. 82, č. 5, s. 977 – 1008. https://doi.org/10.1177/0003122417725865.

BURDA, E., ČENTÉŠ, J., KOLESÁR, J., ZÁHORA, J. a kol.: Trestný zákon. Všeobecná časť. Komentár. I. diel. 1. vydanie. Praha : C. H. Beck, 2010;

BUTTIGIEG, Christopher P. a ZIMMERMANN, Beatriz Brunelli, 2024. The digital operational resilience act: challenges and some reflections on the adequacy of Europe's architecture for financial supervision. In: *ERA Forum*. Online. Roč. 25, č. 1, s. 11–28. ISSN 1863-9038. Dostupné na: https://doi.org/10.1007/s12027-024-00793-w [cit. 2026-04-07].

CASEY, E.: Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet. Third Edition. London : Academic Press, 2011;

COLOMBO, Carlo and ELIANTONIO, Mariolina. Harmonized Technical Standards as Part of EU Law: Juridification with a Number of Unresolved Legitimacy Concerns? Case C-613/14 James Elliot Construction Limited v. Irish Asphalt Limited, EU:C:2016:821. Maastricht Journal of European and Comparative Law. 2017, vol. 24, no. 2, pp. 323–340. Dostupné na: DOI: 10.1177/1023263X17709753.

CONNOLLY, L. Y.; WALL, D. S.; LANG, M. and ODDSON, B. An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability. Journal of Cybersecurity [online]. 2020, vol. 6, no. 1, tyaa023 Dostupné na: DOI: 10.1093/cybsec/tyaa023.

CRAWFORD, James R.: Brownlie's Principles of Public International Law. 8. vyd. Oxford: Oxford University Press, 2012.

ČENTÉŠ, J. a kol. Trestné právo procesné - Osobitná časť, 3. vydanie, Šamorín, Heuréka, 2025;

ČENTÉŠ, J. a kol.: Trestné právo procesné. Všeobecná časť. Šamorín : Heuréka, 2016;

ČENTÉŠ, J., BELEŠ, A. Vzťah kódexu správneho trestania a trestného práva. In. *Havelková, M., Grešová, L. a Bleho, Š. (zost.).* Nová právna úprava správneho trestania, Zborník

z vedeckej konferencie konanej v dňoch 14. a 15. októbra 2021 v Bratislave. Bratislava : Univerzita Komenského v Bratislave, Právnická fakulta, 2021, s. 53 - 62. ISBN 978-80-7160-616-1.

ČENTÉŠ, J.: Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. 1. vydanie. Bratislava : C. H. Beck, 2013;

ČENTÉŠ, J.; RAMPÁŠEK, M. Ransomvér a úhrada výkupného v kontexte trestného práva. Časopis pro právní vědu a praxi. roč. 33 (2025), č. 3, s. 555 – 578. ISSN: 1210-9126 LINK;

DENZA, Eileen: Diplomatic Law: Commentary on Vienna Convention on Diplomatic Relations. Oxford: Oxford University Press, 2016.

DOBROVODSKÝ, Róbert: K novému medzinárodnému mechanizmu ochrany práv detí. In: JURČOVÁ, Monika – DOBROVODSKÝ, Róbert – NEVOLNÁ, Zuzana – ŠTEFANKO, Jozef (eds.): Liber amicorum Lazar. Trnava: Universitatis Tyrnaviensis, 2014. ISBN 978-80-8082-791-5.

DRAŽOVÁ, P., KORDÍK, M.: Efektivita postihu počítačovej kriminality. In Efektívnosť prípravného konania – jej skúmanie, výzvy a perspektívy. Bratislava : Univerzita Komenského v Bratislave, Právnická fakulta, 2020, Dostupné dňa 06.02.2026 na: LINK;

DRAŽOVÁ, P.; KORDÍK, M. Trestnoprávny presah vybraných zakázaných praktík podľa Aktu o umelej inteligencii, Bratislavské právnické fórum 2025 / MIHÁLIKOVÁ, M.; ŤAŽKÁ, V. (zost.). Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2025. ISBN 978-80-7160-772-4, s. 641-642. Dostupné dňa 06.02.2026 na: LINK;

DROEGE, Cordula: Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. In: International Review of the Red Cross, No. 886, June 2012. Dostupné na: https://international-review.icrc.org/articles/get-my-cloud-cyber-warfare-international-humanitarian-law-and-protection-civilians.

DUŠKOVÁ, Šárka – HOFSCHNEIDEROVÁ, Anna – KOUŘILOVÁ, Kamila: Úmluva o právech dítěte. Komentář. Praha: Wolters Kluwer ČR, 2021. ISBN 978-80-7598-683-2.

DUNCAN, Jamie. Data protection beyond data rights: governing data production through collective intermediaries. Internet Policy Review, 2023, roč. 12, č. 3. Dostupné na: https://policyreview.info/articles/analysis/data-protection-beyond-data-rights.

ELISAN, CH. C.: Advanced Malware Analysis. McGraw-Hill Education, 2015.

EYUSUN, H. Lethal Autonomous Weapons: The Next Frontier in International Security and Arms Control, Stanford International Policy Review, Ford Dorsey Masters in International Policy, 30th January 2025, dostupné dňa 13.12.2025 na LINK;

FRIDRICH, B. a kol.: Ústavné garancie ľudských práv. Bratislava: Právnická fakulta UK, 2013.

FUNTA, Rastislav: Dohovor Rady Európy o počítačovej kriminalite (Budapeštiansky dohovor): komentár. Bratislava: Wolters Kluwer, 2021. 136 s.

FUSTER, G. – HIJMANS, H.: The EU rights to privacy and personal data protection: 20 years in 10 questions. Discussion paper. Dostupné na: https://brusselsprivacyhub.eu/events/20190513.Working_Paper_Gonza%CC%81lez_Fuster_Hijmans.pdf.

FUSTER, G. – JASMONTAITE, L.: Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights. In CHRISTENSEN, M. et al. (eds).: Ethics of Cybersecurity. Springer, 2020, s. 97 - 116.

FUSTER, G., HIJMANS, H.: The EU rights to privacy and personal data protection: 20 years in 10 questions. Discussion paper. Dostupné na: https://brusselsprivacyhub.eu/events/20190513.Working_Paper_Gonza%CC%81lez_Fuster_Hijmans.pdf.

GISEL, Laurent – RODENHÄUSER, Tilman – DÖRMANN, Knut: Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. In: International Review of the Red Cross, 102(913), 2020, s. 287–334. Dostupné na: https://international-review.icrc.org/articles/twenty-years-international-humanitarian-law-and-protection-civilians-against-effects-cyber-913.

HALÁSZ, Csenge (ed.): Children in Digital Age. Miskolc – Budapest: Central European Academic Publishing, 2025. Dostupné online: Children in Digital Age | Human Rights – Children's Rights.

HAMUĽÁKOVÁ, Z. Zákaz reformatio in peius v správnom konaní. 1. vydanie. Bratislava : Wolters Kluwer SR s. r. o., 2020, 216 s. ISBN 978-80-571-0293-9.

HAMUĽÁKOVÁ, Z., HORVAT, M. Základy správneho práva trestného. Bratislava : Wolters Kluwer, 2019, 308 s. ISBN 978-80-571-0142-0.

HAVELKOVÁ, M. Plná jurisdikcia správnych súdov a jej vplyv na administratívne konanie vo veciach správneho trestania. In Acta Facultatis Iuridicae Universitatis Comenianae, Tomus XXXIX, č. 1/2020. Bratislava : Právnická fakulta Univerzity Komenského v Bratislave, 2020, s. 117 - 129.

CHALUPA, B. HEURISTICKÉ ŘEŠENÍ PROBLÉMU SE ZŘETELEM KE KOMPLEXNOSTI ODPOVĚDI, Sborník prací Filozofické fakulty brněnské univerzity. I, Řada pedagogicko-psychologická. 1988, vol. 37, iss. I23, pp. [41]-5, dostupné na: LINK;

CHIRCOP, Luke: Territorial sovereignty in cyberspace after Tallinn Manual 2.0. In: Melbourne Journal of International Law, vol. 20, 2019.

CHLIPALA, M., MAKATURA, I., PILÁR, *Š.* Zákon o kybernetickej bezpečnosti Komentár. Prvé vydanie. Žilina : Eurokódex s. r. o. 2019, 408 s. ISBN 978-80-8155-086-7.

CHRISTEN, M. et al. (eds): The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology, 21. Dordrecht: Springer, 2020.

CHRISTENSEN, M. et al. (eds.): Ethics of Cybersecurity. Springer, 2020.

CHRISTODOULOU, Klitos, eds. *Information Systems: 19th European, Mediterranean, and Middle Eastern Conference, EMCIS 2022, Virtual Event, December 21–22, 2022, Proceedings*.

ELIANTONIO, Mariolina and VOLPATO, Annalisa. The European System of Harmonised Standards: Legal Opinion for ECOS [online]. 11 March 2022 Dostupné na: DOI: 10.2139/ssrn.4055292.

