UNIVERZITA KARLOVA

Právnická fakulta

JUDr. Kristina Ramešová

Kyberprostor a informační bezpečnost

Disertační práce

Školitel: Prof. JUDr. Richard Pomahač, CSc.

Studijní program: Teoretické právní vědy - Správní právo a správní věda

Datum vypracování práce (uzavření rukopisu): 15. 12. 2022

Prohlašuji, že jsem předkládanou disertační práci vypracovala samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 711 106 znaků včetně mezer.

Kristina Ramešová

V Hradci Králové dne 15. 12. 2022.

Poděkování

Děkuji prof. JUDr. Richardu Pomahačovi, CSc. za jeho vstřícnost a ochotu, za podnětné připomínky a odborné rady, jakož i za jeho trpělivost a důvěru, kterou mi při vedení této práce věnoval.

Obsah

Úvod

Předkládaná dizertační práce si klade za cíl pojednat o právní úpravě bezpečnosti informací v kyberprostoru a o kybernetické bezpečnosti. Získání, uchování a následné využití informací bylo pro lidskou společnost vždy zásadní, neboť člověk těžko volí rozumné cesty, nemá-li ke svému rozhodování dostatečné informace. Informace byly důležitým faktorem při spravování věcí soukromých i veřejných a jejich šíření v podobě faktů, názorů a idejí se často stávalo předmětem cenzury a represe ze strany státní moci.

Během posledních dvou dekád informační a komunikační technologie významně transformovaly lidskou společnost. Vedle fyzického světa založeného na hmotné podstatě stvořily prostředí, které je zdánlivě všudypřítomné, prostředí, v němž je lidská komunikace nahrazena kódy, a v němž se hranice jednotlivých států stávají mnohem snáze prostupnými než kdy dříve. Kyberprostor se stal synonymem virtuálního prostředí vzájemně propojených počítačových systémů a sítí, kde je umožněn vznik, výměna i zpracování informací v digitální podobě.

Přístup k informacím a jejich sdílení se ukazuje klíčovým pro globalizované finanční trhy, zabezpečení států na národní i mezinárodní úrovni, zajištění vzdělávání i pro náležitou úroveň zdravotní péče či sociálních služeb. Ačkoli se značná část ekonomické aktivity a práce odehrává na národní, regionální či místní úrovni, klíčové a strategické ekonomické aktivity jsou celosvětově propojeny skrze elektronicky přístupné sítě, díky nimž dochází k výměně kapitálu i nejrůznějších komodit, a vždy také k výměně informací.[1]

Vlivem globalizace, která přináší další technologický pokrok spolu s proměnami kulturních vzorců, a tím i lidského společenství, doznal v průběhu času podstatných změn i obvyklý výskyt informací a přístup k nim. Nebezpečí související se zneužitím informací, s jejich ztrátou či únikem, ovšem přetrvává bez ohledu na zásadní společenský a technologický vývoj. Mezinárodní společenství i jednotlivé státy přistupují k ochraně a zabezpečení informací v kyberprostoru různým způsobem. Přesto lze sledovat určitý trend ve sbližování právních úprav, a to zpravidla vlivem členství v mezinárodních organizacích, či vzhledem k prosté skutečnosti, že využívat výhod globálních počítačových sítí a informačních technologií na poli ekonomiky a bezpečnosti se vyplácí také státům.

Proměny, které v mnoha oblastech světa přinesl technologický pokrok, zapříčinily řadu kulturních a společenských změn. Těžko si lze představit existenci tzv. Arabského jara bez

[1] Podrobněji CASTELLS, Manuel. *The Information Age: Economy, Society and Culture, vol. I, The rise of the network society.* 1. vydání. Malden: Blackwell, 1996, str. 1 - 27.

masového rozšíření počítačových zařízení umožňujících připojení k síti Internet[2] a sdílení nejrůznějšího obsahu. Informační a komunikační technologie znamenají možnost do značné míry neomezené komunikace, o níž se obyvatelům mnoha zemí před několika dekádami nezdálo. Rozmach nových technologií současně přinesl dosud nevídané příležitosti k páchání trestné činnosti[3] a síť Internet, klasické prostředí globální počítačové sítě, umožnila rozvoj kybernetické trestné činnosti.[4] Jejími oběťmi nejsou pouze jednotlivci, ale i průmyslové podniky, politická uskupení, vládní činitelé nebo státní orgány. Kybernetické bezpečnostní incidenty a útoky mohou cílit na kritickou infrastrukturu státu, napadat řídící systémy v klíčových hospodářských odvětvích, jako jsou například energetika, doprava či zdravotnictví, a narušovat fungování informačních systémů veřejné správy. Posloužit mohou též mezinárodně-politickým či teroristickým účelům.

Českou republiku lze zařadit mezi evropské země s nejvyšším rozšířením a využíváním moderních technologií.[5] Zároveň je jednou z prvních zemí, která přijala komplexní právní úpravu kybernetické bezpečnosti.[6] Roku 2014 přijatý zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále též „zákon o kybernetické bezpečnosti" či jen „ZKB"), přinesl novou regulaci reagující na vzrůstající výskyt bezpečnostních incidentů v kybernetickém prostředí a zásadně ovlivnil soukromou i veřejnou sféru. Zákon rovněž otevřel cestu pro uplatňování státní moci v kyberprostoru v souladu s ústavněprávními požadavky.

Cílem disertační práce je prozkoumat problematiku kybernetické bezpečnosti v širších teoretických i praktických souvislostech. Úroveň právní úpravy je determinována stavem vědeckého poznání; zvláště to platí pro oblast kybernetického (virtuálního, myšleného) prostředí, tj. kyberprostoru. Současně by měla právní úprava být do určité míry stálá tím, že obstojí i během

---

[2] „Internet" jako celosvětová informační a komunikační síť je v této práci uveden s velkým počátečním písmenem, naopak výrazem „internet" označuji jakékoli propojené počítačové sítě. Obdobně SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Aleš Čeněk, 2015, str. 52.

[3] Srov. GRABOSKY, Peter. Virtual criminality: Old wine in new bottles? (online). *Social and legal studies*. 2001, (10), str. 243 – 249. Dostupné: http://sls.sagepub.com/content/10/2/243.full.pdf. [cit. 2018-03-15]; WALL, David. *Cybercrime: the transformation of crime in the information age*. 1. vyd. Cambridge: Polity, 2007, str. 44 – 48. K rozvoji trestné činnosti v informační vědě viz ZAVRŠNIK, Aleš. Definiční problémy a kriminologická specifika kyberzločinu. In: GŘIVNA, Tomáš; POLČÁK, Radim (eds.). *Kyberkriminalita a právo*. 1. vyd. Praha: Auditorium, 2008, str. 32 - 33.

[4] Literatura obvykle užívá pojmy počítačová kriminalita, informační kriminalita nebo kybernetická kriminalita. Odborná i laická veřejnost tyto pojmy běžně zaměňují, anebo jimi rozumí různé věci. Shoda ohledně definic nepanuje ani u souvisejících pojmů jako software či počítačový program. Srov. SMEJKAL, Vladimír; SOKOL, Tomáš; VLČEK, Martin. *Počítačové právo*. 1. vyd. Praha: C.H. Beck, 1995, str. 99. SMEJKAL, Vladimír. *Kybernetická kriminalita*. Op. Cit., str. 25-27. Označení trestné činnosti spojené s počítači jako kybernalita se neujalo. Srov. JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. vyd. Praha: Grada, 2007.

[5] NÚKIB. *Národní strategie kybernetické bezpečnosti České republiky na období let 2021 - 2025* (online), str. 18. Dostupné: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/ [Cit. 2022-03-05].

[6] POLČÁK, Radim. *Kybernetická bezpečnost jako aktuální fenomén českého práva** (online). Revue pro právo a technologie, 2015, č. 11, str. 95-149. Dostupné: https://journals.muni.cz/revue/article/view/2980 [Cit. 2022-09-21].

probíhajících technologických změn. S ohledem na závislost společnosti na zabezpečení přenosu i obsahu informací i vzhledem k průniku virtuálního světa do mnoha oblastí lidského života, se informační bezpečnost v kyberprostoru stává prioritou veřejné správy. Lze též říci, že kybernetická bezpečnost sama o sobě je jedním z předpokladů nerušeného výkonu veřejné správy ve všech jejích oblastech.

Právní úprava kybernetické bezpečnosti je ojedinělá ze dvou důvodů. Předně jde o oblast, v níž je právo ovlivněno technickými normami, naukou mezinárodních bezpečnostních vztahů a aktuální politickou a bezpečnostní situací. Pro právníky, kteří technologiím rozumí spíše zřídkakdy, není problematika kybernetické bezpečnosti snadno uchopitelná. Český zákonodárce nadto nemohl v oblasti právní úpravy kybernetické bezpečnosti navázat na žádnou existující právní úpravu ani judikaturu. Jednoznačně se proto jedná o materii, jež si zaslouží pozornost akademické obce.

K uvedenému názoru mne vedla i skutečnost, že o problematice kybernetické bezpečnosti a institutech zákona o kybernetické bezpečnosti pojednává v současnosti nemnoho odborných textů. V tuzemském prostředí sice vycházejí odborné právní články dotýkající se i právní úpravy kybernetické bezpečnosti, bývají však zaměřeny spíše na dílčí oblasti práva informačních a komunikačních technologií.[7] Řízením kybernetické bezpečnosti v informačních systémech se věnuje publikace autorů Doucka, Konečného a Nováka z Fakulty informatiky a statistiky Vysoké školy ekonomické v Praze,[8] zaměřena je však předně na manažerskou obec, přičemž se soustředí zejména na ekonomické aspekty systému řízení bezpečnosti informací v organizacích. Komplexnější pohled nabízí i publikace s názvem „Bezpečnost informačních systémů podle zákona

---

[7] Výjimkou je článek Radima Polčáka z roku 2015: POLČÁK, Radim. *Kybernetická bezpečnost jako aktuální fenomén českého práva** (online). Revue pro právo a technologie, 2015, č. 11, str. 95-149. Dostupné: https://journals.muni.cz/revue/article/view/2980. Z dílčích českých odborných textů lze poukázat například na následující: PORADA, Viktor, RAIS, Karel, SMEJKAL, Vladimír. *Právní, kriminalistické a kybernetické aspekty kybernetické kriminality a bezpečnosti: pocta Vladimíru Smejkalovi*. Brno: Akademické nakladatelství CERM, 2021. KASL, František. *Porušení bezpečnosti osobních údajů v kontextu internetu věcí.* Brno: Masarykova univerzita, 2021. VOSTOUPAL, Jakub. *Certifikace kyberbezpečnostních technologií* (online). Revue pro právo a technologie, 2019, č. 20, str. 147-268. Dostupné: https://journals.muni.cz/revue/article/view/12570. KLODWIG, Jakub. Varování NÚKIB v systematice zákona o kybernetické bezpečnosti a možnosti jeho zohlednění v zadávacím řízení. In: *Revue pro právo a technologie* 23/2021. Dostupné: https://journals.muni.cz/revue/article/view/14590. HARAŠTA, Jakub, MIŠEK, Jakub. IP adresy v kybernetické bezpečnosti. *Revue pro právo a technologie*, 2015, č. 12, s. 21-42. Dostupné: https://journals.muni.cz/revue/article/view/4091/pdf. TÁBOROVÁ, Alice. Veřejnoprávní ochrana informační společnosti a místní působnost práva. *Revue pro právo a technologie: odborný recenzovaný časopis pro technologické obory práva a právní vědy*. Brno: Masarykova univerzita, 2010, 1(1). MAISNER, Martin, VANÍČEK, Zdeněk. *Odpovědnost za obsah přenosu v elektronických komunikacích*. 1. vyd. Praha: Wolters Kluwer Česká republika, 2012. KOLOUCH, Jan. *Cybercrime* (online). Praha: CZ.NIC, 2016. Dostupné: https://knihy.nic.cz/files/edice/cybercrime.pdf. KOLOUCH, Jan, BAŠTA, Pavel a kol. *CyberSecurity* (online). Edice CZ.NIC, 2019. Dostupné: https://knihy.nic.cz/files/edice/cybersecurity.pdf. Všechny odkazy [Cit. 2022-09-21]. DONÁT, Josef, TOMÍŠEK, Jan. *Právo v síti: průvodce právem na internetu*. V Praze: C.H. Beck, 2016.

[8] DOUCEK, Petr, KONEČNÝ, Martin, NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnost informací*. 1. vydání. Praha: Professional Publishing s.r.o., 2019.

o kybernetické bezpečnosti" od autorů Smejkala, Sokola a Kodla.[9] Publikace se obsahově již zaměřuje na právní úpravu, určena je však spíše laické veřejnosti a subjektům, jimž zákon o kybernetické bezpečnosti ukládá povinnosti. Kromě stručnějšího představení tématu kybernetické bezpečnosti zmíněná publikace rozebírá trestněprávní kvalifikace možných útoků na informační systémy a technologie i trestní odpovědnost fyzických a právnických osob, řízení bezpečnosti informací a řízení rizik i různé normy, standardy a metodiky. Věnuje se i zákonu o kybernetické bezpečnosti a vyhlášce č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „vyhláška o kybernetické bezpečnosti"), jejichž jednotlivá ustanovení především dává do souvislostí a podává čtivě srozumitelnějším jazykem. Hlubší analýzu opatření a jiných úkonů podle zákona o kybernetické bezpečnosti však tato publikace nepodává. Obdobně se ustanovením zákona o kybernetické bezpečnosti věnuje i publikace „Cybersecurity" autorů Koloucha, Bašty, Kropáčové a Kunce.[10] Tato publikace o problematice kybernetické bezpečnosti je zaměřena spíše prakticky, určena je širší veřejnosti sestávající z povinných subjektů podle ZKB, hlubší právní analýzu jednotlivých zákonných institutů nepodává. S problematikou seznamuje i monografie Vladimíra Šulce „Kybernetická bezpečnost,"[11] jež se zaobírá zejména způsobem páchání kybernetických útoků a praktickými bezpečnostními opatřeními ohledně možnosti detekce kybernetických útoků a jejich zastavení. Široký pohled na téma nabízí publikace autorského kolektivu z Fakulty podnikatelské Vysokého učení technického v Brně „Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru."[12] Dotýká se historického vývoje problematiky i klíčových pojmů jako jsou kybernetické bezpečnostní incidenty a útoky, internet věcí, umělá inteligence, zálohování, cloud computing, audity atd. Publikace je však svým zaměřením určena pro optimalizaci podnikových procesů a neobsahuje právní rozbor tématu. Podstatná část dalších publikací čtenáře seznamuje s problematikou kybernetické či informační bezpečnosti, případně je orientována spíše prakticky, čímž spadá zaměřením do oboru řízení

[9] SMEJKAL, Vladimír, SOKOL, Tomáš, KODL, Jindřich. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti.* Plzeň: Aleš Čeněk, 2019.

[10] KOLOUCH, Jan, BAŠTA, Pavel a kol. *CyberSecurity* (online). Edice CZ.NIC, 2019. Dostupné: https://knihy.nic.cz/files/edice/cybersecurity.pdf. [Cit. 2022-09-21].

[11] ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o, 2018.

[12] SEDLÁK, Petr, KONEČNÝ, Martin a kol. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021.

bezpečnosti informací.[13] Nejedná se však o právní odbornou literaturu. Řada odborných právních textů a článků pochází především od zahraničních autorů, jak dokládá i citační aparát této práce. Právní úpravě kybernetické bezpečnosti v širších souvislostech se dosud nevěnuje žádná odborná publikace. Porovnáme-li zájem, který je této problematice věnován, s jinými oblastmi veřejného práva, jde o značný nepoměr. Domnívám se proto, že sepsání práce pojednávající o kyberprostoru a informační bezpečnosti, respektive o kybernetické bezpečnosti, by se mohlo stát přínosem pro akademickou obec i pro lepší pochopení problémů legislativního a aplikačního rázu.

Práce je nazvána Kyberprostor a informační bezpečnost. Pojem informace se jeví být v kontextu práce vhodnějším než pojem data. Ačkoli jsou informace ve virtuálním světě představovány právě daty, tj. smyslovými vjemy, které umožňují zpracování informace počítačem, to, co je u dat klíčové pro člověka jako jejich adresáta, je právě jejich informační potenciál. Jistě i z tohoto důvodu se právní úprava zaobírá především informacemi (ochranou a nakládáním s utajovanými a jinak citlivými informacemi, zajištěním přístupu občanů k relevantním informacím pro výkon veřejných subjektivních práv, ochranou informačních systémů klíčových pro fungování veřejné správy, atp.)[14], než daty, která lze chápat spíše v technickém smyslu. Vzájemné vztahy mezi informacemi a daty podrobněji vysvětluji v 1. části disertační práce v podkapitole 1.1.2. Základní pojmy - počítač, data, informace, kyberprostor, Internet.

Právní úprava kybernetické bezpečnosti je veřejnoprávní oblastí práva, která je úzce propojena s dalšími právními i neprávními obory. Kromě norem správního a ústavního práva souvisí především s trestní úpravou; značný význam má i mezinárodní právo veřejné. Mezi další působící faktory patří politické prostředí, zahraniční orientace a působení státu, jakož i technologická vyspělost veřejné a soukromé sféry ve státě.

Z tohoto důvodu se mi jeví účelné přistoupit k problematice komplexně a věnovat se i proměnám společnosti souvisejícími s nástupem nových technologií a globalizačními vlivy, vysvětlit hodnoty a principy informační společnosti, které zásadně ovlivňují podobu práva informačních a komunikačních technologií, a zabývat se i samotným působením práva ve virtuálním prostředí. Řadu otázek a praktických problémů stále působí suverenita států a jurisdikční

---

[13] Např. POLICEJNÍ AKADEMIE ČR. Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech. Praha: Policejní akademie České republiky v Praze, 2020. POLICEJNÍ AKADEMIE ČR. *Bezpečnostní výzvy současného světa.* Praha: Policejní akademie České republiky v Praze, 2020. ČAPEK, Jan, HUB, Miloslav, ROUDNÝ, Radim, KOPÁČKOVÁ, Hana, FUKA, Jan, IBL, Martin. UNIVERZITA PARDUBICE. EKONOMICKO-SPRÁVNÍ FAKULTA. *Vybrané aspekty kybernetické bezpečnosti*. Pardubice: Univerzita Pardubice, 2015. MOC, Michal. *Bezpečné užívání internetu: metodická příručka*. Praha: Centrum pro studium vysokého školství, v.v.i, 2015.

[14] O informacích takto pojednávají např. zákon č. 106/1999 Sb., o svobodném přístupu k informacím, zákon č. 123/1998 Sb., o právu na informace o životním prostředí, zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, či zákon č. 365/2000 Sb., o informačních systémech veřejné správy.

konflikty. Lze si představit situaci, v níž bude cizí stát odmítat součinnost nutnou k výkonu správního aktu či zajištění správního dozoru, popřípadě v níž vyvstanou jurisdikční konflikty mezi dvěma či více státy. Správní právo, jež má umožnit efektivní správu veřejných záležitostí i v podmínkách různých ústavních systémů, by mělo zajistit funkční výkon pravomoci správních orgánů v co nejvyšší míře. Kybernetické operace mohou rovněž zapříčinit vznik mezinárodněprávní odpovědnosti státu. Odpovědný stát je povinen zcela odčinit újmy způsobené poškozenému státu mezinárodně protiprávním činem spáchaným kybernetickými prostředky. Z tohoto důvodu je klíčové i hledisko mezinárodního a evropského práva. Zejména sekundární normotvorba Evropské unie se dotýká regulace kyberprostoru členských států v čím dál tím vyšší míře. Příkladem je problematika bezpečnosti sítí a informačních systémů. Promítá se i do české zákonné úpravy kybernetické bezpečnosti, která přinesla nové instituty a nástroje správního práva. Zvolený komplexní přístup umožní nahlížet na českou právní úpravu kybernetické bezpečnosti v širších souvislostech.

Disertační práce je rozdělena do tří částí:

První část si klade za cíl představit informační společnost a její hodnoty, jakož i související společenské změny, seznámit s vůdčími principy a východisky právní úpravy kybernetické bezpečnosti a s problematickými aspekty působení práva v kyberprostoru. V této části se věnuji proměnám společnosti, které přinesly globalizace, digitální revoluce, a s nimi i nebývalý rozvoj informačních a komunikačních technologií. Uvedenými tématy se zaobírá spíše sociologie nežli právo, avšak pro pochopení problematiky bezpečnosti informací v kyberprostoru i kybernetické bezpečnosti a souvisejících jevů je zapotřebí popsat vliv globálních informačních sítí na českou společnost a veřejnou správu. V důsledku globalizace a vlivem digitální revoluce jsme zahlceni informacemi (obecně daty), což vede ke ztrátě kontroly nad nimi a ke zvýšení rizika jejich zneužití, jež existuje ze strany soukromých subjektů i orgánů státní moci. Dochází rovněž k proměnám v pojetí informace, k proměnám chápání obecného společenského dobra i veřejného zájmu, který je klíčem k určení regulace a kritériem legality činnosti subjektů veřejné správy. V první části též vysvětluji pro problematiku základní pojmy, mezi něž bezesporu patří počítač, data, informace, kyberprostor, či globální veřejně dostupná počítačová síť Internet, a představuji rizikové faktory této sítě z hlediska trestné činnosti, které jsou platné i pro bezpečnost informací v kyberprostoru. Analyzuji právní principy a hodnoty informační společnosti a kybernetické bezpečnosti i jejich vývoj. Kladu si otázky, k jakým proměnám právních principů v této oblasti dochází a jaká je pravděpodobnost jejich udržitelnosti do budoucna. Dále se zabývám legitimitou a vymahatelností práva v kyberprostoru a v souvislosti s tím se věnuji otázkám, do jaké míry lze regulovat

kyberprostor, respektive zda je vůbec zapotřebí právní regulace kyberprostoru, případně jeho celosvětové veřejně přístupné části - počítačové sítě Internet. Jaké skutečnosti hovoří ve prospěch a jaké skutečnosti v neprospěch této regulace, a jakou roli zde mohou hrát veřejná subjektivní práva? Jak regulovat kyberprostor při zachování základních principů globální informační společnosti? Jsou principy a hodnoty, na nichž je informační společnost vystavěna, do budoucna udržitelné? Existuje odpor vůči regulaci kyberprostoru veřejnou mocí? Jaké jsou rozdíly mezi regulací kyberprostoru právní normou a jinými normativními systémy? Závěrem se věnuji rovněž problematickým aspektům působení práva v kyberprostoru, mezi něž patří suverenita státu a výkon jurisdikce.[15]

Druhá část práce se zaměřuje na úlohu státu na zajištění informační bezpečnosti v kyberprostoru. Jsou zde vymezeny pojmy kybernetické bezpečnosti i kybernetické obrany. Pojem kybernetické bezpečnosti je představen též skrze orgány státní správy podílející se na jejím zajišťování a různé právní předpisy a dokumenty, které se problematiky dotýkají. Kromě zákona o kybernetické bezpečnosti mezi ně patří Akt EU o kybernetické bezpečnosti,[16] Nařízení o Evropské síti a centru kompetencí pro kybernetickou bezpečnost,[17] aktuální Národní strategie kybernetické bezpečnosti 2021-2025 i Akční plán k Národní strategii kybernetické bezpečnosti 2021-2025. V části věnované kybernetické obraně se po definování samotného pojmu zabývám pravomocí i kontrolou Vojenského zpravodajství v oblasti kybernetické obrany státu, jehož Národní centrum kybernetických sil bylo do doby přijetí novely zákona č. 289/2005 Sb., o Vojenském zpravodajství, činné bez zákonného podkladu. Kapitola se věnuje též případům veřejnoprávních smluv, kdy soukromý sektor může, do určité míry, přispět k zajišťování kybernetické obrany, neboť k detekci stanovených útoků a hrozeb může Vojenské zpravodajství využít nejen svých vlastních nástrojů, nýbrž i spolupráce s provozovateli veřejných sítí a služeb, kteří mají na základě dohody s Vojenským zpravodajstvím vyhledávat kybernetické útoky a hrozby. Dále je vymezen pojem bezpečnosti informací a dat skrze složky důvěrnosti, integrity (celistvosti) a dostupnosti. Pojednáno je též o bezpečnosti informačních a komunikačních systémů nakládajících s utajovanými informacemi. Vzhledem k různé terminologii je uveden i přehled zákonných definic a termínů

---

[15] Jurisdikce označuje soubor práv a povinností vykonávaných státem skrze jeho orgány v rovině mocenské, v rovině normotvorby a v soudnictví. V užším pojetí představuje jurisdikce místní působnost. Jelikož v rámci kyberprostoru činí problémy především otázky výkonu státní moci vůči určitému území, užívá text pojmu jurisdikce bez dalšího přívlastku ve smyslu užšího pojetí. Podrobněji viz podkapitola 1.4.4.2. Jurisdikční principy.

[16] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA (Agentuře Evropské unie pro kybernetickou bezpečnost) a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií (akt o kybernetické bezpečnosti).

[17] Nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center.

souvisejících s narušením bezpečnosti informací, služeb a sítí, jako jsou kybernetická hrozba, kybernetický incident, kybernetický útok, kybernetická událost, kybernetický konflikt, apod. Text je doplněn rovněž o konkrétní příklady narušení důvěrnosti, celistvosti i dostupnosti informací a dat, včetně kybernetického útoku na průmyslový systém dispečerského řízení dat jaderného zařízení v íránském Natanzu (případ Stuxnet). Dále je uveden přehled právních předpisů a dokumentů z oblasti mezinárodního práva, které mohou být z hlediska českého kyberprostoru zásadní, přičemž jsou stručně rozebrána jejich klíčová ustanovení. Závěrem druhé části je představen pohled mezinárodního práva na kybernetické operace, a to zejména skrze pravidla uvedená v druhé verzi Tallinnského manuálu,[18] vycházející mimo jiné z Návrhu článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování. Jednotlivé podkapitoly rozebírají případy státních i nestátních původců kybernetických operací a útoků, a podmínky, za nichž lze jednání státního orgánu nebo soukromých osob přičíst státu, neboť problematika atribuce, tj. přičitatelnosti kybernetických operací, je z hlediska dovození mezinárodní odpovědnosti státu zásadní. Podán je dále přehled okolností vylučujících protiprávnost kybernetických operací. Text se věnuje rovněž tématu aktivní kybernetické obrany, neboli zpětného hackingu (hack-back), přičemž je podán rozbor argumentů pro i proti jeho použití. Závěrem je stručně rozebrána odpovědnost státu za mezinárodně protiprávní čin v kyberprostoru a přehled způsobů odčinění vzniklé újmy.

Třetí část disertační práce je zaměřena již přímo na český zákon o kybernetické bezpečnosti. Představuje okolnosti a důvody přijetí nové právní úpravy kybernetické bezpečnosti, vztah k evropské sekundární normotvorbě, především směrnici Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (dále jen „směrnice NIS" či „směrnice o kybernetické bezpečnosti sítí a informačních systémů"), a dosavadní vývoj zákona o kybernetické bezpečnosti. Jádrem třetí části práce je pojednání o systému zajištění kybernetické bezpečnosti. Právě zákon o kybernetické bezpečnosti zavedl v oblasti síť opatření, která představují různorodou, a z hlediska odborné literatury opomíjenou oblast správních činností. Text se věnuje rozboru bezpečnostních opatření preventivního charakteru, jakož i rozboru opatření v užším slova smyslu. Za ně lze považovat varování, reaktivní opatření a ochranné opatření. Rozebrána jsou dosud vydaná varování ústředního správního úřadu kybernetické bezpečnosti - Národního úřadu pro kybernetickou a informační bezpečnost (dále též „NÚKIB"), jakož i reaktivní a ochranná opatření vydaná ve formě opatření

[18] SCHMITT, Michael. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* [online]. 2. vydání. Cambridge: Cambridge University Press, 2017. Dostupné: https://www.cambridge.org/core/books/abs/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/law-of-international-responsibility/99E333F8578ADCC567A92BECF932E4C3 [Cit. 2022-11-04].

obecné povahy, spolu s analýzou jejich dopadu v podmínkách ČR. Dále se text věnuje nápravným opatřením, která jsou součástí sankčního systému zákona o kybernetické bezpečnosti. Stručně je pojednáno též o rozhodnutí o uložení povinnosti předat data, provozní údaje a informace, což je institut, jímž NÚKIB může k návrhu oprávněné osoby rovněž reagovat na situaci hrozícího kybernetického bezpečnostního incidentu. S ním souvisí i v zákoně upravená mandatorní migrace dat. Dále jsou představeny týmy reagující na počítačové bezpečnostní incidenty: *Computer Security Incident Response Team*, neboli CSIRT, či *Computer Emergency Response Team*, neboli CERT. Pojednáno je o národním a o vládním CERT týmu. Na příkladu národního CERT týmu je ukázána možnost privatizace veřejné správy v oblasti kybernetické bezpečnosti. V souvislosti s tím text rozebírá i veřejnoprávní smlouvu uzavřenou za účelem provozování národního CERT. V závěru pojednává třetí část o parlamentní kontrole výkonu správy v oblasti kybernetické bezpečnosti. Tou je pověřen zvláštní kontrolní orgán Poslanecké sněmovny Parlamentu České republiky, jímž je Stálá komise pro kontrolu činnosti Národního úřadu pro kybernetickou a informační bezpečnost.

Disertační práce vychází z právního stavu a dostupné literatury a rozhodovací činnosti ke dni 15. 12. 2022.

1. Globální informační sítě, digitální revoluce a proměny společnosti

1.1. Digitální revoluce a informační společnost

1.1.1. Digitální revoluce, globalizace a společenské změny

Někteří shledávají, že lze každou společnost považovat za informační, neboť informace jsou tím, co zajišťuje lidskému společenství přežití a rozvoj.[19] Z tohoto pohledu lze nahlížet i na minulá společenství jako na informační společnosti,[20] avšak právě přisouzení zvláštního významu a důležitosti informacím a využívání informačních a komunikačních technologií za účelem zvýšení informovanosti je tím, co ze společnosti činí společnost informační.[21] Jiní považují společenské změny již za natolik strukturované, jelikož ovlivňují i vzájemné vztahy ve výrobě, při výkonu moci a v lidské zkušenosti obecně, že hovoří o vzniku nové společnosti informačního věku.[22] Lze se však setkat i s poměrně zjednodušujícím přístupem, který informační společnost chápe prostě jako společnost „vzdělanostní", společnost zaměřenou v co nejširší míře na sdělovací média, sdílení a šíření informací.[23]

Podle Castellse žijeme v době, kdy bohatství, moc a kulturní vzorce závisí na technologické vyspělosti společností i jednotlivců, přičemž jádrem této vyspělosti jsou informační technologie; online komunity a sociální sítě zprostředkovávají jednotlivcům zkušenosti mimo fyzický svět a proměňují tak kulturní vzorce a společnost jako takovou.[24]

Právo se zabývalo regulací informací již několik staletí, vezmeme-li v potaz cenzuru a propagandu či ochranu duševního vlastnictví.[25] Obvyklý výskyt informací ovšem doznal v průběhu času podstatných změn. Státy absolutistického typu nesdílely se svými občany informace o vládnutí. Je-li ale vláda státu omezena a založena na důvěře občanů, informační embargo

---

[19] POLČÁK, Radim. *Internet a proměny práva.* 1. vyd. Praha: Auditorium, 2012, str. 275.

[20] BIRKINSHAW, Patrick. *Freedom of information: the law, the practice, and the ideal.* 4th ed. Cambridge University Press, 2010, str. 8. Překlad autorka.

[21] POLČÁK, Radim. *Internet a proměny práva.* Op. cit., str. 275.

[22] CASTELLS, Manuel. *End of Millennium, The Information Age: Economy, Society and Culture, vol. III.* 2. vydání. Chichester: Blackwell Publishers, 2010, str. 376 a násl.

[23] Srov. BEZDÍČEK, Viktor. O zveřejňování nezveřejnitelného: Clintonova aféra a informační společnost. In: BĚLOHRADSKÝ, Václav. *Mezi světy & mezisvěty: reloaded 2013*. 2., opr. a rozšíř. vyd. Praha: Novela bohemica, 2013, str. 177 - 185.

[24] CASTELLS, Manuel. Op. cit., str. 376 an., 385 - 387.

[25] POLČÁK, Radim. Informace a data v právu [online]. *Revue pro právo a technologie,* 2016, č. 13, str. 67-91. Dostupné: https://journals.muni.cz/revue/article/view/4946 [Cit. 2022-10-22].

neobstojí.[26] Jak ovšem někteří upozorňují, přes nesporný společenský i technologický vývoj stále přetrvávají tytéž problémy, a sice užití a zneužití informací.[27] Podle Birkinshawa lze v zásazích státu spatřovat vzrůstající tendence, a to bez ohledu na politickou orientaci jednotlivých vlád.[28] S vyjádřeným postojem lze souhlasit. Odhlédneme-li od existence závazků států přijatých s ohledem na jejich členství v nejrůznějších mezinárodních společenstvích, jejichž vlivem dochází ke sjednocování právních úprav jednotlivých států bez ohledu na aktuální vnitrostátní politické směřování, i státy tradičně liberální využívají výhod globálních počítačových sítí a informačních technologií, a to nejen chtějí-li udržet krok s vyvíjející se ekonomikou, nýbrž i tehdy, hodlají-li zajistit bezpečí svého obyvatelstva.

Jednotlivci i vlády jsou si vědomi významu informací. Míru vlastní informovanosti lze zvyšovat stále širším využíváním moderních informačních a komunikačních technologií. V důsledku toho jsme denně konfrontováni s nepřebernou škálou informací i informačních systémů nejrůznějších typů. ČR patří mezi země v Evropě s nejvyšším rozšířením a využíváním moderních technologií.[29] Varování před zápornými vlivy, v něž se mohou zvrátit přednosti informační společnosti, adresovali veřejnosti v 80. letech v Československu autoři publikace Právo a informace[30] vydané v kolektivu pod vedením právního teoretika Viktora Knappa. Jiří Cejpek v předmluvě této publikace varoval před podstatnou částí negativních dopadů, které si dnes spojujeme s rozmachem informačních a komunikačních technologií i virtuálních světů. Za problematické považoval obezřetné nakládání s osobními údaji člověka tak, aby nedošlo k narušení morálních zásad osobního života a soukromí, jakož i postupné nahrazování nejrůznějších oblastí společenského a osobního života výpočetní technikou. Varoval taktéž před rozvojem uniformity myšlení, podporou nepřímé komunikace a vytrácení mezilidské komunikace jako takové, zároveň zdůraznil nutnost přistupovat ke zvyšujícímu se množství informací kriticky, s důkladným hodnocením jednotlivých myšlenek.[31] S většinou předestřených závěrů lze souhlasit, byť problematika ztráty mezilidské komunikace na úkor nepřímé virtuální komunikace je mnohem

---

[26] BIRKINSHAW, Patrick. Op. cit, str. 18 - 23.

[27] BIRKINSHAW, Patrick. Op. cit., str. 9 - 10.

[28] BIRKINSHAW, Patrick. Op. cit., str. 9 - 10. Birkinshaw provádí svůj rozbor v politickém prostředí Spojeného království Velké Británie a Severního Irska, které podle autora příliš nedbá hodnoty ochrany soukromí. Vzhledem k rychlosti a jednoduchosti sběru a sdílení informací napříč státními hranicemi označuje nakládání s informacemi ze strany státu za jejich zneužívání.

[29] NÚKIB. *Národní strategie kybernetické bezpečnosti České republiky na období let 2021 - 2025* [online], str. 18. Dostupné: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/ [Cit. 2022-03-05].

[30] KNAPP, Viktor a kolektiv. *Právo a informace.* Praha: Academia. 1988.

[31] CEJPEK, Jiří. In: KNAPP, Viktor. a kolektiv. Op. cit., str. 9 - 10.

komplexnější. Klíčovou roli totiž mohou hrát především osobnostní dispozice jednotlivců. Vyslovit lze přitom i názor, podle něhož nepřímá komunikace naopak umožňuje prohloubení a přetrvání mezilidských vztahů tam, kde by to v důsledku vnějších překážek již nebylo možné, čímž naopak mezilidské komunikaci napomáhá. Typickými příklady mohou být značná geografická vzdálenost komunikujících osob či zdravotní omezení ztěžující nejen pohyb, ale i běžnou komunikaci.

Internet, jako volně přístupná počítačová síť celosvětového dosahu, bezesporu sehrál zásadní roli v globalizaci a souvisejících společenských změnách. Někteří označují společenské změny spojené s novými technologiemi a informačními systémy, které efektivně propojují fyzické, virtuální i biologické bytí člověka, za čtvrtou průmyslovou revoluci.[32] Dnešní člověk může významnou část svého života prožít na Internetu - *„uměle vytvořeném hájemství života"*.[33] Závislost společenství lidí na informačních a komunikačních technologiích (dále též „ICT") během posledních desetiletí významně vzrostla.[34] Řada běžných aktivit lidí se již neobejde bez ICT, počínaje mezilidskou komunikací,[35] přes bankovnictví a elektronické obchodování, až po obstarání recepisu nutného k vydání léčiva či zajištění návštěvního termínu na úřadu. Objevuje se myšlenka garantovat každému právo na přístup k Internetu, neboť absence připojení se k určité službě či obsahu může pro jednotlivce znamenat i zásah do základních práv.[36] Rozvoj ICT hrál značnou roli i na poli tzv. nové ekonomiky, pro niž je charakteristická kooperace spojená s vysokou mírou globalizace, přidané hodnoty a významem znalostí.[37] Ekonomické vztahy lze navazovat v kratším časovém horizontu s mnohem různorodějšími partnery z velice odlišného kulturního, náboženského i politického prostředí, v důsledku čehož prožíváme, oproti minulosti, soustavnou interakci s větším

---

[32] SALEM, Fadi. *The Arab World Online 2017: Digital Transformations and Societal Trends in the Age of the 4th Industrial Revolution* [online]. Vol. 3. Dubai: MBR School of Government, 2017, str. 4. Dostupné: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3059445 [Cit. 2022-10-22].

[33] POLČÁK, Radim. *Internet a proměny práva*. Op. cit., str. 72.

[34] ICT REVUE. Závislost na ICT pronikla do všech oborů. Zrychlují práci, ale potírají myšlení a paměť [online]. *Hospodářské noviny,* 25. 2. 2019. Dostupné: https://ictrevue.hn.cz/c3-66493870-0ICT00_d-66493870-zavislost-na-ict-pronikla-do-vsech-oboru-zrychluji-praci-ale-potiraji-mysleni-a-pamet [Cit. 2022-10-22]; či SIMON, Matthew, CHOO, Kim-Kwang Raimond. Digital Forensics: Challenges and Future Research Directions [online]. *Contemporary Trends in Asian Criminal Justice: Paving the Way for the Future*. Seoul: South Korea, Korean Institute of Criminology, April 7, 2014, str. 105 - 146. Dostupné: https://ssrn.com/abstract=2421339 [Cit. 2022-10-22].

[35] O kybernetické komunikaci se zmiňuje již roku 1988 kolektiv autorů kolem Viktora Knappa v publikaci Právo a informace, kde je Cejpkem chápána jako poslední období mezilidské komunikace. Předešlá období řečové a dokumentové komunikace se s kybernetickou komunikací mísí, jelikož postupně vznikající technické prostředky nevytlačují ty dosavadní. KNAPP, Viktor a kol. Op. cit., str. 7.

[36] FIALOVÁ, Eva. Právo na přístup k internetu [online]. *Právní prostor*, 1. 7. 2019. Dostupné: https://www.pravniprostor.cz/clanky/pravo-it/pravo-na-pristup-k-internetu [Cit. 2022-10-22].

[37] KISLINGEROVÁ, Eva. *Nová ekonomika: nové příležitosti?*. V Praze: C.H. Beck, 2011, str. 9.

počtem nejrůznějších lidí.[38] Vzájemné vztahy a interakce jsou mnohem strukturovanější a komplexnější. Elektronická komunikace taktéž rozložila tradiční hierarchie ve společnosti.[39] I veřejná správa díky využití ICT poskytuje občanům širší spektrum základních služeb, ať již jde o oblast sociálního zabezpečení, zdravotnictví, dopravy, komunikace s úřadem, či identifikaci občanů.

Proměny, které v mnoha oblastech světa přineslo šíření ICT, vedly k řadě kulturních a společenských změn. Těžko si lze představit existenci tzv. Arabského jara bez masového rozšíření počítačových zařízení umožňujících připojení se k síti Internet a sdílení nejrůznějšího obsahu i více méně neomezenou komunikaci jejich uživatelů. Průnik ICT mezi široké vrstvy obyvatel zásadně ovlivnil průběh Arabského jara díky snáze dostupným informacím z nejrůznějších zdrojů mimo struktury státu, ale i vlivem rychlosti šíření informací. Jak zdůrazňuje Salem, v okamžiku zveřejnění první webové stránky roku 1992 mnoho lidí v arabském regionu nemělo přístup k Internetu, během poslední dekády však došlo ke značné změně. Bez ohledu na politické a násilné konflikty na Blízkém východě a v severní Africe byla podstatná část obyvatel tohoto regionu téměř neustále připojena k síti Internet, a to především skrze svůj smartphone. Většina (98 %) uživatelů smartphonů používala alespoň jednu komunikační aplikaci typu WhatsApp či Messenger od společnosti Facebook, přičemž 32 % internetových uživatelů preferovalo online obsah v angličtině místo v arabštině.[40]

Rozvoj technologií i způsobů jejich využívání poskytl rovněž nové a nevídané příležitosti k páchání trestné činnosti.[41] Síť Internet jako klasické prostředí globální počítačové sítě podnítila rozvoj kybernetické trestné činnosti.[42] Narozdíl od klasické trestné činnosti, která pouze využívá

---

[38] KISLINGEROVÁ, Eva. Op. cit., str. 3.

[39] BĚLOHRADSKÝ, Vojtěch. Op. cit., str. 7.

[40] SALEM, Fadi. Op. cit., str. 13, str. 21-22.

[41] GRABOSKY, Peter. Virtual criminality: Old wine in new bottles? [online]. *Social and legal studies*. 2001, (10), str. 243 – 249. Dostupné: http://sls.sagepub.com/content/10/2/243.full.pdf. [Cit. 2022-10-23]; WALL, David. *Cybercrime: the transformation of crime in the information age*. 1. vyd. Cambridge: Polity, 2007, str. 44 – 48. K rozvoji trestné činnosti v informační vědě viz ZAVRŠNIK, Aleš. Definiční problémy a kriminologická specifika kyberzločinu. In: GŘIVNA, Tomáš; POLČÁK, Radim (eds.). *Kyberkriminalita a právo*. 1. vyd. Praha: Auditorium, 2008, str. 32 - 33.

[42] V literatuře se obvykle setkáváme s pojmy počítačová kriminalita, informační kriminalita nebo nejaktuálněji kybernetická kriminalita. Odborná i laická veřejnost je běžně zaměňují, užívají synonymně, či si jejich obsah vykládají různě. Jednoznačnou definici nemají ani další pojmy z oblasti, jako software či počítačový program. Srov. SMEJKAL, Vladimír; SOKOL, Tomáš; VLČEK, Martin. *Počítačové právo*. 1. vyd. Praha: C.H. Beck, 1995, str. 99. SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Aleš Čeněk, 2015, str. 25-27. Označení trestné činnosti spojené s počítači jako kybernalita se neujalo. Srov. JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. vyd. Praha: Grada, 2007.

ICT, kybernetická trestná činnost se odehrává již zcela ve virtuální realitě kyberprostoru.[43] Těžištěm útoku se stává kyberprostor tvořený počítačovými sítěmi a jednotlivými prvky těchto sítí, kde spolu komunikují všechna zařízení ovládající protokol TCP/IP.[44] Řada uživatelů Internetu se stává oběťmi trestné činnosti. Kromě jednotlivců cílí pachatelé kybernetických útoků i na průmyslové podniky, politická uskupení, vládní činitele nebo státní orgány.[45] Téměř dvě třetiny všech zaznamenaných kybernetických incidentů v roce 2019 cílily na zdravotní a bankovní sektor, a na digitální infrastrukturu.[46] Útoky mohou posloužit i teroristickým cílům,[47] směřovat vůči státní kritické infrastruktuře, ohrožovat řídící systémy v energetice či dopravě a narušovat tak informační systémy veřejné správy.[48]

1.1.2. Základní pojmy - počítač, data, informace, kyberprostor, Internet[49]

Během posledních dvou dekád došlo díky informačním a komunikačním technologiím k transformaci lidské společnosti. Informačními technologiemi lze chápat využívání počítačových a elektronických zařízení k ukládání a zprostředkování informací. Vlivem rozvoje počítačových sítí, v jejichž rámci spolu komunikují počítačové systémy, došlo k doplnění původního konceptu o prvek

---

[43] K rozlišení trestných činů v informační vědě a kybernetických trestných činů viz PICOTTI, Lorenzo. *Biens juridiques protégés et techniques de formulation des incriminations en droit pénal de l´informatique*. Ramonville Sainte Agne: Révue internationale de droit pénal, 2006, str. 529 – 533.

[44] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Op. cit., str. 15.

[45] Roku 2007 došlo ke kybernetickým útokům na webové stránky estonské vlády a politických stran, médií a finančních institucí, jež je vyřadily dlouhodobě z provozu. Útokům předcházelo odstranění ruského válečného pomníku z Tallinnu. Estonsko tudíž podezřívalo z útoků Ruskou federaci a posílilo obranu svých významných informačních struktur. Nyní sídlí v Tallinnu centrum Severoatlantické aliance (dále jen „NATO") pro kybernetickou bezpečnost, a i díky němu se řadí Estonsko mezi země s výbornou úrovní kybernetické obrany. Srov. NATO. *Cyber defence* [online]. 2018. Dostupné: https://www.nato.int/cps/en/natohq/topics_78170.htm [Cit. 2022-10-23]; NATO. *NATO Summit Guide, Warsaw 2016* [online], str. 128. Dostupné: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160715_1607-warsaw-summit-guide_2016_eng.pdf [Cit. 2022-10-23].; PAVLIKOVÁ, Miroslava. Estonsko-ruský incident v kontextu kyberterorismu [online]. *Global Politics: Časopis pro politiku a mezinárodní vztahy*. 2014. Dostupné: http://www.globalpolitics.cz/clanky/estonsko-rusky-incident-v-kontextu-kyberterorismu [Cit. 2017-03-24].

[46] Nejvíce incidentů zaznamenal zdravotní sektor. Povinnost hlásit kybernetické bezpečnostní incidenty vybraným osobám stanoví směrnice NIS i ZKB. NIS COOPERATION GROUP. *Annual Report NIS Directive Incidents 2019*. CG Publication 03/20, December 2020, str. 2. Dostupné: https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group [Cit. 2022-01-22].

[47] RAMEŠOVÁ, Kristina. Public provocation to commit a terrorist offence: balancing between the liberties and the security [online]. *Masaryk Journal of Law and Technology.* 2020, (14/1), str. 123 - 147. Dostupné: https://journals.muni.cz/mujlt/article/view/11626 [Cit. 2022-10-23].

[48] VLÁDA. Důvodová zpráva k zákonu č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), č. 181/2014 Dz (dále jen „Důvodová zpráva k ZKB"), str. 2.

[49] Text vychází i z rigorózní práce autorky: RADEMACHEROVÁ, Kristina. *Počítačová kriminalita: Vybrané aspekty postihu v mezinárodním prostředí* [online]. Praha, 2017, str. 14 - 21. Dostupné: https://dspace.cuni.cz/handle/20.500.11956/73331 [Cit. 2022-10-22]. Rigorózní práce. Univerzita Karlova, Právnická fakulta, Katedra trestního práva. Vedoucí práce Jelínek, Jiří.

komunikace. Informačními a komunikačními technologiemi, neboli ICT (z anglického *Information and Communication Technologies*) rozumíme *„hardwarové a softwarové prostředky pro sběr, přenos, ukládání, zpracování a distribuci dat“*.[50]

Mezi základní principy informačních a komunikačních sítí patří otevřená architektura, svoboda projevu a neutralita.[51] Tyto principy umožňují přesun značné části lidských aktivit do virtuálního prostředí propojených počítačových sítí. Stírají hranice jednotlivých států i kontinentů, usnadňují šíření informací, přetváří mezilidskou komunikaci a poskytují nové příležitosti k páchání trestné činnosti.[52] Pro pochopení problematiky ICT je zapotřebí objasnit klíčové pojmy, jimiž jsou počítač (počítačové systémy), data a informace, kyberprostor a globální počítačová komunikační síť Internet.

Počítačový systém či počítač lze chápat jednoduše jako *„jakýkoliv stroj, který dokáže tři věci: přijímá strukturovaný vstup, zpracovává jej podle předepsaných pravidel a produkuje výsledky jako výstup“*.[53] Zdaleka tedy již nejde pouze o klasický stolní (popř. ani původní sálový) počítač, nýbrž i o mobilní telefony či různá naprogramovatelná zařízení, která mohou být součástí dopravních prostředků, domácích spotřebičů, elektráren, dronů, bezpečnostních systémů, zbraní atd. Pojem počítačový systém je synonymem k pojmu počítač, jedná se o funkční jednotku tvořenou jedním či více technickými zařízeními s programovým vybavením.[54] Vybavení počítače je fyzického charakteru (hardware) i programové (software). Hardware tvoří technické prostředky,

---

[50] HINDLS, Richard, HOLMAN, Robert, HRONOVÁ, Stanislava. *Ekonomický slovník*. 1. vyd. Praha: Beck, 2003, str. 161.

[51] COHEN-ALMAGOR, Raphael. Cyberterrorism [online]. In: Warf, Barney (eds.) *SAGE Encyclopedia of the Internet.* Thousand Oaks, California, 2018, str. 169. Dostupné: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3192089 [Cit. 2022-10-24].

[52] Počítačová trestná činnost se rozvíjí především v oblasti elektronického obchodování a bezpečnosti informačních systémů a sítí. Srovnávací studie Organizace spojených národů, na níž se podílelo 61 zemí světa, uvádí, že 1⁄3 počítačové trestné činnosti se vztahuje k padělání a různým formám podvodného jednání, 1⁄3 až 1⁄2 ke škodlivému obsahu a zbývajících 10 až 33% představuje hacking, tj. trestnou činnost spojenou s neoprávněným přístupem k počítačovému systému. UNODC. *Comprehensive Study on Cybercrime* [online]. United Nations Office on Drugs and Crime, Draft - February 2013, str. 26. Dostupné: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [Cit. 2022-10-24].

[53] ZOUHAR, Jiří, WOODCOCK, JoAnne. *Slovník výpočetní techniky*. 1. vyd. Praha: Microsoft Press, Plus s.r.o., 1993, str. 81. Zmíněná dnes již historická definice obstojí vzhledem ke své jednoduchosti a obecnosti. Jiná definice pojmem počítač rozumí *„každý programovatelný stroj, který může provést naprogramovaný seznam instrukcí a reagovat na pokyny zadávané z vnějšku, přičemž zpracovává určitá data, zadaná prostřednictvím vstupních zařízení a výsledky prezentuje pomocí výstupních zařízení“*. SMEJKAL, Vladimír. *Kybernetická kriminalita*. Op. cit., str. 22.

[54] SMEJKAL, Vladimír. *Právo informačních a telekomunikačních systémů*. 2. vyd. Praha: C.H. Beck, 2004, str. 63. Jinou definici nabízí např. Úmluva Rady Evropy č. 185 ze dne 23. listopadu 2001 o počítačové kriminalitě (dále jen „Úmluva o počítačové kriminalitě”), podle níž jde o *„jakékoli zařízení nebo skupina propojených nebo přidružených zařízení, z nichž jedno nebo více provádí automatické zpracování dat podle programu“*. Srov. čl. 1 písm. a) Úmluvy o počítačové kriminalitě. Sdělení č. 104/2013 Sb. m. s., Ministerstva zahraničních věcí o sjednání Úmluvy Rady Evropy ze dne 23. listopadu 2001 o počítačové kriminalitě.

především počítače, přídavná, komunikační a rozšiřující zařízení.[55] Software představuje instrukce, díky nimž hardware pracuje.[56]

Data jsou čísla, text, zvuk a jiné smyslové vjemy v podobě způsobilé zpracování počítačem.[57] Podle Úmluvy o počítačové kriminalitě jsou počítačová data *„jakékoli vyjádření faktů, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému, včetně programu způsobilého zapříčinit provedení funkce počítačovým systémem.“*[58] Můžeme se rovněž setkat s pojmem provozní data či metadata, což jsou data udávající informaci o jiných datech,[59] tedy např. údaje o uskutečnění hovoru, o připojení počítače k síti atp. Data mohou být ukládána buď na paměťová média, tzv. nosiče dat, která fungují na základě fyzikálních principů,[60] v operační paměti počítače, či v síťových datových úložištích, včetně tzv. cloud computingu.[61]

Jelikož data mohou vyjadřovat názory, myšlenky a pojmy, a odkazovat na skutečnost, mají potenciál stát se informací. Pojem informace pochází z latinského *informatio*, tedy představy či poučení; jde o způsob a míru uspořádání určitého jevu, který je v daném okamžiku rozpoznatelný příjemcem informace.[62] Data mohou či nemusí mít charakter informace, avšak i jejich absence může být v konkrétním kontextu informací.[63] Podle zakladatele kybernetiky Norberta Wienera je informace veličinou míry uspořádanosti určitého systému, jde tak o opak entropie.[64]

Kybernetika a informatika jsou vývojově i logicky těsně spjaty. Kybernetiku ovlivnil vznik prvních počítačů za 2. světové války. Stala se impulzem pro rozvoj vědy v druhé polovině 20. století. Integrovala v sobě poznatky matematiky, radiotechniky, biologie či neurofyziologie, a

---

[55] HINDLS, Richard; HOLMAN, Robert; HRONOVÁ, Stanislava. *Ekonomický slovník*. Op. cit., str. 135.

[56] ZOUHAR, Jiří, WOODCOCK, JoAnne. *Slovník výpočetní techniky*. Op. cit., str. 346.

[57] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Op. cit., str. 31.

[58] Čl. 1 písm. b) Úmluvy o počítačové kriminalitě.

[59] (NESIG.) *Česká terminologická databáze knihovnictví a informační vědy* [online]. Dostupné z http://aleph22.nkp.cz/F/?func=file&file_name=find-b&local_base=ktd [Cit. 2022-10-23]. Úmluva o počítačové kriminalitě definuje metadata jako *„jakákoli počítačová data vztahující se ke komunikaci prostřednictvím počítačového systému, vytvořená počítačovým systémem, jakožto součástí komunikačního řetězce, uvádějící původ, cíl, cestu, čas, datum, objem nebo trvání komunikace nebo typ příslušné služby.“* Viz čl. 1 písm. d) Úmluvy o počítačové kriminalitě.

[60] Kdysi rozšířené diskety či magnetické pásky fungovaly na magnetickém principu, optickými médii byla CD, DVD či Blue-ray disky, zatímco USB flash paměťová média fungují na elektronickém principu.

[61] Podrobněji SMEJKAL, Vladimír. *Kybernetická kriminalita*. Op. cit., str. 55.

[62] Tamtéž, str. 36.

[63] Tamtéž, str. 38.

[64] POLČÁK, Radim. Autoritativní regulace kyberprostoru a legitimita trestního práva. In: GŘIVNA, Tomáš; POLČÁK, Radim (eds.). *Kyberkriminalita a právo*. 1. vyd. Praha: Auditorium, 2008, str. 13.

podnítila také rozvoj informatiky.[65] Počátky kybernetiky se pojí již s rokem 1948, kdy v USA vyšlo dílo Norberta Wienera *Cybernetics, or Control and Communication in the Animal and Machine* (Kybernetika, čili řízení a komunikace u živočichů a ve stroji).[66] Jak upozorňuje Knapp, Wiener zprvu považoval za předmět kybernetiky řízení a vazby v živých organismech a strojích, později rozšířil její záběr i na systémy sociální.[67] Díky kybernetice proto nevnímáme informace pouze ve spojení s lidským myšlením, ale mohly se stát i předpokladem pro komunikaci strojů.

Kyberprostorem lze rozumět virtuální (myšlené) prostředí vzájemně propojených počítačových systémů a jejich sítí. Lze se však setkat i s názorem, podle kterého je chybou vnímat kyberprostor skrze různé metafory. Metafory kyberprostoru údajně mají vést k nebezpečným myšlenkám o alternativní sféře, v níž neplatí dosud známá pravidla ani principy, natož právní řád; podle zmíněného přístupu je kyberprostor pouze specifickým druhem komunikační sítě umožňující spojení lidí a informací.[68] Daný přístup však ztotožňuje kyberprostor pouze s komunikační sítí Internet. Současně přitom přehlíží specifické vlastnosti Internetu, jež zásadně ovlivňují aplikaci právních norem. Jiní označují kyberprostor *„virtuálním prostředím, v němž se ekonomická hodnota pojí k myšlenkám a jejich virtuálnímu vyjádření, spíše než k fyzickému majetku."*[69] ZKB definuje kybernetický prostor jako *„digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací".*[70] Z uvedených definic je patrné, že klíčovými prvky kyberprostoru jsou virtualita, informace, jakož i schopnost vzájemného propojení a výměny myšlenek.

V kyberprostoru se nachází, shodně jako ve fyzickém světě, nejrůznější objekty. K jejich efektivnímu využívání však stačí stlačení příslušných kláves na počítači nebo pohyb a klik

---

[65] Mezi teoretické základy kybernetiky patří mechanizace početních úkonů, automatizace, programování a algoritmizování. Významnou úlohu hrálo poznání německého filozofa G. W. Leibnitze. Kybernetika se zabývá studiem chování organizovaných otevřených systémů technických, biologických a sociálních - složitých dynamických systémů. Zaměřuje se na jejich řízení, které chápe jako informační proces. Podrobněji KNAPP, Viktor a kol. Op. cit., str. 14 - 15.

[66] WIENER, Norbert. *Cybernetics, or Control and Communication in the Animal and Machine.* New York: The Technology Press, 1950.

[67] KNAPP, Viktor a kol. Op. cit., str. 15.

[68] GRAHAM, Mark. There are No Rights 'in' Cyberspace [online]. *Research Handbook on Human Rights and Digital Technology.* Elgar, January 2019. Dostupné: https://ssrn.com/abstract=3323660 [Cit. 2022-10-23].

[69] BARLOW, John Perry. The economy of ideas: a framework for rethinking patents and copyrights in the digital age (Everything you know about intellectual property is wrong). *Wired*, 1994, 2(3), str. 84. Citováno dle WALL, David. Op. cit., str. 32.

[70] § 2 písm. a) ZKB.

počítačovou myší.[71] Předpona *kyber*[72] odkazuje na řízení a kontrolu elektronických dat, což umožňuje manipulaci s nimi, *prostor* značí *„virtuální místo, kde dochází k interakci dvou či více lidských aktivit"*.[73] Pojmu poprvé užil Barlow v roce 1990 jako *„v daném čase aktuální nexus mezi počítačem a telekomunikačními sítěmi."*[74] Jako virtuální prostředí kyberprostor umožňuje řadu aktivit bez překážek fyzického světa. Součástí kyberprostoru je Internet jako celek a veškerá globální média i komunikační kanály; pojem kyberprostoru je širší než pojem Internet, neboť zahrnuje i všechna zařízení kontrolovaná počítačovým programem, byť by nebyla propojená se sítí Internet.

Spojení a sdílení informací, respektive dat mezi počítači, a tím i mezi jejich uživateli, zajišťují počítačové sítě, jež jsou tvořeny technickými i programovými prostředky.[75] Jednou z počítačových sítí je i Internet. Všeobecně přijímaná právní definice Internetu neexistuje,[76] a ani český právní řád není výjimkou. Běžně je však Internet chápán jako celosvětová komunikační a informační síť. V řadě právních předpisů je namísto pojmu Internet užíván termín veřejně přístupná počítačová síť[77] nebo veřejná informační síť.[78] S ohledem na živelnost internetového prostředí a rychlý vývoj informačních a komunikačních technologií však není zapotřebí vnímat absenci jeho definice negativně. Podle Smejkala se Internet skládá z různých subjektů práva, a sice z *„lidí a organizovaných sdružení lidí (právnických osob) včetně státu, a dále z majetku, tj. věcí a práv."*[79] Smejkal poukazuje rovněž na problematickou absenci určité institucionalizace Internetu, když *„na rozdíl od automatizovaných informačních systémů netvoří technické a programové prvky a lidé s*

---

[71] AWAN, Imran, BLAKEMORE, Brian (eds.). *Policing cyber hate, cyber threats and cyber terrorism*. 1. vyd. Farnham: Ashgate, 2012, str. 5.