IVOR, I.; POLÁK, P.; ZÁHORA, J. Trestné právo hmotné II. Osobitná časť. 2. vydanie. Bratislava: Wolters Kluwer SR s.r.o., 2021;

JANČIŪTĖ, Laima, 2025. Cybersecurity in the financial sector and the quantum-safe cryptography transition: in search of a precautionary approach in the EU Digital Operational Resilience Act framework. In: *International Cybersecurity Law Review*. Online. Roč. 6, č. 2, s. 145–154. ISSN 2662-9739. Dostupné na: https://doi.org/10.1365/s43439-025-00135-7 [cit. 2026-04-20].

JENSEN, Eric Talbot: The Tallinn Manual 2.0: Highlights and Insights. In: Georgetown Journal of International Law, vol. 48, no. 3, 2017.

KAYE, D.: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression : note / by the Secretary-General. Dostupné na https://digitallibrary.un.org/record/1304394.

KLUČKA, Ján: Medzinárodné právo verejné (všeobecná a osobitná časť). Košice: Wolters Kluwer, 2017.

KOOPS, Bert-Jaap. The Concept of Function Creep. Information, Communication & Society, 2021, roč. 24, č. 4, s. 538.

KRÁLIK, Ján: Aktuálne výzvy v oblasti kybernetickej kriminality: návrh druhého dodatkového protokolu k Dohovoru Rady Európy o počítačovej kriminalite. In: Míľniky práva v stredoeurópskom priestore 2021: zborník z medzinárodnej vedeckej konferencie. Bratislava: Právnická fakulta UK v Bratislave, 2021, s. 11–22.

KNOOPS, G. Defenses in contemporary international criminal law, 2nd Edition, Koninklijke Brill NV, Leiden, The Netherlands, 2008, ISBN: 978-1-57105-158-5;

KOLOUCH, J.: Cybercrime. 1. vydání. Praha : Edice CZ.NIC, 2016;

KORDÍK, M.: Právny styk s cudzinou. Bratislava : C. H. Beck SK, 2017;

KOSSEFF, J.: Defining Cybersecurity Law. In Iowa Law Review. 2018, 103: 985.

KOŠIČIAROVÁ, S. Zákon o priestupkoch. Podrobný komentár s judikatúrou. Praha : Leges, 2020, 830 s. ISBN 978-80-7502-465-7.

KOŠŤÁLOVÁ, S.: Regulatory sandbox ako nástroj pre efektívnu reguláciu automatizovaných vozidiel. Marec 2025. Dostupné na: https://www.flaw.uniba.sk/fileadmin/praf/Pracoviska/Ustavy/UPITPDV/PST_PI/Regulatory_sandbox_ako_nastroj_pre_efektivnu_regulaciu_AV_Kostalova.pdf.

KRAJEWSKI, Markus: Mandatory Human Rights Due Diligence Laws? Blurring the Lines between State Duty to Protect and Corporate Responsibility to Respect? In: Nordic Journal of Human Rights, roč. 41, 2023, č. 3, s. 265-278.

KUN, E., 2024. Challenges in regulating cloud service providers in EU financial regulation: From operational to systemic risks, and examining challenges of the new oversight regime for critical cloud service providers under the Digital Operational Resilience Act. In: *Computer*

Law & Security Review. Online. Roč. 52, čl. 105931. ISSN 0267-3649. Dostupné na: https://doi.org/10.1016/j.clsr.2023.105931 [cit. 2026-04-29].

LESSIG, L.: The Laws of Cyberspace. Draft 3. 1998. Dostupné na: https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf.

LIEVENS, Eva: Protecting Children in the Digital Era: The Use of Alternative Regulatory Instruments. Leiden – Boston: Brill/Nijhoff, 2010. ISBN: 978-90-04-18972-0

LOI, M. – CHRISTEN, M.: Ethical Frameworks for Cybersecurity. In CHRISTEN, M. et al. (eds): The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology, 21. Dordrecht: Springer, 2020.

LYNSKEY, O.: The Foundations of EU Data Protection Law. Oxford University Press, 2015.

LYNSKEY, O.: The Foundations of EU Data Protection Law. Oxford: Oxford University Press, 2015.

LYON, David (ed.). Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination. Routledge, 2003.

LYON, David. Surveillance, Security and Social Sorting: Emerging Research Priorities. International Criminal Justice Review, 2007, roč. 17, č. 1, s. 161.

ĽALÍK, Tomáš a kol.: Ochrana základných práv. Bratislava: Wolters Kluwer SR, 2026. ISBN 978-80-571-0813-3

MACNISH, K. – VAN DER HAM, J.: Ethics in Cybersecurity research and practice. In Technology in Society 63 (2020).

MAKATURA, Ivan. Technická normalizácia v informačnej a kybernetickej bezpečnosti. Bezpečnosť v praxi [online]. Žilina: Poradca podnikateľa, 2024 ISSN 2729-885X. Dostupné na:

https://www.bezpecnostvpraxi.sk/odborny-clanok/technicka-normalizacia-v-informacnej-a-kybernetickej-bezpecnosti.htm.

MARKOŠ, J.: Medzi dobrom a zlom. 16 etických dilem, pred ktorými môžete stáť raz i vy. Bratislava: N PRESS, 2020.

MAREČEK, Lukáš: Criminal liability of legal persons under international law – retrospection and current status. In: The Lawyer Quarterly, vol. 10, no. 4, 2020, s. 413–425.

MAREČEK, Lukáš: Medzinárodné trestné právo a jeho implementácia v slovenskom právnom poriadku. Bratislava: Právnická fakulta UK v Bratislave, 2025. 266 s.
SCHMITT, Michael N. (ed.): Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge: Cambridge University Press, 2013. 278 s.

MARTVOŇ, A. Vplyv európskeho práva na slobodný prístup k informáciám a na zásadu informovanosti v konexte správneho trestania. In. *Lenhart, M., Hapčová, I., Hamuľák, J. (ed).* 2016. Vplyv európskeho práva na kreovanie princípov a zásad správneho trestania: Zborník príspevkov z medzinárodnej vedeckej konferencie Bratislavské právnické fórum 2016 organizovanej Univerzitou Komenského v Bratislave, Právnickou fakultou v dňoch 21. – 22. októbra 2016. Bratislava : Univerzita komenského v Bratislave, právnická fakulta, vydavateľské oddelenie, s. 127 – 134. ISBN 978-80-7160-430-3.

MASÁROVÁ, Ľ., MASLEN, M. Princíp legitímnych očakávaní – integrálny prvok princípu právnej istoty v oblasti verejného práva. In. *Maslen, M. – Masárová, Ľ. (ed.).* 2018. Legitímne očakávania, transparentnosť verejnej správy a zneužívanie práv v aplikačnej praxi v právnom štáte: Zborník z medzinárodnej vedeckej konferencie „Právny štát – medzi vedou a umením", ako súčasti medzinárodného vedeckého kongresu Trnavské právnické dni, 20. – 21. septembra 2018. Trnava : Právnická fakulta TU v Trnave, 2018. Bratislava : Wolters Kluwer, 2018, s. 84 - 102. ISBN 978-80-8168-984-0.

MÁČAJ, Ľ. Rozšírenie dispozičnej zásady v priestupkovom konaní? In. *Potešil, L., Hejč, D., Valdhans, J. (eds.).* Dny práva 2018 – Days of law 2018 Část III. – Řízení o přestupcích (nejen)

z pohledu správních orgánů a správnich soudů. Sborník z konference. Brno : Masarykova univerzita. 2019, s. 172 - 191. ISBN 978-80-210-9326-3.

MCGUIRE, M., DOWLING, S.: Cyber crime: A review of the evidence. UK Home Office;

MESARČÍK, M. a GYURÁSZ, Z.: Umelá inteligencia a právna úprava zdravotníctva v Slovenskej republike. 1. vydanie. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2020.

MESARČÍK, M. Nástroje verejného práva pre boj s dezinformáciami v online prostredí. 1. vydanie. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2023, ISBN: 978-80-7160-706-9;

MESARČÍK, M.: Ochrana osobných údajov. Učebnica. 1. vydanie. Bratislava: C.H. BECK, 2020.

MITNICK, K. D.; SIMON, W. L. The art of deception: Controlling the human element of security. John Wiley & Sons, 2011.

MORGAN, B. a YEUNG, K.: An introduction to law and regulation. Texts and materials. The law in context series. Cambridge: Cambridge University Press; 2007.

MURRAY, Daragh. The Chilling Effect of Surveillance under the European Convention on Human Rights. Journal of Human Rights Practice, 2024, roč. 26, č. 1, s. 1.