[72] Předpona *kyber* je odvozena z řeckého termínu *kybernetes*, v českém jazyce jde o výrazy kormidelník, vladař či pilot. ZAVRŠNIK, Aleš. Op. cit., str. 34.

[73] AWAN, Imran, BLAKEMORE, Brian (eds.). Op. cit., str. 5. Překlad autorka.

[74] BARLOW, John Perry. Crime and Puzzlement: in advance of the law on the electronic frontier. *Whole Earth Review.* Sausalito: New Whole Earth, 1990, (68), str. 44 – 57. Překlad autorka.

[75] Podrobněji k počítačovým sítím a přenosu dat v jejich rámci viz SMEJKAL, Vladimír. *Kybernetická kriminalita.* Op. cit., str. 45 - 52.

[76] Internet jako věc v právním slova smyslu neexistuje, neboť si jej nelze přivlastnit či jej ovládat, byť slouží potřebám lidí. Srov. § 489 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

[77] Srov. výkladové ustanovení § 117 písm. a) zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů (dále jen „trestní zákoník"), jež vyvozuje ze spáchání konkrétního trestného činu veřejně přístupnou počítačovou sítí vyšší míru společenské závažnosti takového činu. Z hlediska trestněprávní nauky značí veřejně přístupná počítačová síť *„funkční propojení počítačů do sítí s cílem vytvořit informační systém pracující s tzv. dálkovým přístupem, jakým je především internet a jiné podobné informační systémy."* Viz ŠÁMAL, Pavel. *Trestní zákoník: komentář*. Sv. 1, § 1 – 139. [Obecná část]. 2. vyd. V Praze: C.H. Beck, 2012, str. 1300.

[78] Viz § 2 písm. h) zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, (dále též „ZEK"), který se pokouší o vymezení internetové sítě.

[79] SMEJKAL, Vladimír. *Internet a §§§*. 1. vyd. Praha: Grada, 2001, str. 17 - 18.

nimi pracující určitou společenskou celistvost, tj. instituci, která může být subjektem práva."[80] S tím se nutně pojí ztížená kontrola internetového prostředí a horší vymahatelnost práva. Počet uživatelů Internetu se přitom každým rokem zvyšuje o 10 %, v roce 2019 přesáhl 4 miliardy lidí.[81]

Internet jako celosvětová informační a komunikační síť měl svojí architekturou v době vzniku chránit před vnějšími zásahy a cenzurou. Vyvinul se ze sítě ARPANET (*the Advanced Research Projects Agency Network*). ARPANET, který byl sponzorován armádou USA, spojoval koncem 60. let 20. století výzkumná univerzitní pracoviště a komunity s vládními agenturami. Jeho cílem byla bezpečná a vůči vnějším zásahům odolná vojenská komunikace.[82] Na počátku představovali uživatelé především odborníky, kteří se řídili specifickými pravidly sítě, včetně určitého morálního kódu, přičemž řada z nich se znala i osobně. S postupným rozšiřováním sítě Internet[83] a celosvětovým nárůstem jeho uživatelů však brzy začalo docházet i ke společensky neakceptovatelnému chování. V současnosti využívají Internet jednotlivci, soukromé i veřejné organizace, státy i mezinárodní společenství. Vyvstávají otázky, co je ještě akceptovatelné chování, jaké porušení specifických pravidel sítě by mělo být regulováno v rámci internetové komunity a kdy by měl zasáhnout stát jako garant ochrany práv a svobod ve virtuálním prostředí. Na uvedené problematické otázky lze nahlížet jak z pohledu jednotlivců porušujících normy, tak v situaci, kdy stojí za porušením norem stát.

Ač je Internet běžně považován za informační síť, nelze jej automaticky ztotožňovat s informačním prostředím. Polčák například zdůrazňuje, že Internet není perfektně organizován a je zahlcen nejen nadbytečnými, ale i nesprávnými daty - srovnává jej proto s prostředím entropickým.[84] Zda lze považovat konkrétní data za informaci či nikoli je však subjektivní. Skutečnost, zda budeme konkrétní data či jejich absenci považovat za informaci, totiž často závisí na dalších informacích, jimiž adresát disponuje. Teprve se znalostí určité věci pro nás mohou mít konkrétní data využití v podobě informace, zatímco pro předem neinformovaného uživatele

---

[80] Tamtéž.

[81] INTERNATIONAL TELECOMMUNICATION UNION. Internet usage keeps growing, but barriers lie ahead. [online]. *Facts and figures 2019: Measuring digital development*. Dostupné: https://itu.foleon.com/itu/measuring-digital-development/internet-use/ [Cit. 2022-10-24].

[82] Podrobněji viz Yar: *„Díky technologii probíhala komunikace skrze tzv. pakety, menší části mířící různými cestami k adresátovi, kde byly složeny do původní podoby. Variabilita možných cest zajišťuje větší odolnost sítě."* YAR, Majid. *Cybercrime and society: crime and punishment in the information age*. 2. vyd. Thousand Oaks, CA: SAGE Publications, 2013, str. 7. Překlad autorka.

[83] Československo bylo připojeno k síti Internet dne 13. 2. 1992 jako v pořadí 39. země na světě. VÁCLAVÍK, Lukáš. Před 25 lety se Československo připojilo k Internetu. Připomeňme si hlavní milníky [online]. *cnews.cz* Dostupné: https://www.cnews.cz/pred-25-lety-se-ceskoslovensko-pripojilo-k-internetu-pripomente-si-hlavni-milniky/ [Cit. 2022-10-23].

[84] POLČÁK, Radim. Autoritativní regulace kyberprostoru a legitimita trestního práva. Op. cit., str. 14.

zůstanou data i nadále nevyužitelnými. Internet proto lze považovat za prostředí, které má informační potenciál. Více než 95 % veškerých informací na světě je digitalizovaných a většina z nich je přístupná skrze počítačové sítě.[85] V roce 2007 bylo možné uložit přibližně 300 exabajtů[86] optimálně komprimovaných informací na úložištích - tedy zhruba 80krát více informací na osobu než tomu bylo v Alexandrijské knihovně okolo roku 300.[87] Možnosti ukládání informací na úložištích a jejich vybavení ve virtuálním prostředí tak dalece přesahují tradiční způsoby jejich schraňovaní v minulosti.

1.1.3. Rizikové faktory sítě Internet[88]

Mnozí autoři poukazují na rizikové vlastnosti Internetu, díky nimž dochází v prostředí globální komunikační sítě k výskytu nežádoucích jevů.[89] Tyto faktory lze rozčlenit do následujících oblastí:

1.1.3.1. Globální dosah

Internet jako volně přístupná počítačová síť není omezen hranicemi jednotlivých států, což vede k téměř neomezenému okruhu uživatelů, obtížné kontrole šíření dat po síti, jurisdikčním konfliktům i obtížné vymahatelnosti právních norem. Suverenita státu je tradičně spojována s určitým územím a souvisí s územní působností norem (princip teritoriality) a jejich vymahatelností v daném místě a čase. Ve virtuálním prostředí propojených počítačových sítí toto tradiční pojetí

---

[85] HILBERT, Martin., LÓPEZ Priscila. The World's Technological Capacity to Store, Communicate, and Compute Information [online]. *Science* 332, no. 6025 (April 1, 2011), str. 60–65. Dostupné: https://www.science.org/doi/10.1126/science.1200970 [Cit. 2022-10-24].

[86] Exabajt je jednotka kapacity paměťového média. 1 exabajt odpovídá bilionu gigabajtů či trilionu megabajtů. Wikipédia : slobodná encyklopédia [online]. St. Petersburg (Florida) : Wikimedia Foundation, 2001- . Slovenská verze. Dostupné: https://sk.wikipedia.org/wiki/Exabajt [Cit. 2022-10-24].

[87] HILBERT, Martin. The World's Technological Capacity to Store, Communicate, and Compute Information [online]. Dostupné: https://www.martinhilbert.net/worldinfocapacity-html/ [2021-11-30].

[88] Text vychází i z diplomové práce autorky: RADEMACHEROVÁ, Kristina. *Právní rámec vyšetřování počítačové kriminality* [online]. Praha, 2016, str. 14 - 17. Dostupné: https://dspace.cuni.cz/handle/20.500.11956/81814 [Cit. 2022-10-22]. Diplomová práce. Karlova univerzita, Právnická fakulta, Katedra trestního práva. Vedoucí práce Tomáš Gřivna.

[89] Např. KOOPS, Bert-Jaap. The Internet and its Opportunities for Cybercrime: Tilburg Law School Research Paper No. 09/2011 [online]. *Transnational Criminology Manual*. Nijmegen: WLP, 2010, (1). Dostupné: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1738223. [Cit. 2022-10-24]. POLČÁK, Radim. *Internet a proměny práva*. Op. cit., str. 93 - 94. K problematice civilní odpovědnosti srov. HUSOVEC, Martin. *Zodpovednosť na internete* [online]. Edice CZ.NIC, 2014. Dostupné: https://knihy.nic.cz/files/edice/zodpovednost_na_internete.pdf [Cit. 2022-10-24]. Ke kriminologickému úhlu pohledu srov. WALL, David. Op. cit., str. 30 – 51. GRABOSKY, Peter. Op. cit., str. 243 – 249. DELUCA, Christopher D. The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors [online]. *Pace International Law Review Online Companion.* 2013, Vol. 3, Issue 9, str. 315. Dostupné: https://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1033&context=pilronline [Cit. 2022-10-24].

vede k problematickému vymáhání vnitrostátních právních norem s ohledem na nedosažitelná úložiště informací, takřka neomezené možnosti šíření informací skrze počítačové sítě přes hranice jednotlivých států, či anonymitě uživatelů sítě. Internet ztížil snahy podnikatelů, veřejných institucí i vlád jednotlivých států omezit či kontrolovat výskyt a šíření pro ně nežádoucích informací, neboť *„neomezené množství informací může být zpřístupněno na rozličných počítačových zařízeních a z mnoha různých pramenů.”*[90]

1.1.3.2. Decentralizovaná architektura, anonymita

Internet je ve své podstatě *„systém předem daných informačních protokolů, které umožňují vzájemnou komunikaci jednotlivých osobních počítačů skrze sítě. Jde o úspěšný model, jak propojit počítačové technologie s komunikačními technologiemi ve výsledný uživatelsky atraktivní produkt.”*[91] Síť Internet byla vytvořena jako decentralizovaná a flexibilní pro snazší odolnost vůči zásahům zvenčí. Tytéž vlastnosti sítě znemožňují její efektivní kontrolu a podstatně ztěžují i různé snahy o cenzuru. Kdokoli se může relativně anonymně připojit k síti. Právě anonymita umožňuje existenci černých trhů s nejrůznějšími komoditami od autorských děl a vědeckých publikací, přes nejrůznější užitečný i škodlivý software, až k pornografii, drogám či zbraním. Ceněnými komoditami jsou rovněž citlivá data v podobě osobních údajů, přístupových informací a hesel, bankovních čísel i IP adres počítačů infikovaných malwarem (škodlivým počítačovým programem).[92] Anonymní prostředí zbavuje řadu uživatelů sociálních bariér, které by jim mimo virtuální svět bránily následovat určitý model chování. Virtuální identita může mnohým z nich poskytnout útočiště před pravidly reálného světa a zbavit je strachu z odhalení nelegální nebo morálně pochybné činnosti.[93]

---

[90] WALL, David. Op. cit., str. 14. Překlad autorka.

[91] WALL, David. Op. cit., str. 35. Překlad autorka.

[92] Návštěvníci černých trhů mohou krýt svoji identitu skrze síť TOR (The Onion Router). Srov. TOR. Hidden Service Protocol [online]. Dostupné: https://support.torproject.org [Cit. 2022-10-24].

[93] V prostředí počítačových sítí zpravidla chybí prvek sociální kontroly, který je podle kriminologické teorie rutinních aktivit jeden z rozhodujících elementů, které brání páchání trestné činnosti. Srov. GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana. *Kriminologie*. 4. aktualizované vydání Praha: Wolters Kluwer, 2014, str. 69.

1.1.3.3. Informační hodnota, snadná manipulace s daty, automatizace

Podstatou Internetu zůstává zprostředkování informací. Letitý pojem *„information brokering"*, označuje proces sběru a šíření, či přerozdělení informací.[94] Internet jej výrazně usnadňuje, neboť umožňuje snáze získat přístup ke konkrétním datům s cílem vytěžit z nich požadované informace. Většina internetových uživatelů například platí za určitou on-line službu tím, že s jejím poskytovatelem sdílí data o sobě samých, byť je služba na první pohled zdánlivě poskytována zdarma.

Získá-li určitý subjekt přístup k většímu množství informací, může z nich vytěžit další informace a znásobit tak hodnotu původních dat. Jde o koncept tzv. *big data*, termín, jenž označuje *„velké objemy strukturovaných, semi-strukturovaných nebo nestrukturovaných a zároveň personalizovaných, pseudonymizovaných nebo anonymizovaných dat, která jsou shromážděna v databázi a umožňují tzv. data mining."*[95] Termín *data mining*, tedy doslovně „těžbou dat", je *„filtrování nebo kombinování dat za účelem identifikace vzorců chování a vztahových řetězců mezi jednotlivými daty."*[96] K analýze dat však s ohledem na jejich velikost a složitost nestačí tradiční nástroje k jejich zpracování. Vzrůstají proto nároky na zpracování, přenos, ukládání i shromažďování dat. Řada analytických programů umožňuje z dat vytěžit cenné informace, které lze využít v různých oblastech (marketing, pojišťovnictví, zdravotnictví apod.). Jejich význam je však založen na predikci, kterou provádí počítačový program (analytický software). V souvislosti s tím vyvstává problém chybných korelací, ale i nízké míry autenticity výchozích dat.

S nárůstem množství dat na úložištích v cloudových technologiích se pojí i problematická ochrana dat a jejich úniky. Podle studie Dell Technologies Global Data Protection Index z roku 2021 spravují firmy desetinásobný objem dat oproti době před pěti lety. Třetina celosvětově dotazovaných subjektů z oblasti soukromého i veřejného sektoru zaznamenala za poslední rok kybernetický útok, který zablokoval přístup k firemním systémům či datům. Vedle nárůstu objemu spravovaných dat jsou z hlediska jejich ochrany považovány za rizikové faktory i nárůst počtu

---

[94] Podrobněji BRESSAN, Stephane, LEE, Thomas. *Information Brokering On The World Wide Web* [online]. Cambridge, MA: The Sloan School of Management Massachusetts Institute of Technology, 1997. Dostupné: http://dspace.mit.edu/bitstream/handle/1721.1/2663/SWP-3963-37617980-CISL-9708.pdf;sequence=1 [Cit. 2022-10-24].

[95] KASL, František. Internet věcí a ochrana dat v evropském kontextu [online]. *Revue pro právo a technologie.* 2016, č. 13, str. 116. Dostupné: https://journals.muni.cz/revue/article/view/5422 [Cit. 2022-10-24]. Pojem anonymizovaný údaj autor vysvětluje jako *„osobní údaj, který byl nenávratně změněn tak, že subjekt údajů není možné nadále identifikovat ani nepřímo, a to jak správcem osobních údajů samotným, tak i ve spolupráci s někým jiným",* pseudonymizace pak představuje *„formu zabezpečení osobních údajů vedoucí ke snížení rizika jejich ohrožení za současného uchování vlastností těchto údajů, čímž je na rozdíl od anonymizace umožněno jejich další efektivní využití";* alternativou pseudonymizace je šifrování dat. Tamtéž, str. 124 - 127.

[96] Tamtéž, str. 116.

zaměstnanců pracujících z domova a vzestup využívání cloudových technologií bez toho, že by společnost využívala specifické ochrany dat.[97]

Rovněž možnost snadné manipulace s daty bez podstatných nákladů se ukazuje problematickou, neboť data lze kopírovat a přisvojit si tak jejich hodnotu, tj. využít informací v nich obsažených, aniž by vlastníku dat bylo znemožněno s nimi dále manipulovat.[98] Data lze také pozměnit a šířit v nové podobě jako autentická, aniž by bylo jakkoli zřejmé, že došlo k jejich změně.

Ve vztahu k trestné činnosti páchané na Internetu poukazuje Wall rovněž na možnost automatizace, tedy na využití propojených počítačů a jejich systémů k „automatizovanému" páchání trestné činnosti.[99]

1.1.3.4. Rychlý koloběh inovace

Časový rámec, v němž dochází k vývoji nových on-line funkcí a služeb i metod páchání trestné činnosti, je kratší než mimo globální počítačovou síť. Někteří dokonce zdůrazňují rychlost inovací tvrzením, že jeden internetový rok odpovídá přibližně třem měsícům reálného času.[100] Právě podstata propojených počítačových sítí, tj. výměna a sdílení informací, názorů, myšlenek, postupů i návodů, jakož i jejich celosvětový dosah a využití v rámci mezinárodního i vnitrostátního obchodování, podporuje inovaci. Objevují se nové komunikační kanály a služby (např. mobilní aplikace či chatboxy uvnitř virtuálních herních světů či webových stránek). Současně však existuje riziko vyloučení osob, které nemají přístup k informacím a inovativním technologiím, ať již z důvodu absence internetového připojení či vhodného zařízení, anebo pro nedostatek svých znalostí umožňujících informaci nalézt, přečíst a porozumět jí.

S rychlým kolobě hem inovace souvisí i koncept Internetu věcí (známý též pod anglickou zkratkou *IoT*, neboli *Internet of Things*). Jde o často zmiňovaný pojem související s nejmodernějšími technologickými trendy a pokrokem ve všech oblastech elektroniky, díky němuž je možné (a komerčně dostupné) instalovat komunikační moduly do předmětů každodenní potřeby.

---

[97] DELL TECHNOLOGIES. *Global Data Protection Index 2021: Key Findings - July 2021* [online], str. 30 - 31. Dostupné: https://www.delltechnologies.com/en-us/data-protection/gdpi/index.htm#pdf-overlay=//www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/global-data-protection-index-key-findings.pdf [Cit. 2021-11-12].

[98] Něco jiného je kybernetický útok typu ransomware, který znemožní oprávněnému uživateli manipulovat s daty, dokud nebude zaplaceno „výkupné". Podrobněji k útoku typu ransomware srov. KOLOUCH, Jan. Op. cit., str. 221-231.

[99] WALL, David. Op. cit., str. 43.

[100] MOORE, Gordon E. Cramming more components onto integrated circuits. *Electronics*, 1965 (38/8), str. 114-117. Citováno dle WALL, David. Op. cit., str. 3.

Tato tzv. „chytrá zařízení" jsou následně schopná komunikovat a zpracovávat dodatečné informace, díky čemuž mohou nabízet nové funkce.[101] Každý předmět tak může být připojen k Internetu a sdílet data, čímž se zvyšuje jeho hodnota a využitelnost.[102]

1.1.3.5. Konflikt mezi soukromou a veřejnou správou

Rozlišení veřejné správy od soukromé lze provést s odkazem na soukromou či veřejnou povahu cílů či zájmů sledovaných danou činností, případně rozlišením činnosti vrchnostenské povahy u veřejné správy, od spíše hospodářských aktivit a manažerské činnosti u soukromé správy.[103] Odlišit veřejnou či soukromou povahu činností ovšem nemusí být v prostředí Internetu zcela jednoznačné. Uživatelé počítačových sítí mohou být soukromé osoby, podnikatelské subjekty, zpravodajské služby, orgány státní správy, apod. Jejich zájmy se mohou lišit i překrývat. Soukromým zájmem podnikatele může být získání co největšího souboru dat o uživatelích webové stránky za marketingovými účely, tj. s cílem dosažení finančního zisku. Stejný zájem získat co největší soubor uživatelských dat může mít i stát, avšak jeho cílem může být dosažení lepšího zabezpečení sítě.

Soukromé subjekty obvykle požadují ve virtuálním prostředí co nejvyšší míru svobody za současného zajištění bezpečí pro své transakce i vysokého stupně ochrany osobních údajů a soukromí. Stát by měl zaručit ochranu práv a zájmů v prostředí sítě Internet i mimo ni. V oblasti kybernetické bezpečnosti a ochrany před podvodným jednáním však soukromý sektor často spoléhá více na své možnosti a způsoby prevence a nápravy než na státem garantované prostředky ochrany. Značná část obětí bezpečnostních incidentů se s nimi vypořádá raději svépomocí, nežli by se obrátila na policejní orgány a umožnila zjistit zranitelnost vlastního zabezpečení.[104] Veřejný zájem (státu) na náležitém vyšetření kybernetické trestné činnosti a odhalení a potrestání jejích pachatelů tak může být ohrožen snahou neohrozit postavení oběti v rámci konkurenčního prostředí soukromé sféry.

Další problematickou oblastí může být využívání objemného souboru dat k automatickým predikcím nežádoucího chování. Řadu otázek vzbuzuje využívání automatizovaných procesů při

---

[101] KASL, František. Internet věcí a ochrana dat v evropském kontextu [online]. Op. cit., str. 112.

[102] ROPERT, Samuel. *Internet of things: Outlook for the top 8 vertical markets* [online]. IDATE DigiWorld, 7 April 2016. Dostupné: https://en.idate.org/internet-of-things-2/ [Cit. 2022-10-25].

[103] HENDRYCH, Dušan. Oddíl 1. Pojem veřejné správy. In: HENDRYCH, Dušan a kol. *Správní právo. Obecná část.* 9. vydání. Praha: C. H. Beck, 2016, s. 2, marg. č. 3.

[104] Srov. též WALL, David. Op. cit., str. 25 - 26.

předvídání a odhalování protiprávní činnosti nebo nebezpečného chování osob, které by mohlo ohrozit bezpečnost státu. Zarsky zmiňuje využití automatizovaných analýz (tzv. *predictive modeling*) ve dvou oblastech, a to v daňovém řízení ve vztahu k odhalení poplatníků podvodně si nárokujících vratku na dani, a v oblasti zabezpečení státu. Automatizovaný počítačový systém vybere z objemného souboru dat (např. z podaných daňových formulářů, z údajů o letištních pasažérech, z osobních údajů jednotlivců v policejních databázích, atp.) na základě předem zadaných kritérií osoby, jež nesou vyšší riziko podání neoprávněné žádosti o vratku na dani, či pro bezpečnost státu. Takto automaticky vybrané osoby jsou následně podrobeny bližší kontrole ze strany správního orgánu, která je provedena již „manuálně", tj. lidmi, nikoli počítači.[105] Využívání automatizovaných prediktivních analýz ze strany veřejné moci ovšem může kolidovat s principy zákonnosti, předvídatelnosti a transparentnosti veřejné správy, jakož i s požadavkem minimálního zásahu do základních lidských práv a svobod. U automatizovaných analýz je rozhodujícím zadání klíčových kritérií, na jejichž základě teprve má být provedena manuální analýza potenciálně škodlivé činnosti. Uvedený proces by proto měl být proveden na základě zákona, s transparentním určením jednotlivých kritérií.

1.1.4. Vliv globálních informačních sítí na pojetí informace

Cejpek na konci 80. let 20. století spatřoval v kybernetické komunikaci, jež měla následovat po tzv. řečové a dokumentové komunikaci, poslední fázi vývoje lidského způsobu dorozumívání.[106] Množství informací, k nimž má člověk přístup, v kybernetické fázi lidské komunikace rychle roste. Lidské společenství si je vědomo významu informací. Za účelem zvýšení míry informovanosti využíváme v čím dál tím vyšší míře informačních a komunikačních technologií, v důsledku čehož jsme denně konfrontováni se značným množstvím informací a informačních systémů. Téměř neomezená dosažitelnost dat, a z nich plynoucích informací, jakož i jejich rostoucí množství, klade vyšší nároky na zpracování, třídění a kritické hodnocení informací. S ohledem na vlastní značný objem jsou data čím dál tím častěji zpracovávána i analyzována skrze technologie, respektive k tomu navrženými a určenými počítačovými programy díky automatizovaným procesům. Člověk do uvedeného procesu zasahuje méně a ztrácí tak možnost ovlivnit dílčí výsledky, a tím i podobu konečného rozhodnutí. Příkladem mohou být různé internetové vyhledávače, které na základě předchozího chování uživatele na Internetu nabízí konkrétní výsledek vyhledávání. Řada prohlížečů

---

[105] ZARSKY, Tal. Z. Transparent Predictions [online]. *University of Illinois Law Review*. Sv. 2013, č. 4, str. 1511 - 1515. Dostupné: https://ssrn.com/abstract=2324240 [Cit. 2022-10-25].

[106] KNAPP, Viktor a kol. Op. cit., str. 7 - 10.

však nezveřejňuje algoritmus ani další kritéria, podle kterých dochází k výběru a zobrazení výsledků vyhledávání, což ztěžuje i kontrolu legitimního zásahu do svobody vyhledávat, přijímat a rozšiřovat informace.[107] Způsob našeho počínání na Internetu po nás zanechává určitou stopu - metadata, která mohou představovat i údaje osobní povahy.[108] Tzv. databáze záměrů obsahuje cenná data pro obchodníky i pro státní orgány. Pro podnikatele je zásadní být vidět i ve virtuálním prostředí. Za účelem dosažení zisku musí být jejich zboží a služby na Internetu co nejsnáze k nalezení, neboť běžný uživatel nemá čas dlouze hledat nejvýhodnější produkty a porovnávat často nepřeberné množství nabídek. Vyhledávač zaznamenává dotazy uživatele pod jeho IP adresou, unikátní číselnou řadou, která byla uživateli určena poskytovatelem internetového připojení. Tene přirovnává IP adresu k adresám a telefonním číslům offline světa, a považuje ji za osobní údaj; objevuje se však i názor, že IP adresa není osobní údaj, protože určuje nikoli konkrétního člověka, nýbrž počítač, z něhož byl zadán požadavek k vyhledání.[109]

Velké soubory dat o jednotlivcích jsou k dispozici soukromé sféře, která je využívá především k analýze za účelem prodeje a reklamy. K dispozici jsou však i státním orgánům. Řada států se přitom snaží využít data k předvídání lidského chování s cílem zvýšit bezpečnost státu a jeho obyvatel.[110] Snahy předvídat lidské chování v nejrůznějších oblastech života na základě dat zpracovávaných počítači však mohou vést k zavádějícím výsledkům, které dosud neumíme ověřit. Z prvotně správných dat v oblasti zdravotnictví, bezpečnosti, pojišťovnictví, či jiných oblastech mohou být dovozeny nesprávné závěry s významnými dopady na život jednotlivců, skupin obyvatel i na stát.[111] Pochyby rovněž vyvolává nedostatek transparentnosti prediktivních analýz, která by zaručila alespoň částečnou kontrolu nad výslednými závěry.[112]

---

[107] Srov. případ KinderStart v. Google, 2007. RICE, Denis. *Google wins out in challenge to its website rating system* [online]. Lexology.com, 12. 10. 2016. Dostupné: http://www.internationallawoffice.com/Newsletters/E-commerce/USA/Howard-Rice-Nemerovski-Canady-Falk-Rabkin/Google-Wins-Out-in-Challenge-to-its-Website-Rating-System [Cit. 2022-10-26].

[108] Způsob zpracování metadat i funkce internetového vyhledávače řeší: OMER, Tene. What Google Knows: Privacy and Internet Search Engines [online]. *Utah Law Review*, October 1, 2007. Dostupné: https://ssrn.com/abstract=1021490 [Cit. 2022-10-26]. Ačkoli článek pochází z roku 2007 a Tene se v něm věnuje hrozbě internetových vyhledávačů na soukromí jednotlivců - uživatelů Internetu, identifikuje zároveň i problém mnohem obecnější - nebezpečí ztráty soukromí v důsledku běžných aktivit na webu.

[109] IP adresa může být dynamická nebo statická, statická bývá považována za osobní údaj spíše. IP adresa je osobním údajem, pokud ji můžeme přiřadit k určitému či určitelnému člověku za využití rozumných prostředků, které mají poskytovatelé informačních služeb obvykle k dispozici. OMER, Tene. Op. cit., str. 15 - 18.

[110] ZARSKY, Tal. Op. cit., str. 1505.

[111] RADEMACHEROVÁ, Kristina. Je svoboda šířit a přijímat informace ve virtuálním prostředí svobodou virtuální? *Jurisprudence*, 2018, č. 3, str. 5.

[112] Zakotvení principu transparentnosti v zákonodárství USA se věnuje ZARSKY, Tal. Op. cit., str. 1506 an.

Dosažitelností informací odkudkoli díky globálním počítačovým sítím dochází ke stírání kulturních rozdílů. Pojetí soukromí, svobody i bezpečnosti se sjednocuje. Globalizované pojetí se však dostává do konfliktu s chápáním problematiky soukromí, svobody a bezpečnosti ve fyzickém světě uživatelů, kde je tradičně ovlivněno konkrétním státním režimem, náboženstvím, kulturou a dalšími místními specifiky. Globální počítačová síť poskytuje zdání života v jediném globálním světě, který však mimo síť neexistuje. Může to vést ke značné frustraci internetových uživatelů, kteří srovnávají virtuální globální svět s okolním fyzickým světem, který jim klade do cesty různé překážky. V extrémních případech může deziluze přispět k revolucím, revoltám a vzepření se místním neutěšeným podmínkám, jako tomu bylo u tzv. Arabského jara,[113] či v současnosti u mladší generace demonstrujících občanů v Íránu.[114]

Otevřenost a neutralita prostředí Internetu umožňuje sdílet nejrůznější informace bez cenzurních zásahů. Negativním aspektem takřka neomezeného sdílení informací je však skutečnost, že se tak děje bez ohledu na jejich chybovost či manipulativní charakter. Požadavky na kritické hodnocení, třídění a zpracování informací jsou nutně vyšší než v minulosti, kdy odpovědným za zveřejněný obsah byl vydavatel. Ten nejen ovlivňoval podobu sdíleného obsahu, nýbrž i jeho auditorium.[115] Podle Lessiga přinesl vznik kyberprostoru *„svět, v němž může být každý vydavatelem"*.[116] V prostředí globální počítačové sítě se tímto vydavatelem může stát každý, kdo má přístup k počítači připojenému k síti.

Rozpoznání kvalitních a pravdivých informací je pro mnohé uživatele obtížné. Řada z nich se táže, jakým způsobem hodnotit nepřeberné množství informací okolo nich; někteří se neubrání ani pochybám, zda je to ještě v silách jednotlivce.[117] Problematické je i úmyslné šíření nepravdivých informací či informací s pravdivým základem, avšak zasazených do nesprávného kontextu, s cílem manipulovat čtenáře. Objevují se na tzv. dezinformačních webech, jejichž tematika je takřka neomezená a běžně navazuje na konkrétní politickou situaci v dané zemi. Podle

---

[113] Podle Salema byl rychlý proces digitalizace jedním z hlavních hybatelů událostí v zemích Arabského regionu v letech 2017 - 2021. SALEM, Fadi, Op. cit., str. 4 an.

[114] KEJLOVÁ, Tamara, SVITÁK, Matěj. *Írán může potkat osud Sovětského svazu. Nemáme co ztratit, hlásá generace Z a riskuje své životy* [online]. ČT24, 26. 10. 2022. Dostupné: https://ct24.ceskatelevize.cz/svet/3538284-iran-muze-potkat-osud-sovetskeho-svazu-nemame-co-ztratit-hlasa-generace-z-a-riskuje-sve [2022-10-27].

[115] MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí* [online]. 1. vyd. Praha: CZ.NIC, 2013, str. 187. Dostupné: https://knihy.nic.cz/files/edice/internet_jako_objekt_prava.pdf [Cit. 2022-10-27].

[116] LESSIG, Lawrence. *Code. Version 2.0* [online]. New York: Basic Books, 2006, str. 2. Překlad autorka. Dostupné: https://lessig.org/product/codev2/ [Cit. 2022-10-27].

[117] Kritickému hodnocení informací na Internetu ve vztahu k vzdělávání studentů středních škol se zabývá článek Michala Černého. ČERNÝ, Michal. *Hodnocení informací* [online]. Metodický portál RVP.CZ., 21.12.2020. Dostupné: https://clanky.rvp.cz/clanek/c/G/22721/hodnoceni-informaci.html [Cit. 2022-10-27].

datového analytika Františka Vrabela na sobě dezinformátoři cíleně pracují a zapojují do svých aktivit i technologie.[118]

1.2. Hodnoty informační společnosti

Československá právní nauka navazuje v oborech právní informatiky a práva informačních a komunikačních technologií na univerzálního právního teoretika Viktora Knappa, který již v 60. letech, v době rozvoje prvních velkých sálových počítačů,[119] formuloval své překvapivě přesné vize budoucího vývoje obou oborů. Z hlediska jejich hodnotového základu se však neměl o co opřít, neboť právní informatika a kybernetika byly chápány spíše jako nástroje umožňující zefektivnění řízení společnosti.[120] Ba co víc, kybernetiku představoval Knapp na počátku 60. let jako vysoce vědeckou metodu umožňující řídit socialistickou společnost v souladu s marxisticko-leninským poznáním přírodních i společenských procesů.[121] Ve vztahu k technicky pojímané kybernetice i právní informatice tak došlo k určitému hodnotovému vyprázdnění. Z uvedeného důvodu se domnívám, že je vhodné připomenout klíčové principy a hodnoty, z nichž vychází idea informační společnosti a které se mohou stát i referenčním hlediskem při výkladu hmotného práva informačních a komunikačních technologií.

1.2.1. Svoboda projevu a svoboda šířit a přijímat informace (informační svoboda)[122]

Právo svobodně šířit a přijímat informace lze považovat za součást široce pojatého práva na svobodu projevu. Matejka jej přirovnává k nástroji *sui generis* k hledání spravedlivé rovnováhy mezi svobodou jednotlivce a jeho povinnostmi. Jako univerzální právní princip se právo svobodně

---

[118] ČESKÝ ROZHLAS RADIOŽURNÁL. *František Vrabel: Více než 90 % dezinformačních webů v Česku jedná ve prospěch Ruska* [online]. Host Lucie Výborné, 27. 11. 2020. Dostupné: radiozurnal.rozhlas.cz [Cit. 2021-11-14].

[119] Prvním počítačem zkonstruovaným v Československu byl v roce 1957 SAPO, neboli Samočinný počítač, umístěný v budově Ústavu matematických strojů na Loretánském náměstí v Praze. HALCIN, Jakub. *Příběh počítače: 1. díl* [online]. Galaxie, 24. 6. 2005. Dostupné: http://www.galaxie.name/index.php?clanek=pribeh-pocitace-1-dil [Cit. 2022-10-27].

[120] Právo informačních a komunikačních technologií se vyděluje jako samostatná právní disciplína až od poloviny 80. let a oproti technicky pojímané právní informatice je chápáno jako hmotněprávní obor. POLČÁK, Radim. *Internet a proměny práva.* Op. cit., str. 51.

[121] KNAPP, Viktor. *O možnosti použití kybernetických metod v právu.* 1. vydání. Praha: Nakladatelství československé akademie věd, 1963, str. 7.

[122] Tato část disertační práce byla publikována v rámci článku autorky: RADEMACHEROVÁ, Kristina. Je svoboda šířit a přijímat informace ve virtuálním prostředí svobodou virtuální? *Jurisprudence*, 2018, č. 3, str. 3 - 18.

šířit a přijímat informace dostává do konfliktu s jinými hodnotami a chráněnými zájmy. Díky vzájemným konfliktům mezi chráněnými zájmy, k nimž dochází ve virtuálním prostředí stále častěji,[123] však právo na svobodu projevu plní svůj účel a smysl.[124]

Svoboda projevu a právo na informace jsou zaručeny v čl. 17 odst. 1 Listiny základních práv a svobod[125] (dále též „Listina" či „Listina základních práv a svobod"). Listina rozumí svobodou projevu a právem na informace právo vyjadřovat názory i svobodu vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na státní hranice.[126] Svoboda projevu a informací je zaručena i Listinou základních práv Evropské unie (dále též „EU"),[127] která v tomto ohledu klade důraz rovněž na pluralitu sdělovacích prostředků.[128] Svoboda projevu i právo na informace se řadí mezi základní náležitosti demokratického právního řádu. Svým charakterem svoboda projevu spadá do osobní autonomie jedince, do níž stát nesmí zasahovat (tzv. *status negativus*).[129] Její nositel ji může využít (pozitivní aspekt svobody projevu), současně však nesmí být nikým jakkoli k projevu nucen (negativní aspekt svobody projevu).[130] Bez ohledu na to, zda hovoříme o svobodě či o právu, obsah je shodný. Smyslem svobody projevu je možnost vyjádřit své myšlenky a pochopit lépe společnost, v níž žijeme, a případně přispět k její nápravě, nejsme-li spokojeni s jejím stavem.

Společenství, v němž probíhá ničím neomezená tvorba, zpracování a šíření informací pomocí informačních a komunikačních technologií, lze považovat za ideální informační společnost.[131] Předpokladem její existence je svoboda projevu a svoboda šířit a přijímat informace; hodnotovým východiskem takové společnosti je svoboda a solidarita.[132]

---

[123] Virtuální prostředí skýtá snadnou příležitost ke konfliktům, které se jinak odehrávají v off-line světě tím, že usnadňuje komunikaci mezi nejrůznějšími osobami a činí ji mnohem četnější. Ztrácí se vzdálenost dvou míst, interakce při neznalosti adresáta a příjemce není nemožná, a jiné kulturní či náboženské prostředí, nedostatek znalostí, prostředků, ale i kuráže, které mohou potenciálnímu konfliktu práv a svobod mimo Internet zamezit, zde nehraje natolik významnou roli.

[124] MATEJKA, Ján. Op. cit., str. 37 - 38.

[125] Usnesení předsednictva České národní rady č. 2 ze dne 28. prosince 1992 o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky.

[126] Viz čl. 17 odst. 2 Listiny.

[127] Listina základních práv Evropské unie, 2012/C 326/02, Dokument 12016P/TXT (dále jen „Listina základních práv EU"). Všechny právní předpisy EU dostupné: https://eur-lex.europa.eu [Cit. 2022-10-29].

[128] Srov. čl. 11 Listiny základních práv EU.

[129] BARTOŇ, Michal. *Svoboda projevu a její meze v právu ČR.* Praha: Linde, 2002, str. 19.

[130] FILIP, Jan. *Vybrané kapitoly ke studiu ústavního práva.* Brno: Masarykova univerzita, 2001, str. 129.

[131] K pojmu ideální informační společnost, jakož i k vývoji pojmu a různým hlediskům, z jejichž pohledu lze nahlížet na informační společnost, POLČÁK, Radim. *Internet a proměny práva*. Op. cit., str. 274 - 281.

[132] POLČÁK, Radim. *Internet a proměny práva*. Op. cit., str. 282. Pro autora možnost volné komunikace jednotlivců dokonce představuje prostor pro rozvoj základních hodnot lidské společnosti.

Solidarita nachází ve virtuálním prostředí svůj projev v přirozené tendenci člověka k výměně informací.[133] Právo šířit a přijímat informace ve virtuálním prostředí zahrnuje aktivní i pasivní složku: v rámci aktivní složky dává neomezenou možnost informace vytvořit a šířit; pasivním přístupem lze chápat možnost informace nalézt a získat k nim přístup umožňující jejich další využití. Virtuální prostředí úzce spojuje svobodu šířit a přijímat informace se svobodou projevu, neboť svobodný projev může být podmíněn informační svobodou, tedy neomezenou možností informace nalézt. Snaha státu cenzurovat jinak veřejně dostupné informace bývá obvykle vedena s úmyslem ovlivnit svobodu projevu svých občanů. Rovněž aktivní přístup v podobě výkonu práva šířit informace ve virtuálním prostředí může být naplněním práva na svobodný projev, neboť i jednoduchým sdílením určitého on-line odkazu lze vyjádřit svobodný názor. Svoboda projevu a právo šířit a přijímat informace jsou ve virtuálním prostředí vzájemně podmíněny výrazněji než mimo svět propojených počítačových sítí. Proto i řada států s politickým režimem nepřipouštějícím svobodu projevu odmítá umožnit svým občanům neomezený přístup k Internetu. Tak například státy s nejvyšší mírou cenzury na světě - Eritrea a Severní Korea, významně omezují přístup k síti Internet. Eritrea zablokovala v roce 2011 v důsledku tzv. Arabského jara své plány zpřístupnit občanům mobilní internetové připojení. Přístup k Internetu má jen 1% populace Eritrey, prostřednictvím internetových kaváren, které jsou snadno sledovány. Severní Korea poskytuje přístup k Internetu pouze vybraným jedincům a politické elitě, přičemž školám a vědeckým institucím umožňuje přístup pouze ke státem kontrolovanému intranetu.[134]

Faktický výkon práva na svobodu projevu i informační svoboda doznaly podstatných změn díky příchodu ICT. Klíčovou úlohu sehrál právě Internet. I podle Evropského soudu pro lidská práva (dále též „ESLP") plní Internet klíčovou roli v přijímání a výměně informací zejména tehdy, jsou-li informace v jiných zdrojích obtížně dohledatelné.[135] Zvláštní a unikátní význam ve smyslu nástroje umožňujícího přijímat a sdílet myšlenky a názory bez ohledu na cenzuru tradičních médií daného státu ESLP přisuzuje platformám jako je YouTube.[136] Podstatou virtualizace šíření informací je podle Michala Bobka demokratizace jejich zveřejňování, kterou umožnil právě Internet

---

[133] Typicky sdílením nejrůznějších dat. Podrobněji tamtéž, str. 284 - 287.

[134] Údaje podle studie Výboru pro obranu novinářů (CPJ) z roku 2019 a z roku 2015. CPJ. *10 Most Censored Countries* [online]. Commitee to Protect Journalists. Dostupné: https://cpj.org/2015/04/10-most-censored-countries/ Aktualizované údaje k roku 2019 dostupné: https://cpj.org/reports/2019/09/10-most-censored-eritrea-north-korea-turkmenistan-journalist/[Cit. 2022-10-27].

[135] Rozsudek ESLP ze dne 1. 12. 2015, *Cengíz and others v. Turkey,* stížnost č. 48226/10 a 14027/11, bod 51.

[136] V případě plošného zamezení přístupu k webu YouTube lze podle ESLP považovat všechny aktivní uživatele za osoby, jejichž práva přiznaná Úmluvou a Protokoly k ní byla porušena ve smyslu čl. 34 Úmluvy. Srov. rozsudek ESLP ze dne 1. 12. 2015, *Cengíz and others v. Turkey*, stížnost č. 48226/10 a č. 14027/11, body 52-53.

díky snadnému šíření informací o fyzických a právnických osobách, ale i o orgánech veřejné moci.[137] V kyberprostoru stejně jako ve fyzickém světě ovšem platí omezující podmínky pro šíření informací.[138] Svoboda projevu i právo šířit a přijímat informace musí být omezeny lidskou důstojností, která je klíčová též pro jiná základní lidská práva, především pro právo na soukromý život a na informační sebeurčení ve smyslu čl. 10 Listiny. Lidskou důstojnost si přitom nelze vykládat subjektivně. Lidská důstojnost by naopak měla být nezcizitelnou hodnotou chápanou v objektivním smyslu, která vytyčí jasné meze svobodě projevu i informační svobodě ve virtuálním prostředí tak, jako to činí mimo kyberprostor.[139]

1.2.2. Informační sebeurčení

Informační sebeurčení úzce souvisí s ochranou soukromí a komunikační svobodou, neboť zaručuje možnost svobodně se rozhodnout, jaké informace a v jakém rozsahu bude jedinec sdílet s okolní společností. Podle Ústavního soudu *„[p]rávo na nerušený soukromý život požívá v liberálních demokratických státech zcela zvláštní respekt a ochranu, neboť zajištění autonomní sféry jednotlivce je nejspolehlivější zárukou individuální nezávislosti a lidské svobody.”*[140] Respekt k soukromému životu umožňuje vznik prostoru pro rozvoj a realizaci individuální autonomní osobnosti, jeho funkcí je tedy zajistit prostor svobody jednotlivce.[141] Evropský soud pro lidská práva obvykle váže pojem soukromí k fyzické a psychické integritě osoby včetně jejího sexuálního života. Teze o povaze soukromí jako obecného práva, jehož se lze dovolat přímo, nikoli zprostředkovaně, pochází ze Spojených států amerických; v Evropě se právo na soukromí obsahově utvářelo až v souvislosti s mezinárodními smlouvami zejména ve smyslu práva na soukromý a rodinný život.[142]

---

[137] Stanovisko generálního advokáta Soudního dvora EU Michala Bobka ve věci C-194/16 (Bolagsupplysningen OÜ Ingrid Ilsjan proti Svensk Handel AB), bod 67.

[138] Pojem „fyzický svět” v této práci užívám s jistou nadsázkou jako protiklad k virtuálnímu světu, resp. kyberprostoru.

[139] Srov. např. čl. 19 odst. 3 Mezinárodního paktu OSN o občanských a politických právech, jenž předpokládá omezení plynoucí ze zákona ve prospěch respektování práv nebo pověsti jiných, k ochraně národní bezpečnosti, veřejného pořádku, veřejného zdraví nebo morálky. Vyhláška č. 120/1976 Sb., ministra zahraničních věcí o Mezinárodním paktu o občanských a politických právech a Mezinárodním paktu o hospodářských, sociálních a kulturních právech. Podrobněji k omezení informační svobody v prostředí Internetu srov. RADEMACHEROVÁ, Kristina. Je svoboda šířit a přijímat informace ve virtuálním prostředí svobodou virtuální? Op. cit., str. 9.

[140] Nález Ústavního soudu ze dne 2. 11. 2009, sp. zn. II. ÚS 2048/09, bod 19. K právu na ochranu soukromí srov. rovněž nálezy Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10, a ze dne 6. 3. 2012, sp. zn. I. ÚS 1586/09.

[141] Nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10, bod 29.

[142] Matejka, Ján. Op. cit., str. 35 - 36.

Listina garantuje ochranu soukromí v různých dimenzích na více místech. Kromě ochrany před neoprávněným zasahováním do soukromého a rodinného života přiznává každému právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.[143] Součástí práva na ochranu soukromí je tak i právo na informační sebeurčení. Omezení svobody projevu a práva šířit a přijímat informace závisí zejména na míře uplatnění informačního sebeurčení v soukromé nebo v sociální sféře života. Podle Ústavního soudu jde v soukromé sféře především o ochranu soukromí a cti, pročež zde platí naprosté informační sebeurčení. Je právem každého z nás určit, co a v jakém rozsahu bude sdílet s ostatními jako veřejnou informaci. Naopak ve sféře sociální, tj. společenské, občanské i profesionální, se absolutní informační sebeurčení neuplatní, neboť může obsahovat fakta, jež budou předmětem oprávněného veřejného zájmu.[144]

Součástí ochrany poskytované v souvislosti s právem na informační sebeurčení je i právo na ochranu před sledováním, hlídáním a pronásledováním ze strany veřejné moci i ve veřejném prostoru nebo na veřejně přístupných místech.[145] Podle Evropského soudu pro lidská práva nesmí státní orgány zároveň v zásadě zamezit přístup k informaci, kterou jiní zveřejnili za účelem jejího šíření.[146] Toto pravidlo nabývá zvláštního významu ve virtuálním prostředí elektronických komunikací. Nelze jej však vykládat bez návaznosti na odpovědnostní vztahy v případě, že zveřejněním určité informace dochází k porušení práv a oprávněných zájmů jiných osob. Orgány veřejné moci musí mít zároveň nástroje k tomu, aby mohly dalšímu šíření informace zveřejněné v rozporu se zákonem zamezit, dostane-li se do konfliktu s veřejným zájmem.[147] I na informační sebeurčení tedy lze nahlížet z hlediska jeho aktivní a pasivní složky: jednotlivec má svobodnou volbu rozhodnout se, jakou část svého života učiní veřejně dostupnou, současně však má i právo na ochranu před zveřejněním, rozhodne-li se informace o sobě nesdílet.

---

[143] Čl. 10 odst. 2 a 3 Listiny.

[144] Nález Ústavního soudu ze dne 15. 5. 2012, sp. zn. II. ÚS 171/12, bod 19. Obdobně srov. nález Ústavního soudu ze dne 17. 7. 2007, sp. zn. IV. ÚS 23/05, body 33 až 35. Ke kolizi práva na ochranu soukromí a informačního sebeurčení v profesní sféře a práva veřejnosti na informace srov. rovněž nález Ústavního soudu ze dne 17. 7. 2007, sp. zn. IV. ÚS 23/05, bod 34 a násl.

[145] Srov. WÁGNEROVÁ, Eliška, ŠIMÍČEK, Vojtěch, LANGÁŠEK, Tomáš, POSPÍŠIL, Ivo a kol. *Listina základních práv a svobod. Komentář.* Praha: Wolters Kluwer, 2014, s. 284. A dále i KOKEŠ, Marian. Čl. 10 [Právo na soukromý a rodinný život; právo na informační sebeurčení]. In: HUSSEINI, Faisal, BARTOŇ, Michal, KOKEŠ, Marian, KOPA, Martin a kol. *Listina základních práv a svobod.* 1. vydání (1. aktualizace). Praha: C. H. Beck, 2021, marg. č. 49.

[146] Rozsudek ESLP ze dne 16. 1. 2016, *Kalda v. Estonia*, stížnost č. 17429/10, body 41 a 42.

[147] RADEMACHEROVÁ, Kristina. Je svoboda šířit a přijímat informace ve virtuálním prostředí svobodou virtuální? Op. cit., str. 11. K odpovědnosti zprostředkovatele informace za zákonnost informací šířených prostřednictvím webových platforem srov. např. rozsudek ESLP ze dne 16. 6. 2015, *Delfi AS v. Estonia*, stížnost č. 64569/09. K zásahu státu do informační svobody srov. např. rozsudek ESLP ze dne 10. 1. 2013, *Ashby Donald and Others v. France*, stížnost č. 36769/08.

Zásahem do práva na informační sebeurčení je, *„pokud je jedinci znemožněno autonomně rozhodovat o tom, co a jak o něm bude známo, tedy pokud je mu znemožněno realizovat rozhodnutí týkající se jeho soukromého a rodinného života (někde bydlet, s někým utvářet vazby atp.) bez vědomí subjektů, kterým je tento jedinec nezamýšlel sdělovat."*[148] Omezení práva na informační sebeurčení je možné toliko za účelem ochrany jiných základních práv či ústavně aprobovaných veřejných zájmů.[149]

Vlivem rozvoje ICT došlo k posunu ve významu pojmů jako veřejný prostor, okolní společnost, či zveřejnění informace. Díky snadnému šíření informací skrze elektronické komunikační kanály se hranice veřejného a soukromého stávají obtížně definovatelné. Informace sdílená na zdánlivě uzavřeném diskuzním fóru či v prostředí komunikační platformy typu Facebook nebo WhatsApp toliko mezi úzkou skupinou přátel se může stát lehce veřejně dostupnou, a to i opakovaně, byť v offline světě by jednorázové sdělení například v prostředí návštěvy či během posezení několika lidí podobné úvahy nevzbuzovalo.[150] Nejenže je obtížné odhadnout budoucí dráhu šíření jednou sdílené informace ve virtuálním prostoru, existuje i mnoho nástrojů, které mohou zasáhnout do soukromí jednotlivců, aniž by tito vůbec měli v úmyslu jakoukoli informaci o sobě samých učinit komukoli dostupnou.[151] V době rozvoje globálních informačních a komunikačních sítí se tak informační sebeurčení stává výzvou. Ideologický základ Internetu však pramení nejen z práva na svobodné šíření a přijímání informací, nýbrž i z práva na informační sebeurčení.[152] I z tohoto důvodu je nutné nahlížet na informační sebeurčení jako na klíčovou ideu informační společnosti.

Respektuje-li se právo jedince svobodně se rozhodnout, jaké informace učiní veřejně dostupnými a jaké ne, je nutno zohlednit i změnu názoru, jež povede k rozhodnutí dříve veřejně sdílené informace již nesdílet. Součástí informačního sebeurčení je tudíž i tzv. právo na výmaz informací (právo být zapomenut), které je zakotveno v čl. 17 obecného nařízení o ochraně osobních

---

[148] Nález Ústavního soudu ze dne 11. 10. 2021, sp. zn. II.ÚS 1022/21.

[149] K podmínkám omezení práva na informační sebeurčení srov. nálezy Ústavního soudu ze dne 22. 1. 2001, sp. zn. II. ÚS 502/2000 a ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10.

[150] Již roku 2001 soudce Nejvyššího soudu Spojených států amerických Antonin Scalia prohlásil, že tvrdit, že míra soukromí zůstala technickým pokrokem nedotčena, by bylo bláznovstvím. Rozsudek Nejvyššího soudu USA ze dne 11. 6. 2001, *Kyllo proti Spojeným státům americkým*, 533 U.S. 27. Dostupný: https://www.law.cornell.edu/supct/html/99-8508.ZO.html [Cit. 2022-10-29].

[151] Příkladem mohou být různé webové vyhledávače, databáze, automatizovaná analýza objemných datových souborů, určování polohy pomocí GPS či IP adresy, sdílení souborů pomocí cloudových úložišť atd., na jejichž základě lze usuzovat nejen o poloze, obvyklém bydlišti, věku, či zájmech jednotlivce, ale též o jeho sexuální orientaci, zdravotním stavu, politickém smýšlení, apod.

[152] YAR, Majid. Op. cit., str. 7.

údajů.[153] Pro příště tak lze žádat neprodlený výmaz osobních údajů z taxativně stanovených důvodů, přičemž jedním z nich je i skutečnost, že došlo k odvolání souhlasu se zpracováním osobních údajů.[154]

V souvislosti s informační svobodou panující na Internetu však žádost o výmaz osobních údajů nemusí nutně vést k jejich celosvětovému výmazu v tom smyslu, že je nebude možno na Internetu vůbec nalézt. Vyvažováním práva na respektování soukromého života a ochranu osobních údajů na straně jedné, s právem svobodně šířit a přijímat informace na Internetu na straně druhé, se zabýval Soudní dvůr EU (dále též „SDEU") za situace, kdy společnost Google odstranila na žádost subjektu údajů odkaz na internetové stránky ze seznamu výsledků zobrazených po zadání jeho jména, avšak pouze pro území EU (tj. došlo k výmazu údajů pouze pro vyhledávání uskutečněné z domén členských států EU).[155] S odkazem na odlišnou úroveň zájmu veřejnosti na přístup k informacím v různých členských státech SDEU shledal, že poměřování dvou kolidujících práv nepovede vždy k jedinému shodnému výsledku pro všechny členské státy. V současnosti tak právo EU neukládá odstranit odkazy z vyhledávačů ve vztahu ke všem členským státům, nicméně to ani nezakazuje. Poměření práva na respektování soukromí a na ochranu osobních údajů s právem na informace z pohledu vnitrostátního standardu pro ochranu základních práv je v pravomoci dozorového úřadu či soudu členského státu.[156] V návaznosti na výsledek poměření lze provozovateli vyhledávače uložit povinnost, aby odkazy odstranil ze všech mutací (verzí) vyhledávače.[157]

1.3. Principy a východiska kybernetické bezpečnosti[158]

Jak bylo řečeno úvodem, právní úprava kybernetické bezpečnosti je ojedinělá předně díky ovlivnění technickými odvětvími, ale i naukou mezinárodních bezpečnostních vztahů a aktuálními

---

[153] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „obecné nařízení o ochraně osobních údajů").

[154] Srov. čl. 17 odst. 1 písm. b) obecného nařízení o ochraně osobních údajů.

[155] Rozsudek SDEU ze dne 24. 9. 2019 ve věci C-507/17, *Google LLC, právní nástupkyně Google Inc. v. Commission nationale de l'informatique et des libertés (CNIL)*.

[156] Srov. rozsudky SDEU ze dne 26. 2. 2013 ve věci C-617/10, *Åkerberg Fransson*, bod 29, a ze dne 26. 2. 2013 ve věci C-399/11, *Melloni*, bod 60.

[157] Rozsudek SDEU ze dne 24. 9. 2019 ve věci C-507/17, *Google LLC, právní nástupkyně Google Inc. v. Commission nationale de l'informatique et des libertés (CNIL)*, bod 72.

[158] Text vychází z práce autorky odevzdané v rámci XI. ročníku Studentské vědecké a odborné činnosti Právnické fakulty Univerzity Karlovy v kategorii doktorandského studia: RADEMACHEROVÁ, Kristina. *Principy a východiska kybernetické bezpečnosti de lege lata.* Praha, 2018. Studentská vědecká odborná činnost. Karlova Univerzita, Právnická fakulta, 2018-04-16.

politickými poměry daného státu.[159] Právní normy jsou zde utvářeny nejen vlivem vědecko-technologického vývoje, ale reagují do značné míry i na aktuální mezinárodní politickou situaci a nároky plynoucí z členství státu v mezinárodních společenstvích a organizacích. Dalším specifikem zmíněného právního odvětví je, že český zákonodárce neměl možnost navázat na žádnou existující právní úpravu ani judikaturu. Klíčové pro poznání a aplikaci nové právní úpravy jsou tudíž specifické právní principy, které zastávají vedle právních norem v regulaci kybernetické bezpečnosti důležitou funkci jako metanormativní prvky.[160]

Právní principy pomáhají právo snáze teoreticky uchopit a aplikovat.[161] Následující text proto představí stěžejní právní principy právní úpravy kybernetické bezpečnosti v ČR a společenská východiska její regulace. Pochopení podstaty klíčových odvětvových principů práva kybernetické bezpečnosti může usnadnit výklad i aplikaci dotčených právních norem.

Mnohé obecné principy správního práva jsou vyjádřeny v normách ústavní úrovně, zejména principy zákonnosti, legality, soudní kontroly správy, či objektivní odpovědnosti státu za nezákonná rozhodnutí a nesprávný úřední postup. Některé nachází konkrétní podobu v principech kybernetické bezpečnosti (např. princip objektivní odpovědnosti státu v principu bdělosti ve vztahu k ostatním státům a mezinárodnímu společenství, tzv. *due diligence*). Řada principů nové právní úpravy kybernetické bezpečnosti se objevuje i ve směrnici NIS, která se jako klíčový právní předpis EU v oblasti kybernetické bezpečnosti promítá i do české zákonné úpravy.[162]

Text vychází zejména z důvodové zprávy k ZKB a dostupné české i zahraniční literatury. Představuje konkrétní projevy principů v zákonné úpravě s cílem zjistit jejich skutečný dopad. Zvláštní pozornost je věnována především dvěma principům, a to principu technologické neutrality a principu ochrany informačního sebeurčení člověka, které jsou pro kybernetickou bezpečnost klíčové.

1.3.1. K právním principům

Právní principy jsou vedle právních norem nejvýznamnější částí objektivního platného práva. Představují vůdčí zásady, na nichž stojí právní systém jako celek i jeho jednotlivá odvětví.

---

[159] Kyberterorismus a obrana proti kybernetickým útokům se v posledním desetiletí stává klíčovým tématem mezinárodních vztahů a bezpečnostní politiky. EICHLER, Jan. *Terorismus a války v době globalizace*. 2., dopl. vyd. Praha: Karolinum, 2010, str. 142 – 146. JIROVSKÝ, Václav. Op. cit., str. 129.

[160] GERLOCH, Aleš. *Teorie práva*. 7. vyd. Plzeň: Aleš Čeněk, 2017, str. 34.

[161] WINTR, Jan. *Říše principů: obecné a odvětvové principy současného českého práva*. Praha: Karolinum, 2006, str. 9.

[162] § 1 odst. 2 ZKB.