NEUMANNOVA, Anita; BERNROIDER, Edward a ELSHUBER, Christoph, 2023. The Digital Operational Resilience Act for Financial Services: A Comparative Gap Analysis and Literature Review. In: PAPADAKI, Maria; RUPINO DA CUNHA, Paulo; THEMISTOCLEOUS, Marinos a

MURRAY, Daragh; FUSSEY, Pete. Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data. Israel Law Review, 2019, roč. 52, č. 1, s. 31 – 60. doi:10.1017/S0021223718000304.

ORIYANO, S-P., SOLOMON, M. G.: Hacker Techniques, Tools, and Incident Handling, 3rd edition. Jones & Bartlett Learning, 2018.

OTTOVÁ, E.: Teória práva. 1. vyd. Bratislava: Heuréka, 2010.

OZKAYA, E.: Learn Social Engineering, Packt Publishing. 2018.

PARKER, Donn B. Fighting Computer Crime: A New Framework for Protecting Information. New York: Wiley Computer Publishing, John Wiley & Sons, 1998. ISBN 978-0-471-16378-7.

PEKÁR, B. : Európske správne právo a európsky správny priestor. 1. vydanie. Euroiuris, 2012

POJMAN, L. – FIESER, J.: Ethics: Discovering Right and Wrong. Cengage Learning, 2011.

PENNEY, Jonathon W. Chilling Effects: Online Surveillance and Wikipedia Use. Berkeley Technology Law Journal, 2016, roč. 31, č. 1, s. 117.

POLČÁK, R. a kol.: Právo informačných technológií. Praha : Wolters Kluwer ČR, 2018;

POLČÁK, R., HARAŠTA, J. a STUPKA, V.: Právní problémy kybernetické bezpečnosti. 1. vyd. Brno : Masarykova univerzita, Právnická fakulta, 2016.

POLČÁK, R.: Kybernetická bezpečnosť. In POLČÁK, R.: a kol. Právo informačných technológií. Praha: Wolters Kluwer ČR, 2018.

PORADA, V., RAK, R.: Digitální stopy v kriminalistice a forenzních vědách. In Soudní inženýrství. 2006, č. 17;

PRÁŠKOVÁ, H. Základy odpovědnosti za správní delikty. 1. vydání. Praha : C. H. Beck, 2013, 446 s. ISBN 978-80-7400-456-8.

POZEN, David E. Privacy–Privacy Tradeoffs. University of Chicago Law Review, 2016, roč. 83, č. 1, s. 221.

RAISZ Anikó (ed.): Children's Rights in Regional Human Rights Systems. Miskolc–Budapest, Central European Academic Publishing, 2024, ISBN 978-615-6474-67-4.

ROSS. R a kol.: NIST Special Publication 800-171 Revision 2, [online] [21.3.2022]. Dostupné na: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final.

SCHELLEKENS, M. Car hacking: Navigating the regulatory landscape. In Computer Law and Security Review. 2015, roč. 32, č. 2.

SCHEPEL, Harm. The New Approach to the New Approach: The Juridification of Harmonised Standards in EU Law. Maastricht Journal of European and Comparative Law. 2013, vol. 20, no. 4, pp. 521–533. Dostupné na: DOI: 10.1177/1023263X1302000404.
SCHMITT, Michael – VIHUL, Liis (eds.): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017. ISBN 978-1-107-17722-2.

SMEJKAL, V.: Kybernetická kriminalita. 2. vyd. Plzeň : Aleš Čeněk, 2018;

SMEJKAL, V.: Současné možnosti boje proti počítačové kriminalitě. In Data Security Management. 2016, č. 4;.

SOLOVE, Daniel J. Nothing to Hide: The False Tradeoff between Privacy and Security. Yale University Press, 2011.
SREBALOVÁ, M. a kol. Zákon o priestupkoch. 2. vydanie. Bratislava: C. H. Beck, 2020, s. 16–23.

SREBALOVÁ, M. Absorbčná zásada vo vnútroštátnej právnej úprave správneho trestania. In. *Lenhart, M., Hapčová, I., Hamuľák, J. (ed).* 2016. Vplyv európskeho práva na kreovanie princípov a zásad správneho trestania: Zborník príspevkov z medzinárodnej vedeckej

konferencie Bratislavské právnické fórum 2016 organizovanej Univerzitou Komenského v Bratislave, Právnickou fakultou v dňoch 21. – 22. októbra 2016. Bratislava : Univerzita komenského v Bratislave, právnická fakulta, vydavateľské oddelenie, s. 182 – 189. ISBN 978-80-7160-430-3.

STOUFFER, Keith; PEASE, Michael; TANG, CheeYee; ZIMMERMAN, Timothy; PILLITTERI, Victoria; LIGHTMAN, Suzanne; HAHN, Adam; SARAVIA, Stephanie; SHERULE, Aslam and THOMPSON, Michael. Guide to Operational Technology (OT) Security. NIST Special Publication 800-82 Rev. 3 [online]. Gaithersburg, MD: National Institute of Standards and Technology, 2023 Dostupné na: DOI: 10.6028/NIST.SP.800-82r3.

STERIO, Milena – TRAHAN, Jennifer: Cyber Operations as Crimes at the International Criminal Court. West Point: Lieber Institute for Law & Land Warfare, 4. 10. 2023. Dostupné na: https://lieber.westpoint.edu/cyber-operations-crimes-icc/.

STOYCHEFF, Elizabeth. Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring. Journalism & Mass Communication Quarterly, 2016, roč. 93, č. 2, s. 296.

STRÉMY, T., KURILOVSKÁ, L., REMETA, R. a kol.. Trestný zákon- praktický komentár. Wolters Kluwer, Bratislava, ISBN: 978-80-286-0378-6, 2025;

STRÉMY, T., KURILOVSKÁ, R. a kol.. Trestný zákon. Komentár. Wolters Kluwer, Bratislava, 2022;

SVÁK, J., GRUNWALD, T.: Nadnárodné systémy ochrany ľudských práv I. Bratislava: Wolters Kluwer, 2019.

SVÁK, J.: Nadnárodné systémy ochrany ľudských práv II. Bratislava: Wolters Kluwer, 2020.

SVÁK, J.: Nadnárodné systémy ochrany ľudských práv III. Bratislava: Wolters Kluwer, 2021.

SVÁK, Ján – GRÜNWALD, Tomáš: Nadnárodné systémy ochrany ľudských práv. I. zväzok. Štruktúra systémov a ochrana politických práv. Bratislava: Wolters Kluwer, 2019. ISBN 9788081689710.

SVÁK, Ján – MAREČEK, Lukáš a kol.: Medzinárodné právo verejné a úvod do verejného medzinárodného práva. Bratislava: Wolters Kluwer, 2024. ISBN 978-80-571-0704-0.

ŠAMKO, P.: Daňové podvodné konania a ich dokazovanie. Bratislava : Wolters Kluwer, 2015;

ŠTURMA, P. Mezinárodní trestní soud a stíhaní zločinu podle mezinárodního práva, Nakladatelství Karolínum, Praha 2002, ISBN 80-246-0305-5,

ŠTURMA, Pavel: „Náležitá péče" v mezinárodním právu: obecný pojem s variabilným obsahem. In: Právník, č. 6, 2021. s. 401—415.

TJOA, Simon; GAFIĆ, Melisa and KIESEBERG, Peter. Cyber Resilience Fundamentals. Cham: Springer, 2024. Studies in Systems, Decision and Control, vol. 520 [online]. Dostupné na: DOI: 10.1007/978-3-031-52064-8.

TOVO, Carlo. Judicial Review of Harmonised Standards: Changing the Paradigms of Legality and Legitimacy of Private Rulemaking under EU Law. Common Market Law Review. 2018, vol. 55, no. 4, pp. 1187–1216. Dostupné na: DOI: 10.54648/COLA2018096.

TURAY, L.; MIHÁLIK, S.; CÁDRA, R.; PETRIČKO, D. a kol. Trestný zákon. Komentár. 1. vydanie. Bratislava: C. H. Beck, 2025;

VAELE, M. – BORGESIUS, F.Z.: Demystifying the Draft EU Artificial Intelligence Act. DOI: https://arxiv.org/ct?url=https%3A%2F%2Fdx.doi.org%2F10.9785%2Fcri-2021-220402&v=ec7cae1dm.

VAELE, M., BORGESIUS, F. Z.: Demystifying the Draft EU Artificial Intelligence Act. Dostupné na: https://dx.doi.org/10.9785/cri-2021-220402.

VALUCH, Jozef – OZORÁKOVÁ, Lilla (eds.): Aktuálne bezpečnostné výzvy a medzinárodné právo. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2021.

VAN DE POEL, I.: Core Values and Value Conflicts in Cybersecurity: Beyond Privacy versus Security. In

VAN DIJK, N. – CASIRAGHI, S. – GUTWIRTH, S.: The 'Ethification' of ICT Governance. Artificial Intelligence and Data Protection in the European Union. In Computer law & security review 43 (2021).

VAN, DEM HOVEN a kol.: Engineering and the Problem of Moral Overload. In Sci Eng Ethics. 2012; 18(1), s. 143–155.