Shodně jako právní normy mají i právní principy preskriptivní charakter, od právních norem se však odlišují vyšší mírou obecnosti a abstraktnosti. Právní principy mohou být i kontradiktorní, neboť vychází z hodnot, které nejsou vždy slučitelné.[163] Vzhledem k proměnlivosti právních norem je nezávislost právních principů na právní normě jejich aplikační výhodou. Při rozhodování konkrétních sporů lze přitom přihlédnout i k právním principům, které nejsou formálně ukotveny v právních předpisech.[164]

Klíčový význam právních principů při interpretaci a aplikaci práva opakovaně potvrdil i Ústavní soud ČR. Podle něj není obecný soud *„výslovně vázán doslovným zněním zákonného ustanovení, ale smí, a dokonce musí se od něj odchýlit v případě, kdy to vyžaduje ze závažných důvodů smysl či účel zákona, historie jeho vzniku, systematická souvislost nebo některý z principů, jež mají svůj základ v ústavně konformním právním řádu…"*[165]

Význam právních principů v soudcovské tvorbě právního systému *common law* zdůraznil Dworkin,[166] který připomněl jejich vliv při výkladu jednoznačné, ale pro daný případ nesmyslné právní normy. Důležitost právních principů spočívá rovněž v tom, že nabízí zjednodušená modelová řešení sporných otázek, aniž je třeba detailně znát i právní normu, čímž umožňují v oblasti intuitivní orientaci.[167] Zatímco právní normy obsažené v právních předpisech mohou být jen splněny či nesplněny, principy přikazují realizovat určité jednání v maximální možné míře.[168]

Právní principy lze dělit na univerzálně platné, které prostupují celým právním řádem, a odvětvové, týkající se jednotlivých právních odvětví. Univerzální právní principy jsou všeobecnými postuláty požadovaného chování osob, uznávané většinou civilizovaných států světa.[169] V tomto ohledu lze odkázat na dostupnou literaturu.[170]

---

[163] GERLOCH, Aleš. Op. cit., str. 34–36.

[164] WINTR, Jan. Op. cit., str. 62.

[165] Nález Ústavního soudu ze dne 13. 6. 2006, sp. zn. I. ÚS 50/03.

[166] DWORKIN, Ronald. *Law's empire*. London: Fontana Press, 1991.

[167] TRYZNA, Jan. *Právní principy a právní argumentace: k vlivu právních principů na právní argumentaci při aplikaci práva*. Praha: Auditorium, 2010, str. 131.

[168] Odlišné stanovisko Pavla Höllandera k nálezu pléna Ústavního soudu ze dne 3. 4. 1996, sp. zn. Pl. ÚS 32/95.

[169] Např. *neminem laedere*, *pacta sunt servanda*, *lex retro non agit* či *lex specialis derogat legi generali* aj.

[170] Např. KUČERA, Stanislav, BOGUSZAK, Jiří. (eds.). *Právní principy: kolokvium*. Pelhřimov: Vydavatelství 999, 1999.; TRYZNA, J. *Právní principy a právní argumentace: k vlivu právních principů na právní argumentaci při aplikaci práva*. Praha: Auditorium, 2010.; KNAPP, Viktor. *Velké právní systémy: Úvod do srovnávací právní vědy*. Praha: Beck, 1996.; WINTR, Jan. *Říše principů: obecné a odvětvové principy současného českého práva*. Praha: Karolinum, 2006.

V oblasti kybernetické bezpečnosti platí zvláštní právní principy. Z hlediska zařazení do právního odvětví má česká právní úprava kybernetické bezpečnosti nejblíže ke správnímu právu, přestože lze některé z principů řadit i do soukromoprávních odvětví. Je tomu tak například u principu autonomie vůle regulovaných subjektů a principu ochrany informačního sebeurčení. Ani o samotném odvětví práva informačních a komunikačních technologií,[171] pod nějž spadá i regulace kybernetické bezpečnosti, nelze říci, že by bylo součástí jediného právního odvětví z oblasti soukromého nebo veřejného práva. Právní úprava kybernetické bezpečnosti je souborem právních norem, jimiž jsou ukládány povinnosti osobám odlišným od státu. Kybernetickou bezpečnost lze tudíž chápat jako zvláštní odvětví veřejného práva, jehož základem je autoritativní rozhodování o právech a povinnostech jiných osob, s cílem kyberprostor spravovat a učinit jej bezpečnějším pro jednotlivé subjekty (státy, skupiny obyvatel, jednotlivce, soukromé i veřejné instituce atp.). Následující text proto krátce připomene některé z obecných principů správního práva, které upravují organizaci a činnost veřejné správy.[172]

1.3.2. Obecné principy správního práva

Mnohé obecné principy správního práva jsou vyjádřeny v normách ústavní úrovně. Zejména to platí pro principy zákonnosti, legality, soudní kontroly správy či objektivní odpovědnosti státu za nezákonná rozhodnutí a nesprávný úřední postup. Konkrétní podoby obecných principů správního práva lze nalézt i v právních normách upravujících kybernetickou bezpečnost. Princip objektivní odpovědnosti státu se promítá do principu označovaném jako *due diligence*, či jako princip bdělosti ve vztahu k ostatním státům a mezinárodnímu společenství, podle něhož bude stát odpovídat za škodlivé následky jednání, k němuž dojde v jeho jurisdikci.

Obecné principy správního práva lze členit podle odvětví práva jako vnějšího nástroje správní činnosti (spravování), práva jako nástroje ochrany spravovaných subjektů a práva jako vnitřního nástroje správní činnosti, přičemž každá z uvedených oblastí má své vlastní principy.[173] Hendrych,[174] vycházeje z třídění podle Morand-Devillerové,[175] poukazuje na dvě oblasti principů.

---

171 Samostatnost odvětví této disciplíny obhajuje např.: POLČÁK, Radim. *Internet a proměny práva*. Op. cit., str. 54–85.

172 HENDRYCH, Dušan a kol. Op. cit., str. 15.

173 POMAHAČ, Richard. Právní principy dobré správy – imaginace či realita? In: KUČERA, Stanislav, BOGUSZAK, Jiří (eds). *Právní principy: kolokvium*. Pelhřimov: Vydavatelství 999, 1999, str. 189.

174 HENDRYCH, Dušan a kol. Op. cit., str. 56.

175 MORAND-DEVILLER, Jacqueline. *Cours de droit administratif.* Paris: Montchrestien, 1989, str. 188.

První je založena na tradici práv člověka a občana a vychází z ní principy rovnosti, ať již ve vztahu k administrativním povinnostem nebo k veřejným službám. Jako projev principů rovnosti lze v právu kybernetické bezpečnosti vidět princip technologické neutrality, který zakazuje diskriminační jednání ve vztahu k užité technologii. Druhou oblastí jsou principy tvořící dobrou správu, principy její organizace a činnosti. Do této oblasti spadají např. principy kontinuity (nepřetržitosti) veřejných služeb, práva na obranu, princip autonomie a speciality osob veřejného práva. Princip kontinuity veřejných služeb se v kybernetické bezpečnosti projevuje v ochraně informačního sebeurčení člověka a jeho nedistributivních práv, a tím i bezpečného kyberprostoru. Jeho cílem je zajištění kontroly nad hrozbami, jež by mohly vést až k přerušení činnosti veřejné správy. Mezi principy dobré správy lze řadit také princip proporcionality, rovnosti, otevřenosti a transparentnosti správy, hospodárnosti a rychlosti, či princip ochrany nabytých práv.[176] Mezi základními principy správního práva zmiňuje Wintr princip jednoty správního práva, projevující se obvykle subsidiaritou správního řádu[177] vůči procesním normám speciálních odvětví, princip presumpce správních aktů a princip jejich vynutitelnosti, které správním orgánům umožňují řádný (a efektivní) výkon správy při autoritativním rozhodování za účelem ochrany státního i veřejného zájmu.[178]

Význam principů správního práva charakterizujících dobrou správu zdůrazňuje i SDEU, který přiznává žalobci nejen právo namítat vůči správnímu orgánu porušení evropského práva, ale i ohrožení principu dobré správy.[179] Zásadní roli v evropském správním právu přiznává obecným právním zásadám a principům i proto, že již od počátku své činnosti byl soud veden snahou formulovat pravidla odlišující dobrou správní činnost od špatné a neodmítal žádný případ pouze pro nedostatečnost evropského práva. V souladu se zákazem odepření spravedlnosti (*denegatio iustitiae*) si v případě absence jasného pravidla, podle něhož by mohl věc rozhodnout, SDEU vypomáhá analogií či obecnými právními zásadami.[180]

Principům dobré správy se věnuje i činnost Rady Evropy odpovídající svojí povahou *soft-law*.[181] Sdílené principy veřejné správy mezi členskými státy EU daly vzniknout Evropskému

---

[176] Blíže např. WINTR, Jan. Op. cit., str. 218–221.

[177] Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů (dále jen „správní řád").

[178] Podrobněji WINTR, Jan. Op. cit.,str. 216–217.

[179] POMAHAČ, Richard. Op. cit., str. 188.

[180] HENDRYCH, Dušan a kol. Op. cit., str. 746 - 750.

[181] COUNCIL OF EUROPE. *12 Principles of Good Governance and European Label of Governance Excellence* [online]. Dostupné: https://www.coe.int/en/web/good-governance/12-principles [Cit. 2022-10-30].

správnímu prostoru (*European Administrative Space*).[182] Dotčené osoby se mohou dovolat principů dobré správy v rámci přezkumu, ať již uvnitř veřejné správy nebo vně, v rámci správního soudnictví. Správní orgány jsou tak povinny respektovat principy veřejné správy při výkonu svých pravomocí.

Ochraně občanů před jednáním, jež neodpovídá principům demokratického právního státu a dobré správy, se věnuje i veřejný ochránce práv. Dobrá správa přitom představuje *„postup úřadu, který je nejen v souladu se zákonem, ale zároveň mu nelze vytknout svévoli, účelovost, vyhýbavost, neefektivnost, liknavost a jiné nežádoucí znaky."*[183] Zvláště principy dobré správy a s nimi související princip odpovědnosti veřejné správy (někdy též uváděný jako součást principů dobré správy) lze chápat jako klíčové hodnoty práva kybernetické bezpečnosti: efektivní veřejná správa by měla zajistit bezpečnost informačních systémů a sítí, umožnit spolehlivou výměnu autentických informací, a tím i nepřetržitou funkčnost řady služeb. Neumožní-li to nebo dojde-li k pochybení, musí nést odpovídající odpovědnost.

1.3.2.1. Principy dobré správy

Pojem dobré správy zprvu správní právo opomíjelo, neboť byl vnímán spíše jako mimo-právní koncept. Zásadní bylo pro právníky naplnění principu legality, tedy zda je veřejná správa vykonávána v souladu s právem, či nikoli.[184] Teprve od sedmdesátých let 20. století se dobrá správa dostává do ohniska zájmu správní vědy díky vývoji doktríny *corporate governance*, zabývající se dobrou správou veřejně obchodovatelných společností. Definitivně je právo na dobrou správu v EU ukotveno v souvislosti s vyhlášením Listiny základních práv EU a přijetím Lisabonské smlouvy.[185] Pod pojmem dobré správy (*good governance*) bylo pod patronátem Organizace spojených národů pro potřeby agendy rozvojové pomoci představeno následujících osm principů: otevřenost k účasti zainteresovaných osob, respekt k právním pravidlům a principům, průhlednost (ve smyslu transparentnosti), vstřícnost k oprávněným požadavkům, schopnost smiřovat rozdílné zájmy, poskytovat rovné příležitosti, uspokojovat potřeby úměrně k disponibilním zdrojům, a provádět

---

[182] OECD. *European Principles for Public Administration* [online]. SIGMA Papers, No. 27. Paris: OECD Publishing, 1999. Dostupné: https://doi.org/10.1787/5kml60zwdr7h-en [Cit. 2022-10-30]. Ačkoli Evropský správní prostor nepředstavoval součást acquis communautaire, slouží jako vodítko pro správně-právní reformy napříč EU, včetně nově přistupujících zemí.

[183] VEŘEJNÝ OCHRÁNCE PRÁV. *Souhrnná zpráva o činnosti veřejného ochránce práv za rok 2006*. Brno: Masarykova univerzita, Kancelář veřejného ochránce práv, 1. vydání, 2007, str. 113.

[184] POMAHAČ, Richard. *Správní spravedlnost*. Právník, č. 144/5, 2005, str. 433.

[185] Podrobněji k termínu *corporate governance* a vývoji úvah o dobré správě v EU srov. POMAHAČ, Richard, HANDRLICA, Jakub. *Evropské správní právo*. Praha: C.H. Beck, 2012, str. 65 - 70.

dobrou kontrolu správy.[186] V uvedených principech lze spatřit konkretizaci obecných principů správního práva a základních zásad činnosti správních orgánů vyjádřených i v Hlavě II správního řádu, jako je princip rovnosti (poskytování rovných příležitostí), princip legality (respekt k právním pravidlům a principům), ochrana práv nabytých v dobré víře a služba veřejnosti (vstřícnost k oprávněným požadavkům i otevřenost k účasti zainteresovaných osob), či princip hospodárnosti (uspokojování potřeb v souladu s disponibilními zdroji).

Zejména na globální a evropské úrovni se dobrá správa prolíná s etickými pravidly.[187] Obsah pojmu byl ovlivněn Veřejným ochráncem práv EU, který skrze definici nesprávných úředních postupů a špatné správy (*maladministration*), jakož i v souvislosti s přijetím Zásad veřejné služby pro úředníky EU v roce 2012, nastavil požadavky profesionálního přístupu úřednictva odpovídající vyšším etickým normám. Dobrá správa tak jednoznačně překračuje pouhé jednání ve smyslu zákona. Má být profesionální, objektivní, srozumitelná, nezávislá, jednající i v souladu se zdravým rozumem a mající na zřeteli závazek vůči občanům.[188] Právo na dobrou správu musí respektovat orgány, instituce a všechny administrativní subjekty EU, jakož i členské státy, pokud aplikují právo EU. Listina základních práv EU garantuje právo na řádnou správu reflektující požadavky nestrannosti, spravedlnosti a rychlosti, jakož i účasti zainteresovaných osob, otevřenosti a odpovědnosti za škodu způsobenou veřejnou správou. V případě nesprávného úředního postupu orgánů, institucí nebo jiných subjektů EU, s výjimkou SDEU při výkonu jeho soudních pravomocí, zaručuje přístup k Evropskému veřejnému ochránci práv.[189] Principy rozhodování a dobré správy v evropském správním prostoru zdůraznila i Bílá kniha Evropské komise o evropském vládnutí z roku 2001.[190] Ve snaze obnovit důvěru obyvatel v orgány, instituce i úřední aparát EU představila reformu evropské správy, kladoucí zvláštní důraz na principy otevřenosti a srozumitelnosti, participace a spolupráce s místní a regionální úrovní správy věcí veřejných, jakož i důraz na princip odpovědnosti, efektivity a souladu jednotlivých politik a správních činností. Komplexní úprava

---

[186] POMAHAČ, Richard, HANDRLICA, Jakub. Op. cit., str. 66.

[187] POMAHAČ, Richard, HANDRLICA, Jakub. Op. cit., str. 66.

[188] Důraz se klade zejména na etiku, objektivitu, transparentnost, úctu k ostatním a existenci určitého závazku vůči EU i jejím občanům. Srov. EVROPSKÝ VEŘEJNÝ OCHRÁNCE PRÁV. *Zásady veřejné služby pro úředníky EU* [online]. Evropská unie, 2012. Dostupné: https://www.ombudsman.europa.eu [Cit. 2022-10-30].

[189] Srov. čl. 41 až 43 Listiny základních práv EU.

[190] EVROPSKÁ KOMISE. European governance - A white paper /* COM/2001/0428 final */. Official Journal 287, 12/10/2001 P. 0001 - 0029. Dostupné: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52001DC0428&qid=1488203863476 [Cit. 2022-10-30].

výkonu správních aktů a opatření však v EU chybí,[191] což může bránit efektivnímu výkonu správních činností napříč EU.

Právní požadavky na dobrou správu a její definici shrnuje i Kodex dobré správy přijatý Výborem ministrů Rady Evropy jako Doporučení REC(2007)7 o dobré veřejné správě/good governance.[192] Jeho cílem je zaručit právo na dobrou správu u adresátů správních aktů, jimiž Kodex rozumí správní nařízení, obecná správní opatření i individuální rozhodnutí při výkonu veřejné správy. Kodex klade důraz na kontrolu kvality a efektivity veřejné správy, kterou definuje skrze zásady zákonnosti, rovnoprávnosti, nestrannosti, proporcionality, právní jistoty, časové přiměřenosti, participace, úcty k soukromí a transparentnosti.[193]

1.3.2.2. Princip odpovědnosti veřejné správy

Odpovědnost veřejné správy je jedním ze základních hodnotových principů evropského správního prostoru. Slouží k ochraně soukromých i veřejných zájmů, je zásadní pro efektivitu a předvídatelnost postupu správních orgánů a brání svévoli. Studie Organizace pro hospodářskou spolupráci a rozvoj (dále též „OECD"[194]), zabývající se evropskými principy veřejné správy, charakterizuje princip odpovědnosti veřejné správy široce jako požadavek, podle něhož každý správní orgán odpovídá za své jednání jiným správním, legislativním i soudním autoritám, přičemž z tohoto pravidla není výjimek (neexistuje neodpovědná správa). Konkrétní způsob přezkumu či kontrolní mechanismus přitom nejsou rozhodné. Nezáleží na tom, zda se lze nápravy dovolat u nadřízeného správního orgánu, veřejného ochránce práv (ombudsmana), k tomu speciálně určené komise, či v rámci parlamentního výboru. Odpovědnost veřejné správy však musí zajistit, že klíčové principy zákonnosti (*rule of law*), otevřenosti, transparentnosti, nestrannosti a rovnosti před zákonem budou vždy respektovány.[195]

Princip odpovědnosti shrnul v roce 2007 Otakar Motejl, první veřejný ochránce práv v ČR, jednoduše jako povinnost správního úřadu nevyhýbat se řešení záležitostí spadajících do jeho

---

[191] Při výkonu správních opatření se uplatňuje princip subsidiarity, když EU nedisponuje pravomocí vytvořit jednotnou úpravu společného základu administrativních procedur, není-li výkon svěřen do výlučné působnosti orgánu EU. KLÍMA, Karel a kol. *Evropské právo.* Plzeň: Aleš Čeněk, 2011, str. 247.

[192] COUNCIL OF EUROPE. *Recommendation CM/Rec(2007)7 of the Committee of Ministers to member states on good administration* [online]. Dostupné: https://rm.coe.int/0900001680709 6b9 [Cit. 2022-10-30].

[193] POTĚŠIL, Lukáš. „Dobrá správa" v dokumentech Rady Evropy [online]. *Veřejná správa,* 2008, č. 12. Dostupné: https://www.mvcr.cz/clanek/verejna-sprava-obsah-cisla-12-2008.aspx [Cit. 2022-10-30]. POMAHAČ, Richard, HANDRLICA, Jakub. Op. cit., str. 69 - 70.

[194] Z anglického názvu The Organisation for Economic Co-operation and Development.

[195] OECD. *European Principles for Public Administration*. Op. cit., str. 12 - 13.

kompetence a přiznávat chyby, kterých se přitom dopustí. Pokud tedy *„úřad udělá chybu, jasně a výslovně tuto chybu přizná, písemně se za ni osobě omluví a neodkladně přijme účinná opatření k nápravě, popřípadě osobu poučí o možnosti žádat o náhradu škody způsobené nesprávným úředním postupem."*[196]

Odpovědnost veřejné správy z obecného hlediska souvisí s hodnotovým posunem chápání správy spíše jako veřejné služby než jen v souvislosti s jejím mocenským pojetím. Závisí především na důsledném uplatňování základních zásad činnosti správních orgánů tak, jak je vymezuje v úvodních ustanoveních správní řád,[197] jakož i na fungování kontrolních mechanismů zakotvených v institucích demokratického právního státu. Jedná se zejména o existenci nezávislého správního a ústavního soudnictví, institut odpovědnosti za škodu způsobenou nezákonným rozhodnutím či nesprávným úředním postupem, jakož i o kontrolu ze strany dalších institucí, jakými jsou například Parlament ČR, veřejný ochránce práv či Nejvyšší kontrolní úřad.

Garancí odpovědnosti veřejné správy je především Listina, která zakotvuje právo na účinnou právní ochranu před nezákonným působením veřejné správy v čl. 36. Nestanoví-li zákon výjimku, zaručuje se každému, kdo se domnívá, že byl zkrácen na svých právech rozhodnutím orgánu veřejné správy,[198] právo obrátit se na soud za účelem přezkumu zákonnosti takového rozhodnutí.[199] Není přitom rozhodné, zda jde o fyzickou či právnickou osobu ani zda je fyzická osoba českým občanem či zda tu má právnická osoba své sídlo. Uvedené právo náleží i státu, pakliže nevystupuje ve vrchnostenském postavení.[200] Tvrzení o zkrácení na právech a z něj dovozenou aktivní procesní legitimaci žalobce je nutno pojímat široce, s cílem umožnit soudní přezkum. Není přitom třeba přesně konkretizovat veřejné subjektivní právo, které mělo být porušeno, postačí tvrzení o zásahu do žalobcovy právní sféry.[201]

---

[196] VEŘEJNÝ OCHRÁNCE PRÁV. *Souhrnná zpráva o činnosti veřejného ochránce práv za rok 2006*. Op. cit., str. 115.

[197] Srov. §§ 2 - 8 správního řádu.

[198] K vymezení zde uvedeného pojmu orgán veřejné správy viz § 4 odst. 1 písm. a) zákona č. 150/2002 Sb., soudní řád správní, ve znění pozdějších předpisů (dále jen „s. ř. s.").

[199] Čl. 36 odst. 2 Listiny.

[200] Srov. rozsudek Nejvyššího správního soudu ze dne 11. 11. 2004, č. j. 2 As 36/2004-46.

[201] Srov. usnesení Nejvyššího správního soudu ze dne 23. 3. 2005, č.j. 6 A 25/2002-42.

Ústavně zaručeno je též právo na náhradu škody. Za podmínek stanovených zákonem[202] má každý[203] právo na náhradu škody způsobené mu nezákonným rozhodnutím státního orgánu a orgánu veřejné správy, či nesprávným úředním postupem.[204] Za výkon státní moci státními orgány, orgány územní samosprávy při přeneseném výkonu státní správy a fyzickými a právnickými osobami, jimž byl svěřen výkon veřejné správy, odpovídá stát. Územní samosprávné celky odpovídají za výkon samostatné působnosti. Zájmové a jiné samosprávy zákon o odpovědnosti za škodu neřeší a odpovědnosti za škodu se tudíž nelze podle tohoto zákona dovolat.[205]

Odpovědnost státu i územní samosprávy nezávisí na zavinění, nýbrž na výsledku, je tedy objektivní. Obecné soudy musí pamatovat při výkladu zákona o odpovědnosti za škodu na ústavní zakotvení uplatňovaných nároků a z nich vyplývající odpovědnost státu nepřípustně nezužovat. Současně je však třeba respektovat i veřejný zájem na efektivním výkonu veřejné moci.[206] Efektivní výkon veřejné moci by mohl být omezen, případně by veřejná správa mohla až rezignovat na uplatňování příslušných pravomocí, pakliže by právo na náhradu újmy způsobené výkonem veřejné moci bylo uplatňováno nepřiměřeně extenzivně.[207] Doktrína nazývá uvedený důsledek tzv. mrazícím účinkem (*chilling effect*), který se, jak podotkl Ústavní soud, může projevit alibistickým rozhodováním či úplnou rezignací na výkon veřejné moci.[208] V rovině kybernetické bezpečnosti je princip odpovědnosti za škodu možno chápat jako požadavek odpovědnosti státu za škodlivé následky jednání, jež nastanou v jeho jurisdikci (*due diligence*). O tomto principu bude pojednáno níže.

---

[202] Právo na náhradu škody provádí zákon č. 82/1998 Sb., o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem a o změně zákona České národní rady č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád), ve znění pozdějších předpisů (dále jen „zákon o odpovědnosti za škodu"). Zákon o odpovědnosti za škodu je ve vztahu speciality k obecné úpravě v občanském zákoníku.

[203] Otázkou však zůstává, zda toto právo svědčí i samotné veřejné moci, je-li zároveň adresátem této ústavní povinnosti. K rozporuplné judikatuře Ústavního soudu v tomto ohledu srov. HUSSEINI, Faisal, KOPA, Martin. Čl. 36 [Právo na soudní a jinou právní ochranu]. In: HUSSEINI, Faisal, BARTOŇ, Michal, KOKEŠ, Marian, KOPA, Martin a kol. *Listina základních práv a svobod.* Op. cit., marg. č. 265.

[204] Čl. 36 odst. 3 a 4 Listiny.

[205] Srov. nález Ústavního soudu ze dne 28. 2. 2017, sp. zn. IV. ÚS 3638/15.

[206] Nález Ústavního soudu ze dne 8. 10. 2019, sp. zn. IV. ÚS 2287/18.

[207] HUSSEINI, Faisal, KOPA, Martin. Čl. 36 [Právo na soudní a jinou právní ochranu]. In: HUSSEINI, Faisal, BARTOŇ, Michal, KOKEŠ, Marian, KOPA, Martin a kol. *Listina základních práv a svobod.* Op. cit., marg. č. 262.

[208] Srov. usnesení Ústavního soudu ze dne 2. 6. 2021, sp. zn. II.ÚS 255/21, a ze dne 24. 8. 2021, sp. zn. IV. ÚS 1547/21, bod 19.

Právo na účinnou právní ochranu při uplatňování unijního práva zaručuje i Listina základních práv EU.[209] Všechny správní úkony by měly podléhat soudnímu přezkumu.[210] Soudní kontrolu administrativních činností členských států lze iniciovat především na základě přímých žalob.[211] Pokud členský stát nesplní povinnosti, jež pro něj vyplývají z unijního práva, může Komise EU či jiný členský stát iniciovat před SDEU řízení pro porušení unijního práva (řízení o porušení Smlouvy, žaloba pro nesplnění povinnosti, či dozorčí žaloba).[212] Může jít o případ, kdy ČR provede nesprávně právní předpis EU, případně neoznámí Komisi EU vnitrostátní právní předpisy, jimiž došlo k provedení právního předpisu EU (např. ČR neprovede požadovaná opatření na zvýšení úrovně bezpečnosti sítí a informačních systémů ve smyslu směrnice NIS). V případě úspěchu žaloby by SDEU určil, které povinnosti byly porušeny a případně nařídil opatření k nápravě protiprávního stavu. Rozsudek je přímo závazný pro vládní, správní i soudní orgány daného členského státu. V případě nesplnění povinností vyplývajících z rozsudku může Komise EU zahájit u SDEU vykonávací řízení s cílem vynutit u členského státu splnění určené povinnosti.[213]

Povinnost nahradit škodu vzniklou z důvodu nesprávné aplikace unijního práva se řadí ke klíčovým principům právního řádu EU. V rámci unijního práva členské státy ručí fyzickým a právnickým osobám za porušení práva EU. Odpovědnost nastává především v případě nedostatečné implementace směrnic, jestliže daná směrnice propůjčuje jednotlivci jasně určitelná práva a existuje příčinná souvislost mezi porušením povinnosti členským státem a vzniklou škodou.[214] Povinnost členských států kompenzovat škody způsobené porušením práva EU je zakotvena i v judikatuře SDEU,[215] přičemž díky zásadě přímého účinku se lze dovolávat práva EU i před vnitrostátními soudy členských států.[216]

---

[209] Srov. čl. 47 a čl. 51 Listiny základních práv EU.

[210] Podrobněji k soudnímu přezkoumávání správních úkonů a evropskému správnímu soudnictví srov. POMAHAČ, Richard, HANDRLICA, Jakub. Op. cit., str. 61 - 62.

[211] Dozorčí žaloba, žaloba na neplatnost, žaloba na nečinnost, služební žaloba, statutární žaloba a tzv. akvilská žaloba. Podrobněji k přímým žalobám srov. např. HENDRYCH, Dušan a kol. Op. cit., str. 751 - 755, KLÍMA, Karel a kol. Op. cit., str. 324 - 326, nebo TOMÁŠEK, Michal, TÝČ, Vladimír, PETRLÍK, David a kol. *Právo Evropské unie*. 3. aktualizované vydání. Praha: Leges, 2021, str. 418 a násl. Ke kontrole a dohledu SDEU srov. např. KLÍMA, Karel a kol. Op. cit., str. 97, 268 - 277. Ke kontrolním pravomocem Komise EU srov. tamtéž str. 316.

[212] Řízení dle čl. 258, resp. v případě žaloby podané jiným členským státem dle čl. 259 Smlouvy o fungování Evropské unie (konsolidované znění), C 202/1, Dokument 12016E/TXT, 1. 3. 2020 (dále jen „SFEU").

[213] Srov. řízení dle čl. 260 SFEU.

[214] Podrobněji viz KLÍMA, Karel a kol. Op. cit., str. 135.

[215] Rozsudek ESD ze dne 19. 11. 1991 ve věci C-6/90 a C-9/90, *Francovitch a Bonifaci*.

[216] Srov. rozsudek ESD ze dne 20. 2. 1979 ve věci C-120/78*, Rewe-Zentral AG proti Bundesmonopolverwaltung für Branntwein*.

1.3.3. Principy práva kybernetické bezpečnosti[217]

1.3.3.1. Technologická neutralita[218]

Technologie skýtají široké spektrum nástrojů i způsobů, které lidé využívají ke změně prostředí, v němž žijí i k přizpůsobení se tomuto prostředí.[219] Neutrální přístup práva k technologiím (na rozdíl od regulace zaměřené na daný typ technologie) vychází z předpokladu, že technologicky neutrální regulace má ve vztahu k novým technologiím delšího trvání i širšího uplatnění. Lze se však setkat i s kritickými názory, jež tvrdí, že technologická neutralita nedosahuje v právu kýžených výsledků. Greensberg vidí hlavní nedostatky v neschopnosti zákonodárce předpovědět míru, v jaké by mělo být právo aplikováno na nové technologie, když mu jsou dosud neznámé, přičemž odkazuje na Hartovu ilustraci interpretačních obtíží právní normy v budoucím světě inovací.[220] S interpretačními obtížemi a neschopností predikce způsobu aplikace právní normy v budoucnu se pojí i zvýšená nejistota, jak bude technologicky neutrální právní úprava aplikována soudy v konkrétních sporech, kde půjde již o konkrétní technologii. Podle Greensberga nelze ani o neutrálním přístupu k technologii hovořit, protože to, co je v daném čase a místě zvoleno za neutrální, závisí na hodnocení zákonodárce.[221] Česká právní úprava kybernetické bezpečnosti činí volbu technologie závislou na hodnocení povinných subjektů, kteří si volí konkrétní typ bezpečnostních technologií.[222] Tím dochází, z pohledu Greensberga, jen k přesunu volby na soukromé subjekty, o neutrální přístup k technologii však nejde.

Princip technologické neutrality má zajistit, aby předmětem právní regulace byly pouze technologické aspekty funkčnosti služeb informační společnosti, ne jejich obsah, což veskrze znamená, že právní regulace kybernetické bezpečnosti nemá vést k regulaci sdílených informací

---

[217] Principy zde uvedené zmiňuje jako klíčové Důvodová zpráva k ZKB.

[218] Text je součástí práce autorky odevzdané v rámci XI. ročníku Studentské vědecké odborné činnosti na Právnické fakultě Univerzity Karlovy. RADEMACHEROVÁ, Kristina. *Principy a východiska kybernetické bezpečnosti de lege lata*. Op. cit., str. 15 - 18.

[219] KOOPS, Bert-Jaap. Ten Dimensions of Technology Regulation - Finding Your Bearings in the Research Space of an Emerging Discipline [online]. In: GOODWIN, Morag E. A. et al. (eds.). *Dimensions of Technology Regulation*. Nijmegen: WLP, 2010. Tilburg Law School Research Paper No. 015/2010, str. 312. Dostupné: https://ssrn.com/abstract=1633985 [Cit. 2022-11-01].

[220] GREENBERG, Brad A. Rethinking Technology Neutrality [online]. *Minnesota Law Review*, č. 100, 2016, str. 1529-1530. Dostupné: https://ssrn.com/abstract=2748932 [Cit. 2022-11-01]. Hart si v roce 1958 kladl základní interpretační otázku, zda se právní pravidlo zakazující vzít *vozidlo* („*vehicle*“) do veřejného parku vztahuje i na jízdní kolo, kolečkové brusle a další (v dnešní době by mohlo být součástí výčtu např. vozítko Segway nebo elektrické koloběžky). Viz HART, Herbert Lionel Adolphus. Positivism and the Separation of Law and Morals. In: *Harvard Law Review*, č. 71, 1958, str. 593–607.

[221] GREENBERG, Brad A. Op. cit., str. 1499.

[222] Srov. § 4 odst. 2 - 5 ZKB.

(obsahu), potažmo k cenzuře. Přístup české právní úpravy kybernetické bezpečnosti je shodný s přístupem EU, která ve virtuálním prostředí odděluje regulaci přenosu dat od regulace obsahu.[223] Princip technologické neutrality má rovněž zajistit nenarušení standardních tržních mechanismů v odvětví ICT.[224] Právní úprava kybernetické bezpečnosti se týká jen regulace přenosu, tj. bezpečného fungování informačních systémů, služeb a sítí pomocí technologií. Volba technologie zajišťující bezpečný přenos dat, a tím i funkčnost služeb informační společnosti, má být odvislá pouze od volby povinných subjektů.[225]

Klíčovým aspektem principu technologické neutrality je nezávislost právní úpravy na konkrétní technologii. ICT mají být neutrální vůči způsobu, jakým jsou používány a právní povinnosti, které ZKB ukládá, ani pravomoci NÚKIB se nesmí týkat obsahu virtuální komunikace. Právní úprava by neměla ani zvýhodňovat jednu technologii před druhou.[226] Zákon však neřeší, co když volbou konkrétní technologie zajišťující bezpečnost dojde k regulaci obsahu přenášených dat, a tím i k narušení principu technologické neutrality. Zákon ani prováděcí předpis se nedotýkají ani problému, jak zajistit, aby nebyly technologie fakticky regulující obsah užívány jako bezpečnostní technologie. V takovém případě nezbude než důsledně trvat na výkladu zákona v souladu s principem technologické neutrality.

Bezpečnostní opatření, jimiž jsou opatření technické a organizační povahy, definuje ZKB v § 5 odst. 2, odst. 3 i prováděcí předpis přijatý v souladu s § 6 ZKB[227] velmi obecně, aby jim bylo možné vyhovět při použití různých technologií.[228] Prováděcí předpis např. v § 21 uvádí požadavky ochrany před škodlivým kódem (malware), aniž by uváděl konkrétní nástroj této ochrany. Bezpečnostní opatření pro poskytovatele digitálních služeb je upřesněno sekundární normotvorbou

---

223 Přenos reguluje např. nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu, směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Obsah upravují např. směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu), či směrnice Evropského parlamentu a Rady 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii.

224 Důvodová zpráva k ZKB, Op. cit., str. 48.

225 Výčet povinných subjektů stanoví § 3 ZKB.

226 POLČÁK, Radim, HARAŠTA, Jakub, STUPKA, Václav. *Právní problémy kybernetické bezpečnosti*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2016, str. 18-23.

227 Vyhláška NÚKIB č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.

228 Důvodová zpráva k ZKB, Op. cit., str. 48.

EU - prováděcím nařízením.[229] Podle směrnice NIS musí povinné subjekty, v souladu s principem technologické neutrality, vyhovět bezpečnostním požadavkům bez ohledu na zvolené technologické řešení, to však musí odpovídat nejnovějšímu technickému vývoji.[230] Princip je výslovně formulován i v čl. 19 odst. 1 směrnice NIS, podle něhož členské státy nesmí vyžadovat používání konkrétního druhu technologie nebo prosazovat jeho užívání diskriminujícím způsobem.

Z hlediska zachování tržních mechanismů lze projev principu technologické neutrality v právní úpravě hodnotit kladně. Obecnost úpravy má však i svá úskalí. Například § 5 ZKB uvádí velmi obecný výčet bezpečnostních opatření, která musí povinné subjekty v nezbytném rozsahu zavést a provádět. Jejich obsah, tj. faktický výčet povinností, stanoví až prováděcí právní předpis. Podle důvodové zprávy jde jen o specifikaci rozsahu a obsahu bezpečnostních opatření,[231] avšak jejich definice v § 5 ZKB je tak obecná, že se nabízí prostor pro úvahu, zda neukládá jednotlivé povinnosti fakticky až podzákonný právní předpis. Ač je praktické zajistit, aby obsah a rozsah bezpečnostních opatření odpovídal nejnovějšímu vývoji ICT, snadné rozšiřování výčtu konkrétních povinností pouhou změnou prováděcího předpisu může být problematické. Nabízí se otázka, na kolik je tato úprava v souladu s čl. 4 odst. 1 Listiny, podle něhož mohou být povinnosti ukládány pouze na základě zákona.[232]

1.3.3.2. Ochrana informačního sebeurčení člověka[233]

O informačním sebeurčení jako o jedné z klíčových hodnot informační společnosti byla zmínka již v předchozí kapitole. Princip zabezpečení informačního sebeurčení člověka tvoří dominantní teleologii české úpravy kybernetické bezpečnosti.[234] Právo na informační sebeurčení garantuje především Listina v čl. 10 odst. 3, která ho řadí mezi základní lidská práva a svobody. Jeho podstatou je úcta k lidské důstojnosti, jež zaručuje každému, aby se v soukromé i sociální sféře svého života rozhodoval, co a v jaké míře bude sdílet jako veřejné informace.

---

[229] Prováděcí nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148, pokud jde o bližší upřesnění prvků, které musí poskytovatelé digitálních služeb zohledňovat při řízení bezpečnostních rizik, jimiž jsou vystaveny sítě a informační systémy, a parametrů pro posuzování toho, zda je dopad incidentu významný. Účinné je od 10. 5. 2018.

[230] Srov. recitály 52 a 53 směrnice NIS.

[231] Důvodová zpráva k ZKB. Op. Cit., str. 56 a 66.

[232] Podrobněji se problémem zabývá tato práce v podkapitole 3.2.1. Bezpečnostní opatření (§§ 4 a 5 ZKB).

[233] Text je součástí práce autorky odevzdané v rámci XI. ročníku Studentské vědecké odborné činnosti na Právnické fakultě Univerzity Karlovy. RADEMACHEROVÁ, Kristina. *Principy a východiska kybernetické bezpečnosti de lege lata*. Op. cit., str. 18 - 21.

[234] Důvodová zpráva k ZKB. Op. Cit., str. 49 a 55.

Právo na informační sebeurčení jako souhrnné pojmenování absolutních informačních práv člověka použil poprvé německý Spolkový ústavní soud[235] v reakci na situace, v nichž se zásahy do informačního sebeurčení začaly projevovat jako systémové selhání se závažnými individuálními i společenskými důsledky. Původně zahrnovalo právo na ochranu soukromí, včetně informací, které soukromí generuje, postupem času posléze docházelo k rozšíření pojetí soukromí člověka o další složky, zejména vytváření a rozvíjení vztahů s dalšími lidmi.[236] Součástí informačního sebeurčení je dnes nejen ochrana soukromí jednotlivce ve virtuálním prostředí, nýbrž i zajištění jeho svobody komunikovat s okolím skrze služby informační společnosti. Na význam práva na přístup k Internetu, umožňujícího komunikaci s ostatními, sdružování, získávání informací i snazší přístup k úřadům, poukázal i Ústavní soud.[237] Právo na informační sebeurčení je v současnosti pochopitelně přiznáno jen člověku. Do budoucna však nelze vyloučit určitý vývoj, který může vést až k přiznání práva na informační sebeurčení i umělým entitám, tj. především právnickým osobám. Obecně lze sledovat trend přisuzování určitých práv, dříve myslitelných jen ve vztahu k člověku, i právnickým osobám. Příkladem je právo na informace o stavu životního prostředí a zejména činnost spolků zabývajících se jeho ochranou. Domnívám se, že v prostředí ICT, kde dochází k rychlému vývoji umělé inteligence a automatizovaných počítačových systémů, můžeme očekávat i rozšiřování kategorie práv právnických osob, potažmo i umělých entit bez právní subjektivity.[238]

Podle Polčáka zahrnuje informační sebeurčení člověka více základních distributivních informačních práv, především právo na ochranu soukromí a osobních údajů, svobodu projevu i svobodu vědeckého bádání, právo na vzdělání, na svobodný přístup k informacím a na přístup ke službám informační společnosti.[239] Ochranu základních práv a svobod přitom považuje za jediný a legitimní smysl a účel kybernetické bezpečnosti.[240] S tímto postojem lze souhlasit, ač se lze tázat, co je na mezinárodní úrovni prvotním hybatelem regulace kybernetické bezpečnosti a spolupráce - zda ochrana základních lidských práv a svobod občanů různých států, anebo rozvoj obchodních vztahů a ochrana před kybernetickými útoky na státní infrastruktury.[241]

---

[235] Nález Spolkového ústavního soudu ze dne 15. 12. 1983, č.j. BVerfGE 65, 1.

[236] Podrobněji POLČÁK, Radim, *Internet a proměny práva*. Op. cit., str. 324-325.

[237] Nález Ústavního soudu ze dne 7. 4. 2010, sp. zn. I. ÚS 22/10.

[238] Srov. např. HALLEVY, Gabriel. *Liability for Crimes Involving Artificial Intelligence Systems*. Springer International Publishing Switzerland, 2015.

[239] POLČÁK, Radim, *Internet a proměny práva*. Op. cit., str. 327.

[240] POLČÁK, Radim, HARAŠTA, Jakub, STUPKA, Václav. Op. cit., str. 19.

[241] Srov. cíle směrnice NIS dle recitálů 1 až 3, či vývoj kybernetické obrany v agendě NATO (srov. níže 2. část této práce).

Možnost realizace informačního sebeurčení v prostředí informačních systémů a sítí v jurisdikci ČR byla zásadní pro přijetí ZKB, který má zabezpečit základní informační kanály, jimiž člověk realizuje právo na informační sebeurčení, proti kybernetickým útokům omezujícím dostupnost služeb informační společnosti. Obsahu práva na informační sebeurčení se ZKB nijak nedotýká a ani záznamy o výskytu a řešení kybernetických bezpečnostních incidentů by neměly umožnit identifikaci jednotlivců či zasáhnout do práva na ochranu soukromí.[242]

Právo na informační sebeurčení se realizuje především skrze fungující služby informační společnosti. Vhodná a přiměřená bezpečnostní opatření musí provádět i poskytovatelé digitálních služeb, přičemž zákonodárce se v tomto ohledu soustředí především na digitální služby klíčové pro elektronické obchodování, vyhledávání informací a cloud computing.[243] Ve vybraných prostředích, která zákonodárce považoval za klíčová pro bezpečnost informací, ZKB stanoví povinnost evidovat kybernetické bezpečnostní události a hlásit kybernetické bezpečnostní incidenty.[244] Evidenční povinnost však závisí na tom, zda bude incident vyhodnocen jako dostatečně závažný, což ji může paralyzovat. Evidence nahlášených incidentů, kterou vede NÚKIB,[245] umožňuje jejich souhrnné vyhodnocení v rámci kyberprostoru, tj. nejen ve vztahu k jednomu subjektu a jeho systému. Následně přijatá opatření by s ohledem na ochranu informačního sebeurčení měla zabezpečit přenos dat při současném zajištění soukromí uživatelů služeb informační společnosti.

1.3.3.3. Ochrana nedistributivních práv[246]

Jedním z principů české právní úpravy kybernetické bezpečnosti je i ochrana nedistributivních práv. Důvodová zpráva připodobňuje právní úpravu k protipožární ochraně, přičemž zákonodárce zdůrazňuje, že necílí ovlivnit obsah informačních služeb a transakcí, nýbrž *„si klade za cíl zabezpečit proti úmyslným nebo nahodilým kybernetickým bezpečnostním incidentům*

---

[242] Důvodová zpráva k ZKB. Op. Cit., str. 5, 18, 49.

[243] Srov. § 4 odst. 3 ve spojení s definicí digitální služby pro účely kybernetické bezpečnosti dle § 2 písm. l) ZKB.

[244] Viz § 8 ZKB. Podle § 7 odst. 2 ZKB je kybernetickým bezpečnostním incidentem *„narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události."*

[245] Srov. § 9 ZKB.

[246] Text je součástí práce autorky odevzdané v rámci XI. ročníku Studentské vědecké odborné činnosti na Právnické fakultě Univerzity Karlovy. RADEMACHEROVÁ, Kristina. *Principy a východiska kybernetické bezpečnosti de lege lata*. Op. cit., str. 21 - 22.

informační kanály, jimiž člověk realizuje své právo na informační sebeurčení a jimiž stát vykonává svá nedistributivní informační práva.“[247]

Smyslem právní úpravy je tedy zabezpečení existence i funkčnosti informačních kanálů, jimiž se realizují práva informačního sebeurčení i nejrůznější služby informační společnosti. Důvodová zpráva výslovně poukazuje na existenci veřejného zájmu na fungování služeb informační společnosti.[248] Zabezpečení veřejného zájmu je jistě vhodné, když právě k jeho uspokojování má směřovat činnost subjektů veřejné správy. Veřejný zájem se stává i kritériem legality, neboť je nutno trvat na tom, aby působnost i pravomoc jednotlivých subjektů veřejné správy byla realizována právě v souladu s veřejným zájmem.[249] Přesto je výslovné konstatování zákonodárce, že na fungování služeb informační společnost je dán veřejný zájem, nešťastné, neboť veřejný zájem má dovodit správní orgán ve vztahu ke konkrétně řešené věci, a to z právní úpravy, aktuální politiky i daných úkolů veřejné správy. Pokud by zákonodárce deklaroval veřejný zájem v konkrétně určené věci přímo v zákoně, jednalo by se podle Ústavního soudu o nepřípustný zásah moci zákonodárné do moci výkonné, jakož i o omezení práva na soudní přezkum. Ačkoli se zde veřejný zájem shledává toliko v důvodové zprávě, nikoli přímo v ZKB, existuje riziko, že správní orgán rezignuje na zjišťování veřejného zájmu v konkrétním případě, neboť se spokojí s konstatováním zákonodárce v důvodové zprávě, na kterou odkáže. Ústavní soud však výslovně uvedl, že *„[v]eřejný zájem v konkrétní věci by měl být zjišťován v průběhu správního řízení na základě poměřování nejrůznějších partikulárních zájmů, po zvážení všech rozporů a připomínek. Z odůvodnění správního rozhodnutí pak musí zřetelně vyplynout, proč veřejný zájem převážil nad řadou jiných partikulárních zájmů. Veřejný zájem je třeba nalézt v procesu rozhodování o určité otázce (typicky např. o vyvlastňování), a nelze jej v konkrétní věci a priori stanovit. Z těchto důvodů je zjišťování veřejného zájmu v konkrétním případě typicky pravomocí moci výkonné, a nikoliv zákonodárné.”*[250]

Ochrana nedistributivních práv v rámci kybernetické bezpečnosti souvisí s jejím pojetím jako veřejného statku. Kybernetická bezpečnost je totiž součástí národní bezpečnosti, která je typickým příkladem veřejného dobra.[251] Podstatu veřejných statků vystihuje Ústavní soud následovně: *„Pro veřejné statky je typické, že prospěch z nich je nedělitelný a lidé nemohou být*

---

[247] Důvodová zpráva k ZKB. Op. Cit., str. 19.

[248] Důvodová zpráva k ZKB. Op. Cit., str. 51.

[249] HENDRYCH, Dušan a kol. Op. cit., str. 82.

[250] Nález Ústavního soudu ze dne 28. 6. 2005, sp. zn. Pl. ÚS 24/04.

[251] Podle Höllandera je národní bezpečnost příkladem veřejného statku. Nález Ústavního soudu ze dne 3. 4. 1996, sp. zn. Pl. ÚS 32/95, odlišné stanovisko Pavla Höllandera.

vyloučeni z jeho požívání. Příklady veřejných statků jsou národní bezpečnost, veřejný pořádek, zdravé životní prostředí. Veřejným statkem se tudíž určitý aspekt lidské existence stává za podmínky, kdy není možno jej pojmově, věcně i právně rozložit na části a tyto přiřadit jednotlivcům jako podíly."[252] Narozdíl od veřejných statků jsou základní lidská práva a svobody tzv. distributivní, neboť je lze konkretizovat a individualizovat, respektive je lze pojmově, věcně i právně členit na části a přiřadit je jednotlivcům.[253] Jelikož bezpečný kyberprostor takto členit nelze, lze jej považovat za veřejný statek a řadit jej mezi nedistributivní práva.

Podstatou chápání nedistributivních práv v kontinentální Evropě je myšlenka, že ačkoli veřejné statky ve svém důsledku směřují taktéž k dobru jednotlivce, nejsou chráněny individuálně, nýbrž kolektivně. Tato ochrana má pak charakter přímé aktivity státu zajišťujícího veřejné dobro. V kontrapozici stojí angloamerické právní pojetí, které chápe veřejné dobro jako klasické distributivní právo, kde však oprávněným subjektem není jednotlivec, nýbrž stát.[254] Podle Polčáka budí dosažení správné míry vyvážení mezi ochranou nedistributivních a distributivních práv, tj. veřejného a soukromého zájmu, často politický konflikt. ZKB však považuje za výjimku, neboť do individuálních práv a svobod zasahuje veřejný zájem (ochrana kybernetické bezpečnosti) jen minimálně. Jako možné omezení uvádí zásah do vlastnického práva u investic do zabezpečení informačních infrastruktur povinných subjektů, nicméně ani zde nejde o podstatný zásah, neboť tyto subjekty obvykle investují do zabezpečení dobrovolně, aby snížily riziko kybernetického útoku a majetkové ztráty.[255] Další možné omezení lze vidět i v zásahu do soukromí a riziku poškození pověsti nebo obchodních zájmů povinných subjektů v případě povinnosti zveřejnit úspěšný kybernetický útok na jejich systém či síť. Podle směrnice NIS je nutné poměřovat mezi zájmem veřejnosti být informován o hrozbách a možným poškozením obchodní pověsti. K tomu účelu by měly existovat neformální a důvěryhodné kanály pro sdílení informací.[256]

Zařazení kybernetické bezpečnosti mezi veřejné statky rozporuje Powell, podle něhož soukromý sektor investuje značné sumy do odvětví bezpečnosti ICT bez ohledu na státní donucení,

---

[252] Nález Ústavního soudu ze dne 3.4. 1996, sp. zn. Pl.ÚS 32/95.

[253] Tamtéž.

[254] Podrobněji POLČÁK, R. *Internet a proměny práva*. Op. cit., str. 342.

[255] POLČÁK, Radim, HARAŠTA, Jakub, STUPKA, Václav. Op. cit., str. 17-18.

[256] Rec. 59 směrnice NIS. Údaje z evidence kybernetických bezpečnostních incidentů, kterou vede NÚKIB, nejsou veřejné. Viz § 9 odst. 3, 4 ZKB.

což by nečinil, pokud by byla kybernetická bezpečnost čistě veřejným statkem.[257] S jeho názorem lze souhlasit jen částečně. Není výhodné předpokládat, že všichni aktéři kyberprostoru budou jednat v souladu s principem *due diligence* a dostatečně zabezpečí své informační a komunikační systémy a sítě. Řada subjektů podílejících se na funkčnosti služeb informační společnosti může být bez potřebných prostředků, případně se rozhodne své prostředky investovat jinde. Mohou přitom poskytovat službu, jejíž narušení může mít významný dopad na základní funkcionality státu. Nelze spoléhat na automatické zabezpečení vlastních informačních systémů a sítí s odůvodněním, že je to ve vlastním zájmů jednotlivých subjektů, neboť i zranitelnost jednotlivých soukromých subjektů v kyberprostoru může mít významné důsledky pro bezpečnost státu.[258]

Princip ochrany nedistributivních práv se v ZKB projevuje ve vymezení kritické informační infrastruktury a v otázce úpravy stavu kybernetického nebezpečí dle § 21 ZKB. Exekutivní reakce k zajištění bezpečného kyberprostoru z podstaty věci nemůže mít povahu přímé akce jako u policejního zásahu.[259] Nabývá tak formy správního rozhodnutí či opatření obecné povahy. Kybernetický bezpečnostní incident řeší NÚKIB pomocí reaktivního opatření ve formě rozhodnutí, proti němuž lze podat rozklad. Týká-li se reaktivní opatření blíže neurčeného okruhu orgánů či osob, vydá se formou opatření obecné povahy, stejně jako ochranná opatření, která reagují na zjištěné nedostatky v zabezpečení.[260]

1.3.3.4. Minimalizace státního donucení[261]

Povinnosti, které ZKB ukládá, nedopadají na koncové uživatele služeb informační společnosti, nýbrž na jejich poskytovatele. Tato osobní příslušnost je projevem fenoménu definičních autorit a odlišuje se od právní úpravy krizového řízení, která počítá s bezprostředním působením vůči všem fyzickým i právnickým osobám.[262]

---

[257] POWELL, Benjamin. *Is Cybersecurity a Public Good? Evidence from the Financial Services Industry* [online]. The Independent Institute Working Paper Number 57, 15. 3. 2005, str. 6 a násl. Dostupné: http://www.independent.org/pdf/working_papers/57_cyber.pdf [Cit. 2022-11-01].

[258] FREDLAND, John S. Building a Better cybersecurity Act: Empowering the Executive Branch Against Cybersecurity Emergencies. *Military Law Review*, 2010, č. 206, str. 4.

[259] POLČÁK, Radim, HARAŠTA, Jakub, STUPKA, Václav. Op. cit., str. 33.

[260] Podrobněji pojednává o jednotlivých opatřeních podkapitola 3.2.2. Opatření v užším slova smyslu (§ 11 ZKB).

[261] Text je součástí práce autorky odevzdané v rámci XI. ročníku Studentské vědecké odborné činnosti na Právnické fakultě Univerzity Karlovy. RADEMACHEROVÁ, Kristina. *Principy a východiska kybernetické bezpečnosti de lege lata*. Op. cit., str. 22-23.

[262] POLČÁK, Radim, HARAŠTA, Jakub, STUPKA, Václav. Op. cit., str. 15-16.

Definiční autority disponují technickými kompetencemi, které jim umožňují přímo a bezprostředně ovlivnit život informační společnosti. Jde zejména o poskytovatele služeb informační společnosti. Podle Lessiga utváří kyberprostor svojí vůlí definiční autority.[263] Mezi ně se řadí mnoho soukromých subjektů vzniklých za účelem vytváření zisku. Definiční autority však shodně jako jiné osoby, které hodlají vytvářet svojí činností zisk, primárně reagují na politické, společenské a právní podmínky uplatňující se na daném trhu. Definiční autority proto neutváří kyberprostor bez jakéhokoli omezení, neboť jejich působení nutně omezuje státní regulace.[264]

V souladu s principem proporcionality se ZKB nezaměřuje na všechny informační systémy a sítě, ale jen na ty se zásadním významem pro bezpečný kyberprostor v jurisdikci ČR. Zákonodárce předpokládal, že se řada subjektů provozujících informační systémy a sítě zapojí do národního systému kybernetické bezpečnosti dobrovolně, vzhledem k možnosti sdílet cenné poznatky o hrozbách či využití metodické pomoci dohledové autority.[265] Metodickou podporu, pomoc a součinnost při výskytu kybernetického bezpečnostního incidentu poskytuje vládní i národní CERT.[266] Z pohledu uživatele služeb informační společnosti ZKB respektuje princip minimalizace státního donucení, neboť uživatele neomezuje ani nenutí plnit žádná bezpečnostní opatření. Princip se projevuje i v povinnosti hlásit až kybernetické bezpečnostní incidenty, nikoli události.[267] Problémem je skutečnost, že bezpečnostní událost jednoho informačního systému, charakterizovaná nízkým stupněm ohrožení na úrovni hrozby, může v jiném systému představovat významný bezpečnostní incident značného dopadu.[268]

K uložení dalších povinností mimo kritickou informační infrastrukturu má dojít pouze při vyhlášení stavu kybernetického nebezpečí. O vyhlášení tohoto stavu rozhoduje ředitel NÚKIB, přičemž jej vyhlásí na dobu nezbytně nutnou, nejdéle však na 7 dnů. Prodloužení stavu kybernetického nebezpečí, a to i opakované, je možné, v souhrnu však doba nesmí přesáhnout 30 dní. Rozhodnutí o vyhlášení stavu kybernetického nebezpečí musí být v souladu s principem

---

[263] LESSIG, L. Op. cit.

[264] Vymahatelnost právních norem a *compliance* definičních autorit s právním řádem daného státu jsou jinými otázkami.

[265] Důvodová zpráva k ZKB. Op. Cit., str. 55.

[266] Srov. § 17 odst. 2 písm. d), resp. § 20 písm. d) ZKB. Název CERT pochází z anglického *Computer Emergency Response Team* a jde o skupinu odpovědnou řídit reakci na kybernetické hrozby. Podrobněji viz 3. část této práce.

[267] Kybernetický bezpečnostní incident je zásadnějšího významu oproti kybernetické bezpečnostní události, neboť jeho definičním znakem je již narušení bezpečnosti informací, služeb, či sítí elektronických komunikací (a jejich integrity). Kybernetická bezpečnostní událost nese pouze potenciál této hrozby. Srov. § 7 odst. 1 a 2 ZKB.

[268] DVOŘÁKOVÁ, Renata, IGNÁCIKOVÁ, Jaroslava. Co lze čekat od zákona o kybernetické bezpečnosti [online]. *IT Systems,* 2014. Dostupné: https://www.systemonline.cz/clanky/co-lze-cekat-od-zakona-o-kyberneticke-bezpecnosti-1.htm [Cit. 2022-11-02].

subsidiarity - tento stav nelze vyhlásit, jestliže NÚKIB může nebezpečí odvrátit jinými zákonnými prostředky.[269]

Co se týče poskytovatelů digitálních služeb, značnou pozornost jim věnuje směrnice NIS. Odůvodněna je vlivem kybernetické bezpečnosti na bezproblémové fungování podniků v EU.[270] Diplomaticky se ovšem zdůrazňuje, že poskytovatelé digitálních služeb by měli podléhat jen mírné reaktivní kontrole, tj. že by orgány státní správy měly zasáhnout až poté, kdy došlo k incidentu, existují-li důkazy, že požadavky směrnice NIS daný poskytovatel nesplňuje.[271] Pravomoc by měl mít ten členský stát EU, v němž je poskytovatel digitální služby usazen, přičemž právní forma jeho struktur (dceřiná společnost či pouhá pobočka) nerozhoduje.[272]

1.3.3.5. Autonomie vůle regulovaných subjektů[273]

Stejně jako princip minimalizace státního donucení se princip autonomie vůle regulovaných subjektů vztahuje k rozsahu a míře ukládaných povinností. ZKB je v tomto ohledu minimalistický, neboť se dotýká jen vybraných orgánů a osob. V souvislosti s očekávaným přijetím nové podoby směrnice NIS lze však počítat s významným nárůstem okruhu povinných subjektů.[274] Princip autonomie vůle se uplatní teprve tehdy, ukládá-li ZKB povinnost. Respekt k autonomii vůle povinných subjektů je projevem liberálního i pragmatického východiska zákona a poskytuje volnost při implementaci bezpečnostních opatření.[275]

Popření principu autonomie vůle by vedlo k nutnosti vymezit různým skupinám osob přesně jejich povinnosti, což by vzhledem k technické povaze regulace kybernetické bezpečnosti učinilo právní úpravu značně rozsáhlou a kazuistickou. Bylo by též obtížné dostát bezpečnostnímu minimu různých subjektů, neboť jejich srovnání není dobře možné; od poskytovatele digitální služby lze

---

[269] § 21 odst. 5 ZKB.

[270] Recitál 48 směrnice NIS.

[271] Recitál 60 směrnice NIS.

[272] Usazení poskytovatele digitální služby v členském státě předpokládá účinný a skutečný výkon činnosti v tomto státě skrze stálé struktury poskytovatele. Viz rec. 64 směrnice NIS.

[273] Text je součástí práce autorky odevzdané v rámci XI. ročníku Studentské vědecké odborné činnosti na Právnické fakultě Univerzity Karlovy. RADEMACHEROVÁ, Kristina. *Principy a východiska kybernetické bezpečnosti de lege lata*. Op. cit., str. 23 - 24.