VAN GESTEL, Rob and MICKLITZ, Hans-W. European Integration through Standardisation: How Judicial Review Is Breaking Down the Club House of Private Standardisation Bodies. Common Market Law Review. 2013, vol. 50, no. 1, pp. 145–181. Dostupné na: DOI: 10.54648/COLA2013007.

VON SOLMS, Rossouw and VAN NIEKERK, Johan. From information security to cyber security. Computers & Security. 2013, vol. 38, pp. 97–102. ISSN 0167-4048. Dostupné na: DOI: 10.1016/j.cose.2013.04.004.

VOJTUŠ, F., KORDÍK, M.: K možnostiam a problémom získania dôkazov z asistenčných systémov vozidiel a automatizovaných vozidiel. In Právny obzor, 109, 2026;

VOLPATO, Annalisa. The Legal Effects of Harmonised Standards in EU Law. REALaw.blog [online]. 27 October 2023 Dostupné na: https://realaw.blog/?p=2879.

VRABKO, M. a kol. Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava : Ch. H. Beck, 2025, 344 s. ISBN 978-80-8232-068-1.

VRABKO, M. a kol. Správne právo procesné. Všeobecná časť. 1. vydanie. Bratislava : C. H. Beck, 2013, 304 s. ISBN 978-80-89603-13-8.

WARDLE, C., DERAKSHANB, H. Information Disorder, Council of Europe, Strasbourg, 2017.

WILLIAMS, B. K.: Cyberattack on Ukrainian power company a 'coordinated effort'. Dostupné na: https://thehill.com/policy/cybersecurity/265394-cyberattack-on-ukrainian-power-company-a-coordinated-effort.

ZÁHORA, J.: Aktuálne trendy v postihu počítačovej kriminality v Slovenskej republike. In Justičná revue. 2016, č. 3;
ZÁHORA, J.: Uplatňovanie zásady primeranosti a zdržanlivosti pri využívaní informačno-technických prostriedkov v trestnom konaní v Slovenskej republike. In Časopis pro právní vědu a praxi 2018, č. 1;

ZEDNER, Lucia. Pre-Crime and Post-Criminology? Theoretical Criminology, 2007, roč. 11, č. 2, s. 261.

ZUBOFF, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Profile Books, 2019.

Dokumenty a právne predpisy zo zahraničia

Article 29 Working Party Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01.

CISA: Understanding Denial-of-Service Attacks, [online] [21.3.2022]. Dostupné na: https://www.cisa.gov/uscert/ncas/tips/ST04-015.

Důvodová zpráva k návrhu zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Dostupné na: https://www.psp.cz/sqw/text/tiskt.sqw?o=7&ct=81&ct1=0.

ENISA: Threat Landscape 2021. Október 2021, [online] [21.3.2022]. Dostupné na: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

ENISA: Threat landscape report 2018. Január 2019, [online] [21.3.2022]. Dostupné na: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

EUROPEAN UNION AGENCY FOR CYBERSECURITY. ENISA Threat Landscape 2025 [online]. Athens: ENISA, October 2025 ISBN 978-92-9204-723-8. DOI: 10.2824/1946374. Dostupné na: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.

EUROPEAN UNION AGENCY FOR CYBERSECURITY. AI Cybersecurity Challenges: Threat Landscape for Artificial Intelligence [online]. Luxembourg: Publications Office of the European Union, 2020 ISBN 978-92-9204-462-6. Dostupné na: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Artificial%20Intelligence%20Cybersecurity%20Challenges.pdf.

EUROPEAN UNION AGENCY FOR CYBERSECURITY. ENISA NIS360 2024: Cybersecurity Maturity & Criticality Assessment of NIS2 Sectors [online]. Athens: ENISA, 2025 ISBN 978-92-9204-687-3. Dostupné na: https://www.enisa.europa.eu/publications/enisa-nis360-2024.

EUROPEAN DATA PROTECTION BOARD: Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Version 2.0. Adopted on 18 June 2021.

EUROPOL. Steal, deal and repeat: How cybercriminals trade and exploit your data – Internet Organised Crime Threat Assessment [online]. Luxembourg: Publications Office of the European Union, 2025 Dostupné na: https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data.

EUROPOL: Bank Phishing E-mails, [online] [21.3.2022]. Dostupné na: https://www.europol.europa.eu/sites/default/files/documents/4_ceo-bec_fraud.pdf.

EUROPOL: Internet organised crime threat assessment (IOCTA) 2020, [online] [21.3.2022]. Dostupné na:https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf.

Expertná skupina na vysokej úrovni pre umelú inteligenciu: Etické usmernenia pre dôveryhodnú umelú inteligenciu. Dostupné na: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_SK.pdf.

EUROPEAN DATA PROTECTION SUPERVISOR. Study on the Essence of the fundamental rights to privacy and to the protection of personal data. 2023. Dostupné na: https://www.edps.europa.eu/data-protection/our-work/publications/papers/2023-11-08-study-essence-fundamental-rights-privacy-and-protection-personal-data_en.

EUROPEAN DATA PROTECTION SUPERVISOR. Data protection. Dostupné na: https://www.edps.europa.eu/data-protection/data-protection_en.

HAGGERTY, Kevin D.; ERICSON, Richard V. The Surveillant Assemblage. British Journal of Sociology, 2000, roč. 51, č. 4, s. 605.

FIRST. Common Vulnerability Scoring System SIG, [online] [21.3.2022]. Dostupné na: https://www.first.org/cvss/.

International Organization for Standardization, International Electrotechnical Commission. ISO/IEC 27000: 2018 - Information technology—Security techniques—Information security management systems—Overview and vocabulary.

International Organization for Standardization, International Electrotechnical Commission. ISO/IEC 27032: 2012 – Information technology—Security techniques—Guidelines for cybersecurity.

International Organization for Standardization, International Electrotechnical Commission. ISO/IEC 15408-1:2005 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model.

International Organization for Standardization, International Electrotechnical Commission. ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management.

INTERPOL: Cryptojacking. September 2020, [online] [21.3.2022]. Dostupné na: https://www.interpol.int/content/download/15670/file/Cybercrime-Cryptojacking-EN.pdf.

Akt Rady z 29. mája 2000 potvrdzujúci v súlade s článkom 34 Zmluvy o Európskej únii Dohovor o vzájomnej pomoci v trestných veciach medzi členskými štátmi Európskej únie. (Ú. v. EÚ C 197, 12.7.2000).

KOMISA: Správa Komisie Európskemu parlamentu a Rade o posúdení jednotnosti prístupov členských štátov pri identifikácii prevádzkovateľov základných služieb v súlade s článkom 23 ods. 1 smernice 2016/1148/EÚ o bezpečnosti sietí a informačných systémov.

Predpis OSN č. 155 – Jednotné ustanovenia na účely typového schvaľovania vozidiel vzhľadom na kybernetickú bezpečnosť a systém riadenia kybernetickej bezpečnosti [2021/387].

Dohovor Rady Európy o počítačovej kriminalite, oznámenie MZV SR č. 137/2008 Z. z. o podpísaní Dohovoru o počítačovej kriminalite.

Usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu stanovených v nariadení (EÚ) 2024/1689 z 29.7.2025, s. 100. Dostupné na LINK.

Konsolidované znenie Zmluvy o fungovaní Európskej únie.

RADA EURÓPY: Study on the human rights dimensions of automated data rocessing techniques (in particular algorithms) and possible regulatory implications. 2017. Dostupné na: https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5.

EURÓPSKA KOMISIA: European Declaration on Digital Rights and Principles. December 2022. Dostupné na: https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles.

European Parliamentary Research Service: Artificial intelligence act and regulatory sandboxes. Jún 2022. Dostupné na: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733544/EPRS_BRI(2022)733544_EN.pdf.
https://www.flaw.uniba.sk/fileadmin/praf/Pracoviska/Ustavy/UPITPDV/PST_PI/Regulatory_sandbox_ako_nastroj_pre_efektivnu_regulaciu_AV_Kostalova.pdf

U.S. DEPARTMENT OF THE INTERIOR: Penetration Testing, [online] [21.3.2022]. Dostupné na: https://www.doi.gov/ocio/customers/penetration-testing.

U.S. DEPARTMENT OF HOMELAND SECURITY: The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research. 2012. Dostupné na: https://www.dhs.gov/sites/default/files/publications/CSD-MenloPrinciplesCORE-20120803_1.pdf.

Odporúčanie CM/Rec(2018)7 Výboru ministrov Rady Európy o usmerneniach na rešpektovanie, ochranu a napĺňanie práv dieťaťa v digitálnom prostredí.

Európska schéma kybernetickej certifikácie založená na Common Criteria; Vykonávacie nariadenie Komisie (EÚ) 2024/482 z 31. januára 2024, ktorým sa stanovujú pravidlá uplatňovania nariadenia (EÚ) 2019/881, pokiaľ ide o prijatie európskej schémy kybernetickej certifikácie založenej na Common Criteria (EUCC).

EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliace with the EU level of protection of personal data. Version 2.0. Adopted on 18 June 2021.

Attack (international humanitarian law). International Cyber Law: Interactive Toolkit. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2025. Dostupné na: https://cyberlaw.ccdcoe.org/wiki/Attack_%28international_humanitarian_law%29.

Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries. In: Yearbook of the International Law Commission, 2001, vol. II, Part Two, as corrected.

Heirs of the Duc de Guise, UNRIAA, vol. XIII, 1951.

ICC Cyberwar Crimes. WIRED. Dostupné na: https://www.wired.com/story/icc-cyberwar-crimes/.

ICRC: International humanitarian law and the challenges of contemporary armed conflicts. Geneva: ICRC, October 2015. 32nd International Conference of the Red Cross and Red Crescent (32IC/15/11). Dostupné na: https://www.icrc.org/sites/default/files/document/file_list/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf.

ICRC: International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC position paper. November 2019. Dostupné na: https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf.

International Criminal Court, Office of the Prosecutor: Policy on Cyber-Enabled Crimes under the Rome Statute. The Hague: International Criminal Court, 2025. Dostupné na: https://www.icc-cpi.int/sites/default/files/2025-12/2025-cyber-eng.pdf.

League of Nations, Conference for the Codification of International Law: Bases of Discussion for the Conference drawn up by the Preparatory Committee, vol. III: Responsibility of States for Damage caused in their Territory to the Person or Property of Foreigners, document C.75.M.69.1929.V.

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996.

NATO: Brussels Summit Communiqué, 14 June 2021.

NATO: Wales Summit Declaration, 5 September 2014.

Open-ended working group on developments in the field of information and telecommunications in the context of international security, A/AC.290/2021/CRP.2.

Rainbow Warrior affair, UNRIAA, vol. XX, 1990.

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98.

Treatment of Polish Nationals and Other Persons of Polish Origin or Speech in the Danzig Territory, Advisory Opinion, PCIJ Series A/B, No. 44, 1932.

Ženevský dohovor o ochrane civilných osôb počas vojny.

Viedenský dohovor o diplomatických stykoch z roku 1961.

Viedenský dohovor o zmluvnom práve z roku 1969.

Budapeštiansky dohovor o počítačovej kriminalite, 2001.

Dodatkový protokol I z roku 1977 k Ženevským dohovorom o ochrane obetí vojny z roku 1949.

Dodatkový protokol II z roku 1977 k Ženevským dohovorom o ochrane obetí vojny z roku 1949.

Rezolúcia Valného zhromaždenia OSN A/RES/29/3314.Charta základných práv Európskej únie (2016/C 202/02), Ú. v. EÚ C 202, 7. 6. 2016.

Dohovor o ochrane jednotlivcov pri automatizovanom spracúvaní osobných údajov, oznámenie Ministerstva zahraničných vecí Slovenskej republiky č. 49/2001 Z. z.

Dohovor o počítačovej kriminalite, oznámenie Ministerstva zahraničných vecí Slovenskej republiky č. 137/2008 Z. z.

Dohovor o právach dieťaťa, oznámenie Federálneho ministerstva zahraničných vecí č. 104/1991 Zb.

Dohovor OSN proti počítačovej kriminalite (Hanojský dohovor), prijatý Valným zhromaždením OSN v roku 2024.

Európsky dohovor o ochrane ľudských práv a základných slobôd, oznámenie Federálneho ministerstva zahraničných vecí č. 209/1992 Zb.

Globálny digitálny pakt (Global Digital Compact), prijatý rezolúciou Valného zhromaždenia OSN A/RES/79/1 *The Pact for the Future* z 22. septembra 2024.

Konsolidované znenie Zmluvy o Európskej únii, Ú. v. EÚ C 202, 7. 6. 2016.

Konsolidované znenie Zmluvy o fungovaní Európskej únie, Ú. v. EÚ C 202, 7. 6. 2016.

Opčný protokol k Dohovoru o právach dieťaťa o predaji detí, detskej prostitúcii a detskej pornografii, oznámenie Ministerstva zahraničných vecí Slovenskej republiky č. 424/2004 Z. z.

Opčný protokol k Dohovoru o právach dieťaťa o procedúre oznámení, oznámenie Ministerstva zahraničných vecí a európskych záležitostí Slovenskej republiky č. 91/2014 Z. z.

Opčný protokol k Dohovoru o právach dieťaťa o účasti detí v ozbrojených konfliktoch, oznámenie Ministerstva zahraničných vecí Slovenskej republiky č. 256/2009 Z. z.

Rámcový dohovor Rady Európy o umelej inteligencii, ľudských právach, demokracii a právnom štáte, CETS No. 225, Štrasburg, 2024.

Dohovor Rady Európy o ochrane detí pred sexuálnym vykorisťovaním a sexuálnym zneužívaním (Lanzarotský dohovor), oznámenie Ministerstva zahraničných vecí Slovenskej republiky č. 164/2016 Z. z.

Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (CRC/C/156).

Všeobecný komentár č. 25 (2021) Výboru OSN pre práva dieťaťa o právach dieťaťa v súvislosti s digitálnym prostredím.

Všeobecný komentár č. 16 (2013) Výboru OSN pre práva dieťaťa o povinnostiach štátu v súvislosti s vplyvom podnikateľského sektora na práva detí.

Všeobecný komentár č. 5 (2003) Výboru OSN pre práva dieťaťa o všeobecných vykonávacích opatreniach Dohovoru o právach dieťaťa.

Vysvetlivky k Charte základných práv Európskej únie (2007/C 303/02).
Nariadenie Rady (EÚ) 2019/796 zo 17. mája 2019 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty;

Rada Európy, Európsky dohovor o ochrane ľudských práv a základných slobôd v znení protokolov č. 11 a 14, 4. november 1950, ETS 5. Dostupné na: LINK.

Rámcové rozhodnutie Rady 2002/465/SVV z 13. júna 2002 o spoločných vyšetrovacích tímoch.

Rámcové rozhodnutie Rady 2003/577/SVV z 22. júla 2003 o vykonaní príkazu na zaistenie majetku alebo dôkazov v Európskej únii.

Rámcové rozhodnutie Rady 2008/978/SVV z 18. decembra 2008 o európskom príkaze na zabezpečenie dôkazov na účely získavania predmetov, dokumentov a údajov na použitie v konaniach v trestných veciach (Ú. v. EÚ L 350, 30.12.2008).

Rozhodnutie Rady 2009/820/SZBP z 23. októbra 2009 o uzavretí v mene Európskej únie Dohody o extradícii medzi Európskou úniou a Spojenými štátmi americkými a Dohody o vzájomnej právnej pomoci medzi Európskou úniou a Spojenými štátmi americkými.

Rozhodnutie Rady 2010/616/EÚ zo 7. októbra 2010 o uzavretí Dohody medzi Európskou úniou a Japonskom o vzájomnej právnej pomoci v trestných veciach.

Charta základných práv Európskej únie (2016/C 202/02), Ú. v. EÚ C 202, 7. 6. 2016.

Uznesenie Valného zhromaždenia OSN č. 79/243 zo dňa 24. decembra 2024 o prijatí Dohovoru Organizácie spojených národov proti počítačovej kriminalite. Dostupné dňa 30.03.2026 na: LINK.

Rozhodnutie Rady 2020/1127 z 30. júla 2020, ktorým sa mení rozhodnutie (SZBP) 2019/797 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty.

Legislatívne akty EÚ

Nariadenie Európskeho parlamentu a Rady (ES) č. 1060/2009 zo 16. septembra 2009 o ratingových agentúrach.

Nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 zo 4. júla 2012 o mimoburzových derivátoch, centrálnych protistranách a archívoch obchodných údajov (EMIR).

Nariadenie Európskeho parlamentu a Rady (EÚ) č. 575/2013 z 26. júna 2013 o prudenciálnych požiadavkách na úverové inštitúcie a investičné spoločnosti a o zmene nariadenia (EÚ) č. 648/2012 (CRR).

Nariadenie Európskeho parlamentu a Rady (EÚ) č. 600/2014 z 15. mája 2014 o trhoch s finančnými nástrojmi, ktorým sa mení nariadenie (EÚ) č. 648/2012 (MiFIR).

Nariadenie Európskeho parlamentu a Rady (EÚ) č. 806/2014 z 15. júla 2014, ktorým sa stanovujú jednotné pravidlá a jednotný postup riešenia krízových situácií úverových inštitúcií a určitých investičných spoločností v rámci jednotného mechanizmu riešenia krízových situácií a jednotného fondu na riešenie krízových situácií (SRM).

Nariadenie Európskeho parlamentu a Rady (EÚ) č. 909/2014 z 23. júla 2014 o zlepšení vyrovnania transakcií s cennými papiermi v Európskej únii a o centrálnych depozitároch cenných papierov (CSDR).

Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/794 z 11. mája 2016 o Agentúre Európskej únie pre spoluprácu v oblasti presadzovania práva (Europol), ktorým sa nahrádzajú a zrušujú rozhodnutia Rady 2009/371/SVV, 2009/934/SVV, 2009/935/SVV, 2009/936/SVV a 2009/968/SVV (Ú. v. EÚ L 135, 24.5.2016).

Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/1011 z 8. júna 2016 o indexoch používaných ako referenčné hodnoty vo finančných nástrojoch a finančných zmluvách alebo na meranie výkonnosti investičných fondov (BMR).

Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/2402 z 12. decembra 2017, ktorým sa stanovuje všeobecný rámec pre sekuritizáciu a vytvára osobitný rámec pre jednoduchú, transparentnú a štandardizovanú sekuritizáciu.

Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018).

Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1727 zo 14. novembra 2018 o Agentúre Európskej únie pre justičnú spoluprácu v trestných veciach (Eurojust) a o nahradení a zrušení rozhodnutia Rady 2002/187/SVV (Ú. v. EÚ L 295, 21.11.2018).

Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1805 zo 14. novembra 2018 o vzájomnom uznávaní príkazov na zaistenie a príkazov na konfiškáciu.

Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti).

Nariadenie Európskeho parlamentu a Rady (EÚ) 2020/1503 zo 7. októbra 2020 o európskych poskytovateľoch služieb hromadného financovania pre podnikanie.

Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011 (DORA).

Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1114 z 31. mája 2023 o trhoch s kryptoaktívami a o zmene nariadení (EÚ) č. 1093/2010 a (EÚ) č. 1095/2010 a smerníc 2013/36/EÚ a (EÚ) 2019/1937 (MiCA).

Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1543 z 12. júla 2023 o európskych príkazoch na predloženie elektronických dôkazov a európskych príkazoch na uchovanie elektronických dôkazov v trestnom konaní a na výkon trestu odňatia slobody v nadväznosti na trestné konanie.

Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii).

Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti).

Delegované nariadenie Komisie (EÚ) 2024/1772 z 13. marca 2024, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, v ktorých sa bližšie určujú klasifikačné kritériá incidentov súvisiacich s IKT a kybernetických hrozieb, stanovujú prahové hodnoty významnosti a spresňujú podrobnosti správ o závažných incidentoch.

Delegované nariadenie Komisie (EÚ) 2024/1774 z 13. marca 2024, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, v ktorých sa bližšie určujú nástroje, metódy, postupy a politiky riadenia rizika v oblasti IKT.

Delegované nariadenie Komisie (EÚ) 2025/301 z 23. októbra 2024, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, v ktorých sa stanovuje obsah a lehoty na počiatočné oznámenie, a priebežnú a záverečnú správu o závažných incidentoch súvisiacich s IKT a obsah dobrovoľného oznamovania v prípade významných kybernetických hrozieb.

Delegované nariadenie Komisie (EÚ) 2025/1190 z 13. februára 2025, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, v ktorých sa bližšie špecifikujú kritériá používané na identifikáciu finančných subjektov povinných vykonať penetračné testovanie na základe konkrétnej hrozby (TLPT),

požiadavky a normy upravujúce využívanie interných testovacích subjektov, ako aj požiadavky týkajúce sa rozsahu, metodiky a jednotlivých fáz testovania a spolupráce v oblasti dohľadu.

Vykonávacie nariadenie Komisie (EÚ) 2025/302 z 23. októbra 2024, ktorým sa stanovujú vykonávacie technické predpisy na uplatňovanie nariadenia Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o štandardné formuláre, vzory a postupy pre finančné subjekty na nahlasovanie závažných incidentov súvisiacich s IKT a na oznamovanie významných kybernetických hrozieb.

Smernica Európskeho parlamentu a Rady 2009/65/ES z 13. júla 2009 o koordinácii zákonov, iných právnych predpisov a správnych opatrení týkajúcich sa podnikov kolektívneho investovania do prevoditeľných cenných papierov (PKIPCP).

Smernica Európskeho parlamentu a Rady 2009/110/ES zo 16. septembra 2009 o začatí a vykonávaní činností a dohľade nad obozretným podnikaním inštitúcií elektronického peňažníctva, ktorou sa menia a dopĺňajú smernice 2005/60/ES a 2006/48/ES a zrušuje smernica 2000/46/ES.

Smernica Európskeho parlamentu a Rady 2009/138/ES z 25. novembra 2009 o začatí a vykonávaní poistenia a zaistenia (Solventnosť II).
Smernica Európskeho parlamentu a Rady 2011/61/EÚ z 8. júna 2011 o správcoch alternatívnych investičných fondov a o zmene a doplnení smerníc 2003/41/ES a 2009/65/ES a nariadení (ES) č. 1060/2009 a (EÚ) č. 1095/2010.

Smernica Európskeho parlamentu a Rady 2011/92/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorou sa nahrádza rámcové rozhodnutie Rady 2004/68/SVV.

Smernica Európskeho parlamentu a Rady 2013/36/EÚ z 26. júna 2013 o prístupe k činnosti úverových inštitúcií a prudenciálnom dohľade nad úverovými inštitúciami a investičnými

spoločnosťami, o zmene smernice 2002/87/ES a o zrušení smerníc 2006/48/ES a 2006/49/ES (CRD).

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.

Smernica Európskeho parlamentu a Rady 2014/41/EÚ z 3. apríla 2014 o európskom vyšetrovacom príkaze v trestných veciach.

Smernica Európskeho parlamentu a Rady 2014/53/EÚ zo 16. apríla 2014 o harmonizácii právnych predpisov členských štátov týkajúcich sa sprístupňovania rádiových zariadení na trhu, ktorou sa zrušuje smernica 1999/5/ES.

Smernica Európskeho parlamentu a Rady 2014/59/EÚ z 15. mája 2014, ktorou sa stanovuje rámec pre ozdravenie a riešenie krízových situácií úverových inštitúcií a investičných spoločností (BRRD).

Smernica Európskeho parlamentu a Rady 2014/65/EÚ z 15. mája 2014 o trhoch s finančnými nástrojmi, ktorou sa mení smernica 2002/92/ES a smernica 2011/61/EÚ (MiFID II).

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 (PSD2).

Smernica Európskeho parlamentu a Rady (EÚ) 2016/97 z 20. januára 2016 o distribúcii poistenia (IDD).

Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 o presadzovaní práva v oblasti ochrany údajov.

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 (Ú. v. EÚ L 194/1, 19.07.2016).

Smernica Európskeho parlamentu a Rady (EÚ) 2016/2341 zo 14. decembra 2016 o činnostiach inštitúcií zamestnaneckého dôchodkového zabezpečenia a o dohľade nad nimi (IORP II).

Smernica Európskeho parlamentu a Rady (EÚ) 2019/713 zo 17. apríla 2019 o boji proti podvodom s bezhotovostnými platobnými prostriedkami a proti ich falšovaniu a pozmeňovaniu, ktorou sa nahrádza rámcové rozhodnutie Rady 2001/413/SVV.

Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) (Ú. v. EÚ L 333, 27.12.2022).

Smernica Európskeho parlamentu a Rady (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/114/ES.

Smernica Európskeho parlamentu a Rady (EÚ) 2023/1544 z 12. júla 2023, ktorou sa stanovujú harmonizované pravidlá určovania určených prevádzkarní a vymenúvania právnych zástupcov na účely zhromažďovania dôkazov v trestnom konaní, Ú. v. EÚ L 191, , s. 181–190.

Smernica Európskeho parlamentu a Rady (EÚ) 2023/1544 z 12. júla 2023, ktorou sa stanovujú harmonizované pravidlá určovania určených prevádzkarní a vymenúvania právnych zástupcov na účely zhromažďovania dôkazov v trestnom konaní.

Smernica Európskeho parlamentu a Rady (EÚ) 2024/1260 o konfiškáciách.

Smernica Európskeho parlamentu a Rady (EÚ) 2024/2853 z 23. októbra 2024 o zodpovednosti za chybné výrobky a o zrušení smernice Rady 85/374/EHS.

Právne predpisy Slovenskej republiky

Zákon č. 71/1967 Zb. o správnom konaní (správny poriadok).

Zákon SNR č. 372/1990 Zb. o priestupkoch.

Zákon č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov.

Zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným odpočúvaním a použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Zákon č. 514/2003 Z. z. o zodpovednosti za škodu spôsobenú pri výkone verejnej moci a o zmene niektorých zákonov.

Zákon č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení zákona č. 284/2002 Z. z.

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

Zákon č. 541/2004 Z. z. o mierovom využívaní jadrovej energie a o zmene a doplnení niektorých zákonov.

Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov.

Zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov.

Zákon č. 40/2015 Z. z. o audiovízii a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Zákon č. 91/2016 Z. z. o trestnej zodpovednosti právnických osôb a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Zákon č. 236/2017 Z. z. o európskom vyšetrovacom príkaze v trestných veciach v znení neskorších predpisov.