[274] NÚKIB. *NÚKIB představuje evropskou směrnici NIS2* [online]. 7. 9. 2022. Dostupné: https://www.nukib.cz/cs/infoservis/aktuality/1874-nukib-predstavuje-evropskou-smernici-nis2/ [Cit. 2022-10-15]. Připravované změny představuje NÚKIB rovněž na webu nis2.nukib.cz. [Cit. 2022-10-15]. Podrobněji viz skapitola 2.3. Narušení bezpečnosti informací, služeb a sítí.

[275] POLČÁK, Radim, HARAŠTA, Jakub, STUPKA, Václav. Op. cit., str. 23-24.

důvodně očekávat jiná bezpečnostní opatření než od provozovatele průmyslového a řídícího systému zabezpečujícího základní službu ve státě. Volbu vhodných technických prostředků k zabezpečení ICT systémů a sítí proto ZKB ponechává na regulovaných subjektech. Investice by měly být využity zpravidla hospodárně, neboť ZKB předpokládá jejich použití na zabezpečení infrastruktur na základě potřeb konkrétních povinných subjektů.[276]

Princip autonomie vůle regulovaných subjektů se promítá i do možnosti zapojit se dobrovolně do hlášení kybernetických bezpečnostních incidentů a požádat o součinnost a podporu od národního CERT. Co se týče konkrétních organizačních a technických opatření, ukládá ZKB povinnost provádět je v nezbytném, resp. u poskytovatelů digitálních služeb ve vhodném a přiměřeném rozsahu,[277] nicméně právní úprava neuvádí, co tomuto rozsahu odpovídá. Soulad ponechává na posouzení povinným subjektům jako otázku *compliance*, tj. následné kontroly činnosti ve vztahu k naplnění požadavků ZKB.[278] S tím souvisí i problém zabezpečení informačních systémů a sítí v různých jurisdikcích, pokud se zákonné požadavky států liší. Princip autonomie vůle tak přináší povinným subjektům volnost i odpovědnost spojenou s rizikem vynaložení značných investic do zabezpečení bez jistoty, že vyhoví požadavkům zákona.

1.3.3.6. Bdělost ve vztahu k ostatním státům a k mezinárodnímu společenství[279]

Jako je bezpečnost Internetu ovlivněna zabezpečením jeho uživatelů,[280] je kybernetická bezpečnost závislá na zabezpečení nejslabšího článku, tj. na nejméně zabezpečeném počítačovém systému či síti. Potvrdil to i incident certifikační autority *DigiNotar,* který zmiňuji níže v 1. kapitole 2. části této práce. Powell přirovnal problém zabezpečení informačních infrastruktur soukromými subjekty ke známému vězňovu dilematu. Jestliže se společnost A rozhodne zabezpečit vlastní infrastrukturu proti kybernetickým útokům, bude z jejího kroku těžit i společnost B. Vzhledem k nutným nákladům ovšem nebude žádná chtít učinit první krok. Pokud ale zabezpečí své infrastruktury obě, bude jejich užitek největší. Pokud zabezpečí infrastrukturu jen společnost A,

---

[276] Důvodová zpráva k ZKB. Op. Cit., str. 56.

[277] § 4 odst. 2, odst. 3 ZKB.

[278] POLČÁK, Radim, HARAŠTA, Jakub, STUPKA, Václav. Op. cit., str. 25.

[279] Text je součástí práce autorky odevzdané v rámci XI. ročníku Studentské vědecké odborné činnosti na Právnické fakultě Univerzity Karlovy. RADEMACHEROVÁ, Kristina. *Principy a východiska kybernetické bezpečnosti de lege lata*. Op. cit., str. 24 - 26.

[280] ANDERSON, Ross. Why Information Security is Hard – An Economic Perspective [online]. *Proceedings of the 17th Annual Computer Security Applications Conference*. New Orleans, LA, 2001. Dostupné: https://www.acsac.org/2001/papers/110.pdf [Cit. 2022-11-02].

bude těžit z jejího kroku více společnost B a z pohledu ekonomie budou veškeré benefity zabezpečení vůči subjektu, který je provedl, externalitou. Ve své studii prováděné na sektoru finančních služeb však Powell dospěl k závěru, že náklady zabezpečení jsou vysoce převýšeny vlastním prospěchem ze zabezpečení infrastruktur soukromým subjektům. Státní regulaci považuje za nevhodnou a odrazující od inovací v zabezpečování vlastních infrastruktur.[281]

Nedomnívám se, že je vhodné vztahovat závěry, k nimž Powell dospěl studií sektoru finančních služeb, na celý soukromý sektor. Ne všechna jeho odvětví se zaměřují na tvorbu zisku, ne všechny subjekty mohou investovat do zabezpečení tytéž sumy jako finanční sektor. Přirovnání zabezpečení kyberprostoru k vězňově dilematu, resp. přímo k teorii her[282] je ale velmi podnětné. Nahradíme-li Powellovy obchodní společnosti státy, dospějeme k podobným výsledkům. Státům se vyplatí regulovat povinné subjekty s cílem zvýšit bezpečnost národních informačních a komunikačních infrastruktur tehdy, bude-li zajištěna nejvyšší možná míra jejich spolupráce. Nicméně s ohledem na konkurující bezpečnostně politické zájmy států nebude nikdy možné dosáhnout maximální mezinárodní spolupráce. Vzhledem k pojetí kybernetické bezpečnosti jako veřejného statku by stát přesto měl maximálně zabezpečit vlastní kybernetické prostředí.

Zajištěním bezpečnosti vlastních informačních a komunikačních systémů stát jedná v souladu i s mezinárodním principem *due diligence.* Ten státu ukládá aktivně bránit škodám s možným mezinárodním přesahem. Státy rovněž nesmí připustit zneužití vlastního území k nepřátelským aktivitám vůči jinému státu.[283] Tuto maximu lze vztáhnout i na kyberprostor. Zanedbání řádného zabezpečení kyberprostoru v jurisdikci státu může založit odpovědnost za škodu vůči ostatním státům i vůči mezinárodnímu společenství.

Zabezpečením informačních a komunikačních systémů a sítí ZKB minimalizuje i riziko zneužití infrastruktur ČR ke kybernetickým útokům mimo jurisdikci ČR a s tím spojený vznik odpovědnosti vůči ostatním státům i mezinárodním organizacím.[284] Prokázat, že příčinou škody bylo zanedbání kybernetické bezpečnosti daného státu, je však v kybernetickém prostoru obtížné,[285]

---

[281] POWELL, Benjamin. Op. cit., str. 3-4.

[282] Podrobněji např. OSBORNE, Martin J. *Selected chapters from draft of An Introduction to Game Theory* [online]. Oxford University Press, 2000. Dostupné: https://mathematicalolympiads.files.wordpress.com/2012/08/martin_j-_osborne-an_introduction_to_game_theory-oxford_university_press_usa2003.pdf [Cit. 2022-11-02].

[283] Rozsudek Mezinárodního soudního dvora ze dne 9. 4. 1949, *Corfu Channel Case* (United Kingdom of Great Britain and Northern Ireland v. Albania). Dostupný: http://www.icj-cij.org/en/case/1/judgments [Cit. 2022-11-02].

[284] Důvodová zpráva k ZKB. Op. Cit., str. 56.

[285] Podrobněji např. ROSCINI, Marco. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations [online]. *Texas International Law Journal*, 2015, č. 50, str. 233. Dostupné: https://ssrn.com/abstract=2611753 [Cit. 2022-11-02].

nemluvě o transparentním vyšetření takového incidentu. Jak ukazují níže popsané případy kybernetických incidentů v Nizozemí, Estonsku či Gruzii, vyvodit odpovědnost cizího státu je v případě cíleného útoku takřka nemožné a ve svém výsledku vede spíše ke zvýšení zabezpečení informačních a komunikačních struktur napadeného státu.[286] Skutečnou podstatou uvedeného principu se tak jeví bdělost ve smyslu ostražitosti vůči ostatním státům.

1.4. Působení práva v kyberprostoru

1.4.1. Legitimita práva v kyberprostoru[287]

Právní řády se tradičně vyvíjely v rámci společností, jež se dosud nesetkaly s informačními a výpočetními technologiemi. Právo vychází z tradičního pojetí světa rozděleného hranicemi jednotlivých států na teritoria, v jejichž rámci se právní norma uplatňuje díky společenskému konsenzu i autoritě daného státu a jeho orgánů. Působení právních norem v kyberprostoru je tudíž specifickou záležitostí dotýkající se otázek státní suverenity a nepřípustných zásahů do ní, vymahatelnosti vnitrostátních právních norem mimo státní hranice i efektivnosti a hospodárnosti regulace a výkonu správních činností.

V rámci kyberprostoru vznikají, mění se a zanikají právní vztahy, díky kterým se právo ve společnosti fakticky realizuje.[288] Přesto v počátcích Internetu existovala snaha vymezit se vůči jakýmkoli zásahům z vnější, včetně působení práva, jež bylo vnímáno jako nežádoucí projev státní moci oklešťující svobodný kyberprostor. Debaty o oprávněnosti státních zásahů a regulace kyberprostoru podnítil dokument nazvaný Deklarace nezávislosti kyberprostoru.[289] S odkazem na problematickou kontrolu globálního virtuálního prostředí, budovaného bez zřetele k institutům jako

---

[286] Mezinárodní odpovědnosti státu za kybernetické operace a problému přičitatelnosti se věnuje 4. kapitola 2. části disertační práce.

[287] Text vychází i z rigorózní práce autorky. RADEMACHEROVÁ, Kristina. *Počítačová kriminalita: Vybrané aspekty postihu v mezinárodním prostředí* Op. cit., str. 59 - 63.

[288] POLČÁK, Radim, ŠKOP, Martin, MACEK, Jakub. *Normativní systémy v kyberprostoru: (úvod do studia)*. 1. vyd. Brno: Masarykova univerzita, 2005, str. 11.

[289] Svobodný jedinec v prostředí Internetu, bez možnosti uplatnění zákonodárství jednotlivých států, se stal ústředním motivem Deklarace nezávislosti kyberprostoru americké organizace Electronic Frontier Foundation, založené roku 1990 aktivistou Johnem Perry Barlowem. Organizace se i nyní zabývá podporou svobodného Internetu. Viz BARLOW, John, Perry. *A Declaration of the Independence of Cyberspace* [online]. Electronic Frontier Foundation, 8. 2. 1996. Dostupné: https://www.eff.org/cyberspace-independence [Cit. 2022-11-03].

vlastnictví či právní subjektivita a okolnosti, tato deklarace požadovala totální volnost od jakékoli regulace zvenčí.[290]

Zastánci Deklarace nezávislosti kyberprostoru, a dalo by se říci až anarchistického přístupu k regulaci kyberprostoru, zdůrazňovali především skutečnost, že vztahy v rámci internetového společenství nejsou svázány žádnou myslitelnou společenskou smlouvou[291] a dané společenství je více méně samořídící bez potřeby autoritativní regulace. Poukazovali rovněž na neschopnost států v kyberprostoru prosadit efektivně právo. S nárůstem množství internetových uživatelů i jejich rozmanitosti se však původní úvahy o tom, že případné konflikty lze řešit uvnitř společenství jeho vlastními samoregulačními mechanismy, ukazují přinejmenším jako liché. I v kyberprostoru, zejména v globální počítačové síti Internet, se pohybuje řada jedinců a institucí zvláště zranitelných, ať již z důvodu nedostatečných znalostí, špatného počítačového zabezpečení, anebo například vzhledem k povaze činností představujících klíčové funkce z hlediska veřejné správy. Rezignovat na jakékoli kontrolní mechanismy by znamenalo volit cestu, na níž přežijí ti silnější, což není v moderním státě, který respektuje hodnoty lidství a chrání práva a svobody svých občanů, přípustné. Uvedená možnost se jeví jako nepřijatelná i vzhledem k tomu, že řada událostí odehrávajících se ve virtuálním prostředí se projevuje mimo svět počítačových sítí. Ani argument o nevymahatelnosti (obtížné vymahatelnosti) právní normy v kyberprostoru nemůže být relevantní, neboť by znamenal rezignaci na regulaci v případě její nevynutitelnosti. Ad absurdum by poté nemělo smysl postihovat podvodné jednání v online prostředí jen s odkazem na obtížnost jeho postihu. Těžko by bylo možné přijmout, aby určité jednání bylo protiprávní v offline světě, zatímco v online prostředí by protiprávní nebylo. Vynutitelnost právních norem přitom upravuje vlastními mechanismy samo právo.

Od doby přijetí Deklarace nezávislosti kyberprostoru došlo k vývoji řady právních institutů a odvětví. Právo již běžně zohledňuje nehmotnou podstatu věcí[292] a počítá s kyberprostorem jako s

---

[290] Pro ilustraci lze odkázat na úvodní část Deklarace nezávislosti kyberprostoru: *„Vy, vlády všech průmyslových světů, Vy, unavení obři z masa a oceli. Já, přicházející z Kyberprostoru, nového sídla Mysli, Vás v zájmu budoucnosti vyzývám: Nechte nás být! Nejste mezi námi vítáni. Nemáte žádnou moc nad místy, kde přebýváme. Nemáme vládu ani po žádné netoužíme. Mluvím k Vám tedy z pozice autority ne větší, než jakou má sama Svoboda. Vyhlašuji, že globální společenství, jež budujeme, nezávisí na tyranii a zákazech, kterými jste nás svázali. Nemáte morální právo nás řídit a nemáte ani nástroje, kterých bychom se museli bát... Pojmy Vašeho práva, jako vlastnictví, vyjadřování, subjektivita, pohyb nebo okolnosti, se na nás nevztahují. Všechny jsou založeny na hmotné podstatě a zde žádná hmotná podstata není.“* Pasáž v překladu z publikace: POLČÁK, Radim. Autoritativní regulace kyberprostoru a legitimita trestního práva. Op. cit., str. 19.

[291] K teorii společenské smlouvy srov. např. HOBBES, Thomas, CHOTAŠ, Jiří, MASOPUST, Zdeněk, BARABAS, Marina (eds.). *Leviathan, aneb, Látka, forma a moc státu církevního a politického*. 1. vyd. Překlad Karel Berka. Praha: OIKOYMENH, 2009.

[292] Srov. § 489 občanského zákoníku, podle něhož je věcí v právním smyslu vše, co je rozdílné od osoby a slouží potřebě lidí, a § 496 odst. 2 občanského zákoníku, podle kterého jsou nehmotné věci práva, jejichž povaha to připouští, a jiné věci bez hmotné podstaty.

prostředím, v němž se rovněž uplatní,[293] a to včetně odpovědnosti za protiprávní jednání.[294] Ani námitka o neexistenci společenské smlouvy neobstojí, neboť internetoví uživatelé a subjekty operující v kyberprostoru přísluší k různým společenstvím zároveň - vedle internetového společenství jsou i občany státu, případně jsou v určitém státě usazeny jako právnické osoby. Státní moc daného státu musí respektovat a dodržovat právní normy i vně státních hranic.

Specifika kybernetického prostředí proto automaticky nevedou k negaci práva. Takový přístup by ve své podstatě mohl znamenat i odepření spravedlnosti a porušení principu *denegatio iustitiae*.[295] Lze se proto ztotožnit s názorem, podle něhož *„mezinárodní transakce v kyberprostoru se nijak neliší od těch, které známe z „reálného" prostředí. Zahrnují jednotlivce umístěné v určitém prostoru pod jurisdikcí nějakého státu, kteří komunikují, ať už s dobrým nebo špatným efektem, s jinými jednotlivci rovněž umístěnými v reálném prostoru pod jurisdikcemi jiných států. Nenacházíme řádné normativní argumenty, které by podporovaly imunizaci kyberprostoru od klasické teritoriální regulace. A máme všechny důvody se domnívat, že státy mohou vykonávat svou autoritu na klasické teritoriální bázi a dostatečně regulovat transakce v kyberprostoru."*[296]

Krátce po rozšíření Internetu mezi podstatnou část počítačových uživatelů světa se původní ideje seberegulujícího se svobodného společenství, které vytváří a sdílí informace bez zásahů státní moci, střetly s pokusy států o zamezení šíření nelegálního obsahu; příležitosti pro omezování práv a svobod druhých spolu s širokým spektrem kriminálních příležitostí se stávají stejnou hrozbou virtuálního společenství jako jakéhokoli jiného lidského společenství a dokazují, že bez určité regulace zvenčí může být kyberprostor pro mnohé uživatele nebezpečný.[297]

---

[293] Např. NATO rozšířilo svoji působnost i na doménu kyberprostoru v roce 2016 s odůvodněním významné role, kterou kyberprostor hraje v moderních bezpečnostních konfliktech. NATO. *NATO Summit Guide, Warsaw 2016*, Op. cit., str. 128.

[294] Viz zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů, ve znění pozdějších předpisů, upravující odpovědnost poskytovatelů služeb informační společnosti.

[295] K tomu srov. např. rozsudek Nejvyššího soudu ze dne 16. 1. 2001, sp. zn. 4 Tz 265/2000, jímž soud vyhověl stížnosti pro porušení zákona, podané proti usnesení o odložení trestního stíhání, s odkazem na nemožnost prokázat spáchání trestného činu pomluvy dle § 184 TZ v prostředí internetového fóra.

[296] GOLDSMITH, Jack L. Against Cyberanarchy. *The University of Chicago Law Review*. Chicago, Ill: University of Chicago Law School, 1998, 65(4), str. 1199 an. Překlad úryvku podle: POLČÁK, Radim. *Internet a proměny práva*. Op. cit., str. 72 – 73.

[297] RAMEŠOVÁ, Kristina. Kyberprostor a projevy moci výkonné, aneb nenápadné vytěžení vlivu definičních autorit. In: TRYZNA, Jan (ed.). *Dělba moci a její proměny*. Praha: Auditorium, 2019, str. 31.

1.4.2. Vymahatelnost právních norem v kyberprostoru

Faktická vynutitelnost (vymahatelnost) právních norem v kyberprostoru je problematická. Důvodem jsou charakteristiky vlastní kybernetickému prostředí, zejména možnost vzdálených interakcí a globální charakter sítí. Polčák upozorňuje, že *„teoretická formální platnost hmotného práva je postavena proti fakticitě ovlivněné kromě institucionálního fenoménu poskytovatelů služeb informační společnosti též problémy souvisejícími s globalitou informační sítě a suverenitou národních jurisdikcí.“*[298]

Problematika suverenity státu nad jeho vlastním územím a přípustné zásahy jsou řešeny na poli mezinárodního práva zpravidla smluvně, byť se lze setkat i s názorem poukazujícím na možnou existenci obyčeje.[299] Problém však může nastat, pokud cizí stát odmítne spolupracovat při vyšetřování kybernetického incidentu či protiprávního činu. Poukázat lze příkladem na kybernetické útoky na webové stránky estonských vládních institucí skrze zahlcení nadměrnými příkazy zvenčí (tzv. *Distributed Denial of Service Attack*, neboli DDoS útok), jež se odehrály v květnu 2007. Tehdy se útočníci prohlásili za příslušníky Ruské federace. Část útoků byla vedena z ruských IP adres včetně těch, které příslušely ruským státním institucím. Útok se odehrál v souvislosti s politickým konfliktem obestírajícím odstranění ruského válečného památníku z centra Tallinnu dne 9. května, tedy v den, kdy Ruská federace slaví vítězství v Druhé světové válce, přičemž samotný útok vyžadoval prostředky, jež nebyly běžné populaci dostupné. Ruská federace odmítla spolupracovat s Estonskem při nalezení pachatelů útoků. Ruská prokuratura odmítla estonskou žádost o mezinárodní vyšetřování, byť byla podána na základě dvoustranné mezinárodní smlouvy o vzájemné právní pomoci uzavřené mezi Ruskou federací a Estonskem.[300]

Estonský příklad ukazuje, že vymahatelnost právních norem v kyberprostoru bývá znemožněna neschopností patřičně vyšetřit konkrétní kybernetický incident a nashromáždit důkazy potřebné k potrestání pachatelů a uplatnění nároků na náhradu škody. Problém se týká jak protiprávních činů namířených vůči jednotlivci ve snaze získat materiální prospěch (zneužití osobních údajů, nejrůznější podvodná jednání, vydírání atp.), tak i kybernetických útoků vůči

---

[298] POLČÁK, Radim. *Internet a proměny práva*. Op. cit., str. 14.

[299] SEITZ, Nicolai. Transborder Search: A New Perspective in Law Enforcement? [online]. *Yale Journal of Law and Technology,* 2005, 7(1). Dostupné: http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1016&context=yjolt [Cit. 2022-11-03].

[300] ROSCINI, Marco. Op. cit., str. 234-235.

vlastním i cizím státním institucím,[301] za nimiž jsou především politické motivy, a které mohou cílit i na kritickou státní infrastrukturu a tíživě dopadnout na obyvatele státu.

1.4.3. Regulace kyberprostoru jinou než právní normou

Jak bylo shora nastíněno, v počátcích Internetu se objevovala myšlenka odmítající regulaci s ohledem na existenci společenství (uživatelský substrát) i vzhledem ke specifickým pravidlům, jimiž se dané společenství řídí. Jednalo se o odkaz na technickou podstatu virtuálního světa, který je založen a funguje díky neprávním pravidlům. Slovy amerického konstitucionalisty Lawrence Lessiga[302] jde o kód upravující lidské chování v kyberprostoru. Kódem označuje jakoukoli formu technických pravidel (počítačový program, parametry prostředí, formáty dat, přenosové protokoly atd.), na jejímž základě funguje informační infrastruktura.[303] Kód tvoří ti, kteří mohou definovat v kyberprostoru určité prostředí, tedy definiční autority, a jimi vytvořený kód se stává definiční normou (normou *sui generis*).[304] Podstatná část řídícího kódu je vytvářena těmi, kdo určují technický způsob zpracování dat, což jsou především poskytovatelé služeb informační společnosti.[305] Síla kódu spočívá v jeho efektivitě a neovlivnitelnosti. Lessig jej přirovnává k přírodním zákonům. Kód definuje nové prostředí a utváří požadované chování, nelze jednat proti němu, neboť to není (technicky) možné, respektive jen málokdo zná způsob, jak technické pravidlo změnit ve svůj prospěch či jej obejít (hackeři). Právo samozřejmě takto efektivní není a s určitým zjednodušením lze říci, že právní norma je narozdíl od kódu popisná, nikoli děj utvářející.

Abelovský zdůrazňuje vliv technologie na chování subjektů v rámci kyberprostoru nejen skrze formování chápání příkazů a zákazů, ale i hodnotových otázek v právu. Limitů programovacího jazyka a kódování hodnot se dotýká na příkladu počítačové automatizace soudního rozhodování, neboť *„[a]ni ten najlepší algoritmus umelej inteligencie nie je schopný rozlíšiť v čase rozhodnutia, ktoré preferencie určitých hodnôt sú na úkor iných hodnôt správne alebo*

---

[301] Přičitatelnosti kyberútoků cizímu státu a uplatnění náhrady újmy se věnuje tato práce v kapitole 2.4. Kybernetické operace a mezinárodní odpovědnost státu.

[302] Lawrence Lessig staví normativitu kyberprostoru na vlastní teorii kódování. V rámci regulativů lidského chování zmiňuje právo, sociální normy a kód. LESSIG, Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999.

[303] Podrobněji též POLČÁK, Radim. *Internet a proměny práva*. Op. cit., str. 188.

[304] Definiční normy vytváří blogeři, autoři nejrůznějších webových stránek, mobilních či internetových aplikací, uživatelé programů v jejich rámci, mohou-li měnit nastavení programu, telekomunikační operátoři, apod. Podrobněji POLČÁK, Radim. *Právo na internetu: spam a odpovědnost ISP*. 1. vyd. Brno: Computer Press, 2007, str. 88 a násl.

[305] POLČÁK, Radim. *Internet a proměny práva.* Op. cit., str. 107 a násl.

nesprávne."[306] Za účelem rozhodování případů, na něž konkrétní norma nedopadá, s cílem dostát principu zakazujícímu *denegatio iustitiae*, tj. odepření spravedlnosti, by algoritmus musel využít metodu umělé inteligence. Díky zakódování hodnot (co je dobré a co špatné) by posléze algoritmus přišel s novým řešením. Abelovský přitom však upozorňuje na nebezpečnou relativizaci hodnot při jejich definování a kódování.[307]

Obdobné riziko spočívající v neschopnosti počítače rozlišit hodnotovou otázku a zvolit vhodné řešení může vyvstat i v případě technických norem, pokud by bez dalšího regulovaly kyberprostor. Problematické by bylo rovněž prvotní zakódování hodnot, neboť by se odvíjelo od konkrétních hodnotových hledisek určité definiční autority. Výsledný kód by posléze mohl vést k neférové regulaci a nespravedlivému řešení konkrétních situací. V případě technické normy či kódu definujícího virtuální prostředí bude proto vždy nutné ptát se, kdo stojí za jeho vznikem a jaké hodnotové principy zastává. Obecné nahrazení právní normy kódem se proto nejeví jako vhodné ani pro virtuální prostředí. Komplikovanost snah regulovat virtuální prostředí vystihl i Lawrence Lessig, když nakonec dospěl k závěru, že státní moc, jakkoli se může stát záhubou svobod kyberprostoru, je zároveň k jejich ochraně nezbytná.[308]

1.4.4. Úloha definičních autorit při výkonu státní moci na Internetu[309]

Státní moc, ať již výkonná, zákonodárná či soudní, působí v prostředí Internetu skrze definiční autority spadající pod její jurisdikci, kterým na základě zákona ukládá určité povinnosti. Pojem definičních autorit vysvětluji v předchozí kapitole. Definiční autority představují zejména poskytovatelé nejrůznějších služeb informační společnosti, kteří disponují technickými kompetencemi a schopnostmi bezprostředně ovlivňovat život společnosti informačním kódem.[310] Definiční autority nicméně podléhají, zpravidla skrze místo svého sídla, právnímu řádu konkrétního státu. Nejsou tak ve své kybernetické normotvorbě zcela neomezené.

Jeden z prvních pokusů o regulaci definičních autorit lze spatřit v zákoně přijatém v roce 1994 na půdě amerického Kongresu, který zajistil a upravil možnost orgánů činných v trestním

---

[306] ABELOVSKÝ, Tomáš. Počítač ako sudca [online]. *Revue pro právo a technologie,* 2016, č. 14, str. 34 - 35. Dostupné: https://journals.muni.cz/revue/article/view/6119 [Cit. 2022-11-03].

[307] Tamtéž, str. 36.

[308] LESSIG, Lawrence. *Code. Version 2.0.* Op. cit.

[309] Tato část disertační práce byla publikována v rámci kapitoly monografie: RAMEŠOVÁ, Kristina. Kyberprostor a projevy moci výkonné, aneb nenápadné vytěžení vlivu definičních autorit. In: TRYZNA, Jan (ed.). *Dělba moci a její proměny*. Praha: Auditorium, 2019, str. 32 - 36.

[310] POLČÁK, Radim. *Internet a proměny práva.* Op. cit., str. 102.

řízení provádět po síti skryté sledování.[311] Myšlenka, že se s regulací virtuálního prostředí setkáváme až v posledních letech, je proto lichá: snahy podrobit virtuální prostředí kontrole státní moci existují v podstatě od jeho počátku. Státní moc, chce-li regulovat efektivně, se však musí vydat cestou regulace technologie sítě a uložením povinností subjektům, které vykonávají nad určitými částmi virtuálního prostředí faktickou kontrolu, tj. definičním autoritám. Ani tato myšlenka není ničím novým, neboť již v roce 1999 představili Lessig a Resnick model právní regulace virtuálního prostředí, který měl zajistit lepší vymahatelnost právních norem.[312]Ačkoli se zabývali omezením šíření škodlivého obsahu po síti, jejich model je poplatný i obecné regulaci nežádoucího chování ve virtuálním prostředí. Jelikož Lessig a Resnick rozdělují jednotlivé aktéry ve virtuálním prostředí na odesílatele, příjemce a zprostředkovatele výměny informací, soustředí se na vymahatelnost práva právě u těchto subjektů. Dochází přitom k závěru, že zatímco příjemců informací je ve virtuálním prostředí mnohem více než odesílatelů informací, tak se odesílatelé často nachází mimo jurisdikci státu snažícího se prosadit danou právní normu, a tudíž jsou právními prostředky prakticky neregulovatelní. Mnohem snazší a levnější cestou se proto jeví regulovat příjemce informací, potažmo zprostředkovatele jejich výměny, kteří se nachází většinou v dosahu jurisdikce konkrétního státu.[313]

Poskytovatelé služeb informační společnosti mohou skrze definiční normu regulovat jimi ovládanou část kybernetického prostředí a ukládat povinnosti bez ohledu na státní moc; často se tak děje skrze smluvní podmínky, s nimiž uživatel služby musí před jejím použitím projevit souhlas. Legitimity autoritativního výkonu moci ze strany definičních autorit jako subjektů, v jejichž schopnostech je vymáhat ve virtuálním prostředí státem upravená práva a povinnosti, se dotýká Kasl v rozboru konceptu tzv. *blockchainu*, decentralizované kryptograficky podložené databáze záznamů.[314] Čím dál větší část výkonu státní moci nad online prostředím je podle něj delegována na definiční autority z různých oblastí kyberprostoru, s cílem dosáhnout vyšší vymahatelnosti práva. Státem požadovaný způsob jednání ve virtuálním prostředí je zajišťován zejména díky rozšiřování (spolu)odpovědnosti definičních autorit za protiprávní jednání, k němuž dochází v online prostředí pod jejich faktickou kontrolou. Důvodem je podle Kasla skutečnost, že definiční autority mají *„na*

---

311 Zákon nesl název The Communication Assistance for Law Enforcement Act, neboli CALEA. LESSIG, Lawrence. Op. cit., str. 63.

312 LESSIG, Lawrence, RESNICK, Paul. Zoning Speech on the Internet: A Legal and Technical Model [online]. *Michigan law review*. Ann Arbor: University of Michigan Law School, 1999, 98(2). Dostupné: https://cyber.harvard.edu/wg_home/uploads/200/1999-06.pdf [Cit. 2022-11-06].