Zákon č. 274/2017 Z. z. o obetiach trestných činov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe.

Zákon č. 187/2021 Z. z. o ochrane hospodárskej súťaže a o zmene a doplnení niektorých zákonov.

Zákon č. 264/2022 Z. z. o mediálnych službách a o zmene a doplnení niektorých zákonov (zákon o mediálnych službách) v znení neskorších predpisov.

Zákon č. 367/2024 Z. z. o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov.

Vyhláška Národného bezpečnostného úradu č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov.

Vyhláška Národného bezpečnostného úradu č. 48/2019 Z. z., ktorou sa ustanovujú podrobnosti o administratívnej bezpečnosti utajovaných skutočností.

Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.

Vyhláška Národného bezpečnostného úradu č. 492/2022 Z. z., ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti.
Vyhláška Národného bezpečnostného úradu č. 493/2022 Z. z. o audite kybernetickej bezpečnosti.

Vyhláška Národného bezpečnostného úradu č. 226/2025 Z. z., ktorou sa ustanovujú podrobnosti o hláseniach.

Vyhláška Národného bezpečnostného úradu č. 227/2025 Z. z. o bezpečnostných opatreniach.

Nariadenie vlády č. 216/2004 Z. z., ktorým sa ustanovujú oblasti utajovaných skutočností.

Rozhodnutia

ESĽP, Copland proti Spojenému kráľovstvu, č. 62617/00, rozsudok z 3. 4. 2007.

ESĽP, Huvig proti Francúzsku, rozsudok z 24. 4. 1990, Series A no. 176-B.

ESĽP, Malone proti Spojenému kráľovstvu, rozsudok z 2. 8. 1984, Series A no. 82.

ESĽP, Roman Zakharov proti Rusku, č. 47143/06, rozsudok Veľkej komory z 4. 12. 2015.

ESĽP, Weber a Saravia proti Nemecku, č. 54934/00, rozhodnutie o prijateľnosti z 29. 6. 2006.

Rozsudok Európskeho súdu pre ľudské práva zo dňa 2. decembra 2008, K.U. proti Fínsku, sťažnosť č. 2872/02

ECHR: Ahmet Yildirim v. Turkey, no. 3111/10, Judgment, 18. 12. 2012.

ECHR: Jankovskis v. Lithuania, no. 21575/08, Judgment, 17. 1. 2017.

Rozsudok Súdneho dvora EÚ (veľká komora), spojené veci C-293/12 a C-594/12, Digital Rights Ireland a Seitlinger a i.

Rozsudok Súdneho dvora EÚ, vo veci C-610/15, Stichting Brein proti Ziggo BV and XS4ALL Internet BV ('XS4ALL').

Rozsudok Súdneho dvora EÚ, vo veci C-439/19, Latvijas Republikas Saeima.

Rozsudok Súdneho dvora EU, vo veci C-724/19, Specializirana prokuratura.

Rozsudok Súdneho dvora EÚ, vo veci C-852/19, Gavanozov II.

Rozsudok Súdneho dvora EÚ, vo veci C-817/19; Ligue des droits humains proti Rade.

Rozsudok Súdneho dvora EÚ, vo veci C-204/21, Komisia proti Poľsko.

Rozsudok Súdneho dvora EÚ, vo veci C-670/22 Encrochat.

Rozsudok Súdneho dvora EÚ, vo veci C-511/18, C-512/18 a C-520/18, La Quadrature du Net a i.

SDEÚ, spojené veci C-203/15 a C-698/15, Tele2 Sverige AB v. Post- och telestyrelsen a Secretary of State for the Home Department v. Watson a i., rozsudok z 21. 12. 2016.

SDEÚ, spojené veci C-293/12 a C-594/12, Digital Rights Ireland Ltd a Kärntner Landesregierung, rozsudok z 8. 4. 2014.

COURT OF JUSTICE OF THE EUROPEAN UNION. Judgment of the Court, 12 July 2012, Fra.bo SpA v Deutsche Vereinigung des Gas- und Wasserfaches eV (DVGW) – Technisch-Wissenschaftlicher Verein, C-171/11, ECLI:EU:C:2012:453.

COURT OF JUSTICE OF THE EUROPEAN UNION. Judgment of the Court, 5 March 2024, Public.Resource.Org, Inc. and Right to Know CLG v European Commission, C-588/21 P, ECLI:EU:C:2024:201, para. 73.

COURT OF JUSTICE OF THE EUROPEAN UNION. Judgment of the Court, 12 July 2012, Fra.bo SpA v Deutsche Vereinigung des Gas- und Wasserfaches eV (DVGW) – Technisch-Wissenschaftlicher Verein, C-171/11, ECLI:EU:C:2012:453, paras. 27–32.

COURT OF JUSTICE OF THE EUROPEAN UNION. Judgment of the Court, 27 October 2016, James Elliott Construction Limited v Irish Asphalt Limited, C-613/14, ECLI:EU:C:2016:821, paras. 34 and 40.

COURT OF JUSTICE OF THE EUROPEAN UNION. Opinion of Advocate General Medina, 22 June 2023, Public.Resource.Org, Inc. and Right to Know CLG v European Commission, C-588/21 P, ECLI:EU:C:2023:509.

US District Court of Columbia, US v. Roman Sterlingov, case n. 21-399. Dostupné dňa 19.12.2025 na: LINK .

Rozhodnutie Súdneho dvora Európskej únie, C-1/11 - Interseroh Scrap and Metals Trading.

Rozhodnutie Súdneho dvora Európskej únie, C-101/01- Lindqvist.

Rozhodnutie Súdneho dvora Európskej únie, C-212/13-Ryneš.

Rozhodnutie Súdneho dvora Európskej únie, C-582/14 Patrick Breyer proti Bundesrepublik Deutschland.

Rozhodnutie Súdneho dvora Európskej únie, Spojené veci C-293/12 a C-594/12 Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources a i. a Kärntner Landesregierung a i.

Rozhodnutie Súdneho dvora EÚ, vo veci C-185/19, Public.Resource.Org.

Rozhodnutie Súdneho dvora EÚ, Stanovisko 1/15.

Rozhodnutie Súdneho dvora EÚ, vo veci C-1/11, Interseroh Scrap and Metals Trading.

Rozhodnutie Súdneho dvora EÚ, vo veci C-362/14, Schrems I.

Rozhodnutie Súdneho dvora EÚ, vo veci C-311/18, Schrems II.

Rozhodnutie Súdneho dvora EÚ, spojené veci C-293/12 a C-594/12, Digital Rights Ireland.
Rozsudok Súdneho dvora Európskej únie vo veci C-617/10, *Åkerberg Fransson*.

Rozsudok Súdneho dvora Európskej únie vo veci C-244/06, *Dynamic Medien Vertriebs GmbH proti Avides Media AG*.

Jednotná akcia 97/827/SVV prijatá Radou na základe článku K.3 Zmluvy o Európskej únii, ktorou sa stanovuje mechanizmus na hodnotenie uplatňovania a vykonávania medzinárodných záväzkov v boji proti organizovanému zločinu na národnej úrovni (Ú. v. EÚ L 344, 15.12.1997). Dostupné na: LINK.

KS TT 6To/45/2019.

Nález Ústavného súdu SR sp. zn. III. ÚS 68/2010.

Nález Ústavného súdu SR sp. zn. PL. ÚS 10/2014.

Nález Ústavného súdu SR sp. zn. III. ÚS 172/2010.

Uznesenie Ústavného súdu SR, sp. zn. PL. ÚS 13/2020.

NS ČR 3 Tdo 1031/2021.

NS ČR, sp. zn. 8 Tdo 450/2024.

NS SR sp. zn. 2 Tdo V 21/2014.

NS SR I2 Tdo V 21/2013.

NS SR 2 Tdo 38/2014.

NS SR 2 Tdo 8/2015.

NS SR 3 Tdo 43/2017.

R 4/1974.

R 1/1980.

R 17/1980.

R 27/1982.

R 39/1982.

R 101/2001.

R 8/2009.

R 96/2014.

R 17/2015.

R 8/2017.

R 47/2017.

R 41/2024.

Rozsudok NS SR sp. zn. 8Sžo/28/2007 z 1. septembra 2008.

Uznesenie NS SR sp. zn. 2 Sžf/9/2010 z 16. februára 2011.

Rozsudok NS SR sp. zn. Sžf/44/2011 z 19. októbra 2011.

Rozsudok NS SR sp. zn. 5Sžf/53/2014 zo 16. decembra 2014.

Nález ÚS SR sp. zn. PL. ÚS 12/97 z 15. októbra 1998.

Nález Ústavného súdu SR, sp. zn. PL. ÚS 25/2019-117.

Rozsudok ŠTS 15 T 1/2023.

Odlišné stanovisko Pavla Holländera k nálezu pléna Ústavního soudu zo dňa 3. 4. 1996, PL.ÚS 32/95, 112/1996 Sb., N 26/5 SbNU 215.

Nález Ústavného súdu SR, sp. zn. PL. ÚS 25/2019-117.

Uznesenie NS ČR 3 Tcu 33/2014.

Uznesenie Ústavného súdu SR, sp. zn. PL. ÚS 13/2020.

FRANCISCO Mallén (United Mexican States) v. U.S.A., 27 April 1927. Reports of International Arbitral Awards, vol. IV.

Barcelona Traction, Light and Power Company, Limited, Judgment, I.C.J. Reports 1970.

Corfu Channel Case (United Kingdom v. Albania), Judgment, I.C.J. Reports 1949.

Elettronica Sicula S.p.A. (ELSI), Judgment, I.C.J. Reports 1989.

Foremost Tehran, Inc. v. The Government of the Islamic Republic of Iran, Iran-U.S. C.T.R., vol. 10, 1986.

ICTY: The Prosecutor v. Dusko Tadić, IT-94-1-A, Appeals Chamber, Judgement, 15 July 1999.
Island of Palmas (or Miangas) Case (United States v. Netherlands), Award of 4 April 1928, Reports of International Arbitral Awards, vol. II.

Jurisdictional Immunities of the State (Germany v. Italy: Greece intervening), Judgment, I.C.J. Reports 2012.

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, I.C.J. Reports 1986.

SEDCO, Inc. v. National Iranian Oil Company, Iran-U.S. C.T.R., vol. 15, 1987.

The Case of the S.S. Wimbledon, PCIJ Series A, No. 1, 1923.

Velásquez Rodríguez v. Honduras, Inter-American Court of Human Rights, Series C, No. 4.

Xhavara and Others v. Italy and Albania, application no. 39473/98, European Court of Human Rights, decision of 11 January 2001.

United States Diplomatic and Consular Staff in Tehran, Judgment, I.C.J. Reports 1980.

LaGrand (Germany v. United States of America), Provisional Measures, Order of 3 March 1999, I.C.J. Reports 1999.

Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment, I.C.J. Reports 2003.

Permanent Court of International Justice: S.S. Lotus (France v. Turkey), Judgment, PCIJ Series A, No. 10, 1927.

Kenneth P. Yeager v. The Islamic Republic of Iran, Iran-U.S. C.T.R., vol. 17.

Iné zdroje

Národná rada Slovenskej republiky (2023 – doposiaľ), parlamentná tlač 364 – Vládny návrh zákona o niektorých opatreniach na zlepšenie bezpečnostnej situácie v Slovenskej republike.

Vládny návrh zákona, ktorým sa mení a dopĺňa Trestný poriadok, Legislatívny proces LP/2023/612.

2024 REPORT ON PAYMENT FRAUD, EBA, 2024, dostupné na: LINK;
Spyware [online] [21.3.2022]. Dostupné na: https://malware.fandom.com/wiki/Spyware.

The Digital, the Critical and Fundamental Rights. In CHRISTENSEN, M. et al. (eds).: Ethics of Cybersecurity. Springer, 2020, s. 97 - 116.

Národná rada Slovenskej republiky (2023 – doposiaľ), parlamentná tlač 508 – Vládny návrh zákona, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony.

NÁRODNÁ BANKA SLOVENSKA. TIBER-SK: Implementačný dokument [online]. Bratislava: Národná banka Slovenska, 2025 [cit. 2026-06-07]. Dostupné na internete: https://nbs.sk/dokument/f5665acb-39d2-4fee-bb01-7275de210be2/stiahnut?force=false.

NBÚ: Správa o kybernetickej bezpečnosti v Slovenskej republike v roku 2023. Dostupné na: https://www.nbu.gov.sk/sprava-o-kybernetickej-bezpecnosti-v-slovenskej-republike-v-roku-2023/.

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD. Metodika analýzy rizík kybernetickej bezpečnosti. Verzia 2.0 [online]. Bratislava: Národný bezpečnostný úrad, 2025 Dostupné na: https://www.nbu.gov.sk/data/att/3446.pdf.

Monero, [online] [21.3.2022]. Dostupné na: https://www.getmonero.org/.

Dôvodová správa k Budapeštianskemu dohovoru. Dostupné na: LINK.

MITRE webové sídlo, [online] [21.3.2022]. Dostupné na: https://www.mitre.org/.

MITRE: CVE - Current CVSS Score Distribution For All Vulnerabilities, [online] [12.3.2022]. Dostupné na: https://www.cvedetails.com/index.php.

NÁRODNÝ BEZPENOŠTNÝ ÚRAD SR: Správa o kybernetickej bezpečnosti v Slovenskej republike v roku 2020. Dostupné na: https://www.nbu.gov.sk/wp-content/uploads/urad/Sprava-o-kybernetickej-bezpecnosti-2020.pdf.

Draft Policy on the Cyber Enabled Crimes, Office of the Prosecutor, s. 20, dostupné dňa 06.02.2026 na: LINK.

EMPACT cyklus pre 2026-2029, s. 11. Dostupné dňa 06.02.2025 na: LINK;
Group Governmental Expert Rolling Text of the Convention on Certain Conventional Weapons, July 26th, 2024; dostupné dňa 13.12.2025 na LINK.

Financial Action Task Force (FATF) Report: Countering Ransomware Financing. Marec 2023 dostupné na: LINK.

FBI Internet Crime Report 2024, s. 4 , dostupné dňa 06-02-2026 na: LINK.

Datatilsynet: Regulatory privacy sandbox. Dostupné na: https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/.

CNIL: Bac à sable de données personnelles. Január 2022. Dostupné na: https://www.cnil.fr/fr/bac-sable-donnees-personnelles-la-cnil-lance-un-appel-projets-concernant-les-outils-numeriques.

ICO: Information Commissioner's Office: Regulatory Sandbox. Dostupné na: https://ico.org.uk/for-organisations/advice-and-services/regulatory-sandbox/.

IMY: Swedish Authority for Privacy Protection: Första regulatoriska sandlåda. Jún 2024. Dostupné na: https://www.imy.se/nyheter/forsta-delrapporten-fran-pilotprojekt-om-ai-regulatorisk-sandlada-publicerad/.

ILA Group on Due Diligence in International Law: First Report. 2014. Dostupné online: olympereseauinternational.wordpress.com/wp-content/uploads/2015/07/due_diligence_-_first_report_2014.pdf

Lecture Notes in Business Information Processing, zv. 464. Cham: Springer, s. 570–585. ISBN 978-3-031-30693-8. Dostupné na: https://doi.org/10.1007/978-3-031-30694-5_40 [cit. 2026-04-20].

Project CANVAS. Dostupné na: https://cyberwatching.eu/projects/1267/canvas.

AI and Policing, EUROPOL, s. 24, dostupné dňa 21.10.2025 na: LINK.

Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Center and UN Human Rights Office of the High Commissioner; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, dostupné dňa 10.03.2026 na: LINK.

IOCTA 2025, EUROPOL, dostupné dňa 29.11.2025 na: LINK.

Open source investigations in the age of Google / editors,Henrietta Wilson, SOAS University of London, UK & King's College London, UK,Olamide Samuel, University of Leicester, UK, Dan Plesch, SOAS University of London, UK.Description: New Jersey : World Scientific, [2024] | Series: Security science and technology,2059-1063 ; Vol. 4.

U.S. Department of the Interior. Penetration Testing. Dostupné dňa 31.03.2026 na: LINK.

Valimised: Internet voting in Estonia. Dostupné na: https://www.valimised.ee/en/internet-voting/more-about-i-voting/introduction-i-voting.

Investigatory Powers Tribunal. Dostupné na: https://investigatorypowerstribunal.org.uk/.

ECtHR: When not backed by strong safeguards, mass surveillance violates privacy. Dostupné na: https://ccdcoe.org/incyder-articles/ecthr-when-not-backed-by-strong-safeguards-mass-surveillance-violates-privacy/.

GOV.UK. Profile: GRU cyber and hybrid threat operations [online]. GOV.UK, updated 4 December 2025 Dostupné na: https://www.gov.uk/government/publications/profile-gru-cyber-and-hybrid-threat-operations/profile-gru-cyber-and-hybrid-threat-operations.

FINANCIAL ACTION TASK FORCE. Countering Ransomware Financing [online]. Paris: FATF/OECD, March 2023 Dostupné na: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Countering-Ransomware-Financing.pdf.coredownload.pdf.

OWASP FOUNDATION. AIVSS Scoring System for OWASP Agentic AI Core Security Risks v0.8 [online]. OWASP AI Vulnerability Scoring System, 2026 Dostupné na: https://aivss.owasp.org.

CUSEC
Kompetenčné centrum pre reguláciu kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality

PRÁVNICKÁ FAKULTA
Univerzita Komenského v Bratislave

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

ISBN (e-verzia): 978–80–7160–798–4