313 Tamtéž, str. 424.

314 KASL, František. Blockchain, společenská smlouva digitálního věku? [online]. *Revue pro právo a technologie*, 2018, č. 17, str. 3–8. Dostupné: https://journals.muni.cz/revue/article/view/8922 [Cit. 2022-11-06].

rozdíl od státu ve vymezeném rozsahu své působnosti reálný dosah na přenos, vytváření, ukládání a zpracovávání informací na internetu a ze své zásadně soukromoprávní povahy mohou účinněji reagovat, neboť nejsou limitovány enumerativností veřejnoprávních pretenzí.“[315]

V současné podobě tedy dochází k tomu, že nad dodržováním práv a povinností na konkrétní webové platformě fakticky bdí daný poskytovatel služby informační společnosti, který po uživatelích vyžaduje dodržování smluvních podmínek, a do určité míry spoluodpovídá za dodržování právního řádu na webové platformě.[316] Jakékoli omezení uživatele služby informační společnosti se však děje v režimu soukromoprávního vztahu, tj. na bázi dodržování smluvních podmínek. V případě porušení smluvních podmínek se však poskytovatel služby stává pro daný moment i soudcem (hodnotí, zda uživatel porušil podmínky) a vykonavatelem práva (může uživateli odepřít přístup ke službě). Ačkoli samozřejmě existují prostředky ochrany vůči takovému postupu definičních autorit, pravděpodobnost jejich využití je vzhledem k počtu uživatelů služby informační společnosti a počtu definičních autorit spíše menší. Postavení definičních autorit je tak fakticky silnější a do určité míry může připomínat i pozici orgánu jednostranně rozhodujícího o právech a povinnostech nepodřízených subjektů, byť definiční autority nejsou, a bez zákonného zmocnění ani nemohou být, orgány veřejné moci.

V okamžiku, kdy by zákon ve vztahu k informacím (datům) šířeným skrze Internet plošně přesunul určité pravomoci (typicky kontrolní) na definiční autority, bylo by nutné podrobit je státní kontrole. Z pozice osob soukromého práva by totiž definiční autority byly oprávněny spravovat část veřejně přístupného kybernetického prostředí, kterou by fakticky ovládaly. Vedle smluvních podmínek by vynucovaly dodržování právních norem státu a jejich činnost by odpovídala činnosti nestátního orgánu vykonávajícího přenesenou státní správu. K takovému přesunu pravomocí však nemůže dojít jinak, než na základě zákona, neboť pouze státu a osobám, o nichž tak stanoví ústava nebo zákon, lze přičítat právo být nositelem veřejné správy spolu s právy a povinnostmi, které s tím souvisejí.[317]

Kontrolou výkonu veřejné správy na Internetu a regulací odpovědnosti definičních autorit jako nositelů veřejné správy by sice bylo možné řešit případné nezákonné zásahy do práv a svobod uživatelů, avšak stalo by se tak se současným přispěním k centralizaci státní moci na Internetu. Definiční autority, které by byly subjektem veřejné správy, by totiž nutně musely být podřízeny

---

[315] Tamtéž, str. 8.

[316] Omezení odpovědnosti poskytovatelů určitých typových služeb informační společnosti řeší směrnice o elektronickém obchodu.

[317] HENDRYCH, Dušan a kol. Op. cit., str. 96.

dozorujícímu orgánu a splňovat určitá předem stanovená kritéria (být nositelem licence apod.), čímž by jednoznačně došlo k vychýlení kontroly Internetu ve prospěch moci výkonné. Nabízí se poté otázka, zda by tato státní kontrola nebyla snadno zneužitelná k cenzuře nebo k ovlivnění svobodné soutěže politických stran. S ohledem na globální charakter Internetu by rovněž s nejvyšší pravděpodobností vedla k usídlení definičních autorit na území států s příznivějšími podmínkami pro jejich působení.

Žádný subjekt veřejného nebo soukromého práva, v jehož výlučné pravomoci by bylo dohlížet na dodržování právních norem v prostředí Internetu, případně v kyberprostoru, a spravovat jej, dosud neexistuje. ČR není výjimkou. Idea jediného orgánu či instituce s pravomocí bdít nad stavem virtuálního prostředí je v našich kulturních podmínkách těžko představitelná. S ohledem na globální charakter virtuálního prostředí, které nezná státních hranic a jež bylo navrženo způsobem, aby co nejlépe odolalo nejrůznějším cenzurním snahám, by byla jednotná kontrola virtuálního prostředí i těžko technicky dosažitelná.[318] Na Internetu se nicméně najdou sektory, které jsou do značné míry dotčeny právě působením moci výkonné. Ačkoli zákon nesvěřuje definičním autoritám žádnou pravomoc k výkonu veřejné správy a ani jim taková pravomoc nebyla svěřena na základě zákona, definiční autority fakticky disponují v konkrétní oblasti Internetu, kde vykonávají svůj vliv, určitým typem autoritativní moci ve vztahu k běžným uživatelům Internetu. Technické kompetence a faktické možnosti definičních autorit v určitém sektoru využívá zákonodárce stanovením povinností právě definičním autoritám, skrze něž do značné míry zabezpečuje správu, zejména kontrolu obsahu Internetu.

Jde o sektory, v nichž je patrná snaha zákonodárce chránit veřejný zájem, přičemž okolnost, zda by k jeho ohrožení či porušení mohlo dojít ve virtuálním prostředí nebo mimo něj, je irelevantní. Orgán státní moci, obvykle ústřední správní úřad, v takovém případě zajišťuje správní dozor, tj. srovnává chování nepodřízených subjektů ve virtuálním prostředí a porovnává jej s požadavky právních norem, a následně případně aplikuje nápravné nebo sankční prostředky.[319] Takto je i na Internetu patrný výkon státní správy ze strany ústředních správních orgánů například na poli ochrany osobních údajů, ochrany spotřebitele, ve vztahu k minimalizaci negativních účinků

---

[318] Přesto se najdou státy, které Internet podrobují svojí výlučné kontrole. Činí tak skrze omezení volného přístupu k síti, blokaci webových stránek a kontrolu aplikací, které budou občanům dostupné. Příkladem je vládní cenzura virtuálního obsahu, k němuž mají přístup uživatelé Internetu v Čínské lidové republice. Viz YOUNG, Xu. *Deconstructing the Great Firewall of China* [online]. ThousandEyes Blog, 8. 3. 2016. Dostupné: https://www.thousandeyes.com/blog/deconstructing-great-firewall-china [Cit. 2022-11-06]. BRADSHER, Keith. *China Blocks WhatsApp, Broadening Online Censorship* [online]. The New York Times, 25. 9. 2017. Dostupné: https://www.nytimes.com/2017/09/25/business/china-whatsapp-blocked.html [Cit. 2022-11-06].

[319] STAŠA, Josef. Kapitola XIII. Správní dozor. In: HENDRYCH, Dušan a kol. Op. cit., str. 283.

hazardních her, anebo při zajištění bezpečnosti státu a dostupnosti některých klíčových služeb veřejnosti.

Podle § 2 odst. 2 správního řádu smí správní orgán uplatňovat svou pravomoc pouze k těm účelům, k nimž mu byla zákonem nebo na základě zákona svěřena, a v rozsahu, v jakém mu byla svěřena. Uvedená maxima je vyjádřením zákazu zneužití pravomoci a základní zásadou činnosti správních orgánů. Princip zákazu zneužití pravomoci vychází z čl. 1 odst. 1 Ústavy České republiky a lze jej chápat jako obecný zákaz zneužití práva,[320] neboť uplatňuje-li správní orgán pravomoc mimo zákonný mantinel, jde o rozpor se zákonem. Správní orgán musí respektovat konkrétní účel, k němuž mu byla pravomoc svěřena (ochrana základního práva či ústavně aprobované hodnoty) a uplatňovat ji pouze k tomuto účelu, byť by jí mohl uplatnit i k jinému ospravedlnitelnému účelu.[321] Zejména v oblasti správního dozoru může zákon propůjčit pravomoc i právnickým a fyzickým osobám soukromého práva. Typickým příkladem jsou tzv. veřejné stráže, které působí na poli ochrany různých složek životního prostředí a zákon jim svěřuje řadu vrchnostenských oprávnění.[322] Zapojení definičních autorit by na první pohled mohlo roli veřejných stráží připomínat, definiční autority však, až na příklad autorizace soukromé osoby k výkonu veřejné správy v oblasti kybernetické bezpečnosti,[323] nejsou dosud vykonavateli státní správy a porušení právních norem uživateli Internetu nejsou oprávněny sankcionovat. Jejich roli a spolupráci s orgánem moci výkonné, zejména při kontrole dodržování právních norem na Internetu, tudíž lze charakterizovat především skrze odpovědnostní vztah.[324]

1.4.5. Suverenita, jurisdikce a kyberprostor

V rámci moci výkonné je veřejná správa vykonávána v rozsahu působnosti jednotlivých správních úřadů či orgánů díky pravomoci autoritativně rozhodovat o právech a povinnostech nepodřízených subjektů, které nejsou v rovnoprávném postavení se správními orgány a rozhodnutí

---

320 Nález Ústavního soudu ze dne 13. 8. 2002, sp. zn. Pl. ÚS 3/02.

321 SVOBODA, Petr. *Právo na spravedlivý proces a české správní řízení*. Praha: Univerzita Karlova v Praze. Dizertační práce, 2006, str. 32.

322 Srov. např. oprávnění myslivecké stráže dle § 14 zákona č. 449/2001Sb., o myslivosti, ve znění pozdějších předpisů. Blíže STAŠA, Josef. Op. cit., str. 284.

323 Národním CERT (*Computer Emergency Response Team*) je v současnosti zájmové sdružení právnických osob CZ.NIC, které rovněž plní roli týmu CSIRT.CZ (*Computer Security Incident Response Team*). Podmínky výběru provozovatele národního CERT stanoví § 18 ZKB. Podrobněji srov. níže subkapitolu 3.3. Computer Emergency Response Team (CERT).

324 K modelu odpovědnostního vztahu na příkladu regulace online hazardních her viz RAMEŠOVÁ, Kristina. Kyberprostor a projevy moci výkonné, aneb nenápadné vytěžení vlivu definičních autorit. Op. cit., str. 38-41.

jim učiněné nezávisí na jejich vůli. Pravomoc je obecně vykonávána především skrze vydávání nařízení a jiných abstraktních správních aktů, opatření obecné povahy, konkrétních správních aktů, jakož i skrze výkon rozhodnutí, správní dozor či uzavírání veřejnoprávních smluv.[325] Tuto pravomoc musí být správní orgány a úřady schopny uskutečňovat i tehdy, dotýká-li se výkon jejich působnosti virtuálního prostředí. Nejde přitom pouze o problematiku zajištění kybernetické bezpečnosti jako takovou, ale i o další oblasti veřejné správy (viz proměny spojené s digitální revolucí popsané shora).

Lze též říci, že kybernetická bezpečnost sama o sobě je jedním z předpokladů nerušeného výkonu veřejné správy ve všech jejích oblastech. Zákon o kybernetické bezpečnosti přímo upravuje reaktivní a ochranná opatření (§§ 13 a 14), která mohou nabývat podoby individuálního správního aktu (rozhodnutí) i opatření obecné povahy, týká-li se úkon požadovaný k zajištění kybernetické bezpečnosti blíže neurčeného okruhu orgánů nebo osob. Individuálním správním aktem je dále například rozhodnutí o povinnosti předat data (§ 15a), o určení provozovatele základní služby a informačního systému základní služby (§ 22a), či o uložení správního trestu za nedodržení povinností stanovených ZKB a zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „zákon o ochraně utajovaných informací"). Správní dozor upravuje ZKB v Hlavě V. a zmocnění k uzavírání subordinačních veřejnoprávních smluv v § 19. Abstraktními správními akty na poli kybernetické bezpečnosti jsou například nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, či vyhláška NÚKIB č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci.

S průnikem ICT do správy věcí veřejných vyvstává otázka, do jaké míry lze zajistit efektivní výkon veřejné správy ve vztahu k virtuálnímu prostoru, který nezná hranic, zejména je-li třeba respektovat svrchovanost ostatních států a přitom zajistit v rámci ČR nerušený výkon veřejné správy. Podle dostupné zprávy skupiny pro spolupráci ustanovené směrnicí NIS měla desetina všech hlášených kybernetických incidentů v roce 2019 přeshraniční dopad ve vztahu k ostatním členským státům EU, přičemž nejvíce byl postižen bankovní a zdravotní sektor.[326] Lze si představit situaci, v níž bude cizí stát odmítat součinnost nutnou k výkonu správního aktu či zajištění správního dozoru, popřípadě v níž vyvstanou jurisdikční konflikty mezi dvěma či více státy. Správní právo, jež má umožnit efektivní správu veřejných záležitostí i v podmínkách různých

[325] HENDRYCH, Dušan a kol. Op. cit., str. 112.

[326] NIS COOPERATION GROUP. Op. cit., str. 3.

ústavních systémů, by mělo zajistit funkční výkon pravomoci správních orgánů v co nejvyšší míře.[327]

Čím dál častěji dochází k útokům, jež se odehrávají v prostoru tvořeném počítačovými sítěmi a jejich jednotlivými prvky, tj. jinými sítěmi, podsítěmi, jakož i jakýmikoli zařízeními, která mají přidělenu vlastní IP adresu. Kybernetické hrozby přitom pochází nejen od útočníků motivovaných finančními zisky (typicky v případě tzv. ransomware, kdy dochází k napadení informačního systému a zablokování jeho důležitých funkcí či dat s požadavkem na zaplacení vysokých částek pro obnovení jeho funkčnosti). Útoky pochází i od jiných států, jejichž pohnutky jsou politické a strategické. Státy přitom ve stále větší míře využívají kybernetických nástrojů k posílení svých geopolitických pozic, přičemž dochází i k zasahování do vnitřních demokratických procesů cizích států.[328] Současně mohou mít kybernetické útoky značné ekonomické důsledky a být prostředkem k úmyslnému poškození či narušení provozu sítí a informačních systémů, a způsobit tak značnou újmu státnímu hospodářství.[329] V zájmu států je tedy zabezpečit sítě a informační systémy proti útokům státních i nestátních subjektů, a zajistit tím nerušený výkon veřejné správy.

1.4.5.1. Suverenita státu

Nezávislost státní moci vůči jakékoli jiné moci v rámci vnitřních i vnějších vztahů státu je projevem státní suverenity. Jde o základní pojem mezinárodního práva, jehož součástí je i mezinárodněprávní subjektivita státu. Podle Šturmy *„[p]okud stát, definovaný státovědou i teorií mezinárodního práva jako veřejná moc ovládající státní území a na něm usazené osoby (obyvatelstvo státu), nemá nad sebou nikoho vyššího, nazývá se takový stát suverénní. Suverenita státu však není absolutní, protože i takový stát je ve své nezávislosti omezen suverénními právy jiných států, obecným mezinárodním právem a svobodně převzatými mezinárodními závazky."*[330]

Státní suverenita je tradičně chápána zejména ve vztahu k určitému území. S tímto územím suverénní stát navenek nezávisle disponuje a ve vztahu k němu nezávisle a výlučně vykonává i veškerou moc. Tuto územní výsost Šturma popisuje jako *„právo vykonávat veřejnou (vrchnostenskou) moc nad všemi věcmi a osobami fyzickými i právnickými, které se na tomto území*

---

[327] Podle Otto Mayera, německého administrativisty, zůstává správní právo stále stejné, narozdíl od ústavního práva, jež se mění. Cit. dle HENDRYCH, Dušan a kol. Op. cit., str. 703.

[328] SMEJKAL, Vladimír, SOKOL, Tomáš, KODL, Jindřich. Op. cit., str. 25 - 26.

[329] Srov. rec. 2 směrnice NIS.

[330] ŠTURMA, Pavel. Suverenita státu. In: HENDRYCH, Dušan a kol. *Právnický slovník*. 3. vydání. Praha: C. H. Beck, 2009.

v danou chvíli nacházejí, např. vydávat zákony, ukládat daně, soudit a trestat porušitele práva atd."[331] V tradičním pojetí je respekt vůči státní suverenitě základem mezinárodních vztahů nezávislých států.[332]

Osula a Svantesson poukazují na skutečnost, že *„ačkoli řada mezinárodních organizací i jednotlivých států považuje kyberprostor za prostředí, v němž se rovněž uplatní normy mezinárodního práva, není jednoznačné, zda porušení státní suverenity postačí ke vzniku mezinárodněprávní odpovědnosti a stane se i podkladem pro případná odvetná opatření, anebo zda je koncept státní suverenity jen jedním z principů mezinárodního práva."*[333] Podle druhého ze zmíněných přístupu může jednání v kyberprostoru sice vést k porušení principu nevměšování se do vnitřních záležitostí cizího státu, nedojde však k narušení suverenity státu.[334]

1.4.5.2. Jurisdikční principy

Jurisdikce označuje soubor práv a povinností vykonávaných státem skrze jeho orgány v rovině mocenské, v rovině normotvorby a v soudnictví. Pojem pochází z latinského *ius dicere* a charakterizuje určování práva, či *„moc stanovit nebo nalézat právo, kterou stát svěřuje svým orgánům za tím účelem, aby ji vykonávaly jeho jménem a podle zákona."*[335] Státy nejsou při výkonu jurisdikce neomezené. Jejich práva a povinnosti limitují normy definující působnost státu a charakterizující společenské vztahy, v nichž se uplatní státní moc. Vychází zpravidla z kritérií popisujících místo, čas, osobu a věc (hovoříme o působnosti místní, časové, osobní a věcné).[336]

Lze se setkat i s pojetím jurisdikce v užším slova smyslu označujícím toliko místní působnost.[337] V rámci kyberprostoru činí problémy především otázky výkonu státní moci ve vztahu k určitému území. Tradiční pojetí zaměřené na místní působnost práva (teritorialitu) se sváří s moderním způsobem života odehrávajícím se ve virtuálním prostředí i s požadavky efektivního

---

[331] Tamtéž.

[332] Rozsudek Mezinárodního soudního dvora ze dne 9. 4. 1949, *Corfu Channel Case* (United Kingdom of Great Britain and Northern Ireland v. Albania). Dostupný: http://www.icj-cij.org/en/case/1/judgments [Cit. 2022-11-02].

[333] OSULA, Anna-Maria, NÍ GHRÁINNE, Bríd, SVANTESSON, Dan Jerker B. et al. *Cybersecurity law casebook*. Brno: Masaryk University, 2021, str. 7 - 8. Překlad autorka.

[334] Tamtéž, str. 8.

[335] KLOUČKOVÁ, Světlana, FENYK, Jaroslav. *Mezinárodní justiční spolupráce v trestních věcech*. 2., aktualiz. a dopl. vyd. Praha: Linde, 2005, str. 15.

[336] JELÍNEK, Jiří, DANKOVÁ, Katarína, TLAPÁK NAVRÁTILOVÁ, Jana, PELC, Vladimír, ŘÍHA, Jiří, STEJSKAL, Vojtěch. *Trestní právo hmotné: obecná část, zvláštní část*. 5. aktualizované a doplněné vydání. Praha: Leges, 2016, str. 66.

[337] TÁBOROVÁ, Alice. Op. cit., str. 33.

vyšetřování kyberkriminality, včetně zajištění přístupu k digitálním důkazům.[338] Původ či prostředky použité k vedení útoku v rámci kybernetického incidentu bývají obtížně zjistitelné, popřípadě okolnosti nasvědčují, že za spácháním je konkrétní stát nebo jeho příslušníci. Pozornosti se proto těší především výkon práv a povinností státu ve vztahu k určitému území. Z praktických důvodů proto bude užíváno v následujícím textu pojmu jurisdikce bez uvedení přívlastku v tomto užším slova smyslu.

Ve vztahu k veřejnému právu bývají pravidla místní působnosti nastavena poměrně široce tak, aby stát byl schopen postihnout škodlivé jednání, jež může mít dopad na státem chráněné zájmy. Stejné hledisko zaujala i směrnice NIS, která se použije na orgány veřejné správy, jež jsou určeny jako provozovatelé základních služeb. Za účelem pokrytí všech relevantních kybernetických incidentů a rizik se směrnice NIS vztahuje na provozovatele základních služeb, což jsou například poskytovatelé energií, dopravy, či zdravotní péče ve státě, ale i na poskytovatele digitálních služeb. Případný jurisdikční konflikt v rámci EU směrnice NIS řeší následovně: *„Pravomoc nad poskytovateli digitálních služeb by měl mít ten členský stát, v němž je daný poskytovatel v rámci EU primárně usazen, což v zásadě odpovídá místu, kde se v Unii nachází jeho sídlo. Usazení předpokládá účinný a skutečný výkon činnosti prostřednictvím stálých struktur. Právní forma takových struktur, ať již jde o pobočku, nebo dceřinou společnost s právní subjektivitou, není v tomto ohledu rozhodující. Uvedené kritérium by nemělo záviset na tom, zda se sítě a informační systémy fyzicky nacházejí na daném místě; sama přítomnost a samotné používání takových sítí a systémů nejsou podstatou primárního usazení, a tudíž ani nejsou kritérii pro jeho určení."*[339]

Důrazem na hledisko sídla se směrnice NIS elegantně vyhýbá bezhraniční podstatě virtuálního prostředí. Za zásadní pro výkon pravomoci nepovažuje ani skutečnost, zda se sítě a informační systémy fyzicky nacházejí na území členského státu osobujícího si pravomoc nad poskytovatelem digitální služby. Rozhodné je toliko místo sídla, a to v materiálním slova smyslu, tedy místo, kde daný poskytovatel fakticky uskutečňuje svoji činnost skrze své stálé struktury. Uvedený přístup lze hodnotit kladně, zejména stanoví-li se pro poskytovatele digitálních služeb povinnost mít na území některého z členských států EU usazeného zástupce (srov. níže). Ačkoli směrnice NIS v tomto ohledu upravuje kritéria pravomoci, nezasahuje do možnosti jednotlivých

[338] OSULA, Anna-Maria. Transborder Access and Territorial Sovereignty. *Computer Law and Security Review*. 2015, 31 (6), str. 719-735.

[339] Rec. 64 směrnice NIS.

členských států přijímat nezbytná opatření k ochraně jejich bezpečnosti, veřejného pořádku a odhalování, vyšetřování a stíhání trestné činnosti.[340]

V rámci zajištění kybernetické bezpečnosti je působnost českého ZKB definována souborem vícero norem obsahujících věcné, osobní i místní prvky. Především dopadá na ty orgány a osoby, které mají vzhledem ke své činnosti vliv na zabezpečení významných společenských a ekonomických činností v ČR. Tak jsou kupříkladu povinnosti ukládány provozovatelům základní služby (§ 3 písm. g) ZKB), kterou se rozumí služba, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některém z vybraných odvětví (§ 2 písm. i) ZKB).[341] Povinnosti v oblasti kybernetické bezpečnosti jsou dále ukládány např. poskytovatelům digitálních služeb, jsou-li právnickou osobou usazenou v ČR a nejsou mikropodnikem nebo malým podnikem (§ 3 písm. h), § 33 odst. 3 a 4 ZKB). Působnost českého ZKB je zajištěna ve vztahu ke všem poskytovatelům digitálních služeb poskytujícím tuto službu v ČR tím, že pro ně ZKB stanoví povinnost, aby měl sídlo v ČR alespoň jejich zástupce (ledaže by takový poskytovatel digitální služby již měl sídlo v jiném členském státě EU, anebo si tam ustanovil svého zástupce). Jakmile si poskytovatel digitální služby se sídlem mimo EU ustanoví v ČR svého zástupce, má se za to, že je usazen v ČR a vztahují se na něj povinnosti podle ZKB (§ 3a odst. 2 ZKB).[342] Jde o provedení směrnice NIS, která ukládá poskytovateli digitálních služeb povinnost ustanovit si v rámci EU svého zástupce. Důvodová zpráva poukazuje na nehmotnou povahu poskytovatelů digitálních služeb a upozorňuje, že může snadno dojít k tomu, že dotčený podnikatel nemusí být usazen v EU. Členský stát EU, kde je takový zástupce určen, se však považuje za stát, v němž je poskytovatel digitálních služeb usazen a regulace příslušného orgánu členského státu na něj proto dopadne.[343]

---

[340] Srov. rec. 7 a 8 směrnice NIS.

[341] Jde o odvětví energetiky, dopravy, bankovnictví, infrastruktury finančních trhů, zdravotnictví, vodního hospodářství, digitální infrastruktury a chemického průmyslu.

[342] Podle § 3a odst. 3 ZKB v případě, že je poskytovatel digitální služby usazen v ČR nebo zde má ustaveného zástupce, ale jím využívané sítě elektronických komunikací a informační systémy se nacházejí v jiném členském státu, NÚKIB při výkonu státní správy spolupracuje s příslušným orgánem dotčeného členského státu.

[343] VLÁDA. Důvodová zpráva k zákonu č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony, č. 205/2017 Dz.

1.4.5.3. Jurisdikční konflikty

O jurisdikčním konfliktu zjednodušeně hovoříme tehdy, pokud lze na základě vnitrostátního práva různých států dovodit pravomoc těchto států řešit věc, anebo kdy naopak nelze tuto pravomoc dovodit u žádného z nich. Situace, v níž si pravomoc ve věci osobují orgány dvou či více států, je pozitivním konfliktem jurisdikce (konfliktem konkurujících pravomocí). Naopak nelze-li ve věci dovodit pravomoc žádného státu, respektive není-li žádný stát, který by hodlal ve věci konat či měl zájem na výkonu své pravomoci, hovoříme o negativním jurisdikčním konfliktu. Vzhledem k nastavení pravidel působnosti právních norem zajišťujících bezpečnost sítí a informačních systémů by k negativním jurisdikčním konfliktům zpravidla nemělo docházet, vezme-li se v potaz, že cílem těchto norem je zajistit pravomoc států při zabezpečení jeho základních služeb a infrastruktur. Naopak situace, v níž si budou správní orgány dvou či více různých států osobovat v určité věci pravomoc, nemusí být výjimečná. Pakliže se kybernetický incident dotýká dvou či více členských států EU, mají být tyto informovány zpravidla týmem CSIRT či jiným kompetentním orgánem.[344]

Patrně jedním z prvních popsaných pozitivních konfliktů jurisdikce byl případ srážky francouzského parníku Lotus s tureckým parníkem v tureckých vodách, při níž přišlo o život osm tureckých občanů. Stálý dvůr mezinárodní spravedlnosti v Haagu, který řešil konflikt v roce 1927, uplatnil ve sporu doktrínu efektu a postup tureckých orgánů, které zahájily trestní stíhání francouzského důstojníka podle tureckého práva, neshledal v rozporu s mezinárodním právem.[345] Podle uplatněného principu (*Lotus principle*) mohou suverénní státy jednat podle svého uvážení do té míry, pokud se nedostanou do kolize s výslovným zákazem mezinárodního práva. Případ Lotus se nicméně stal předmětem různých (i odlišných) interpretací a samotným Mezinárodním soudním dvorem nebyla tato zásada všeobecně přijímána.[346]

Konflikt konkurujících pravomocí řeší státy většinou skrze konzultace v rámci mezinárodní spolupráce. Praktickou a rychlou metodou jsou zejména neformální konzultace. S cílem usnadnit strategickou spolupráci mezi členskými státy EU došlo na základě směrnice NIS k ustavení

---

[344] Srov. čl. 16 odst. 6 směrnice NIS.

[345] Rozsudek Stálého dvora mezinárodní spravedlnosti v Haagu ze dne 7. 9. 1927, *The Case of the S. S. Lotus (France v. Turkey)*, Ser. A, No. 10, 1927. Dostupné: https://web.archive.org/web/20101210073754/http://www.worldcourts.com/pcij/eng/decisions/1927/1927.09.07_lotus.htm [Cit. 2022-11-03].

[346] K jednotlivým interpretacím případu Lotus a kritice uplatněné zásady srov. např. HANDEYSIDE, Hugh. *The Lotus Principle in ICJ Jurisprudence: Was the Ship Ever Afloat? [online]*. Michigan Journal of International Law. Vol. 29, č. 1 (2007). Dostupné: https://repository.law.umich.edu/mjil/vol29/iss1/3/ [Cit. 2022-11-03].

speciální skupiny pro spolupráci[347] i sítě bezpečnostních týmů typu CSIRT,[348] jež mají umožnit rychlou a operativní spolupráci při zabezpečení sítí a informačních systémů v EU, jakož i k určení vnitrostátních příslušných orgánů a kontaktních míst.[349] Přeshraniční spolupráci v rámci EU zajišťují v členských státech jednotná kontaktní místa pro oblast bezpečnosti sítí a informačních systémů (dále jen „jednotná kontaktní místa"). V případě ČR je jednotným kontaktním místem NÚKIB. Důležitost přeshraniční spolupráce ukazuje i požadavek, aby jmenovaní zástupci ve skupině pro spolupráci výslovně spolupracovali *„účelně, účinně a spolehlivě"*.[350] Operativní spolupráci mezi členskými státy EU zajišťuje především síť týmů CSIRT, která poskytuje podporu při řešení přeshraničních incidentů.[351] Může rovněž napomoci výkonu pravomoci členského státu např. tím, že určí koordinovanou reakci na incident zjištěný v oblasti spadající do pravomoci tohoto členského státu, pokud o to požádá.[352] ČR si nepočíná při řešení bezpečnostních incidentů špatně. V roce 2020 měla ČR v rámci jednoho státu v Evropě nejvíce zapojených bezpečnostních týmů v mezinárodní komunitě Trusted Introducer.[353]

Negativní jurisdikční konflikt připadá v úvahu tehdy, pokud bude dopad incidentu v kybernetickém prostředí natolik bezvýznamný pro bezpečnost sítí a informačních systémů státu, členských států EU, či jiného mezinárodního společenství, k jehož bezpečnosti se jednotlivé státy zavázaly konat, že nebude vyhodnocen jako důvod pro výkon pravomoci žádného ze států. Existuje však riziko, že z globálního hlediska budou dopady incidentu významnější, než by se to jevilo z pohledu jednotlivých států.[354] Táborová uvádí mezi důvody absence výkonu pravomoci nedostatky vnitrostátního procesního práva, spoléhání se na aktivní konání jiných státních orgánů i pochybení

---

[347] Skupina pro spolupráci je tvořena zástupci členských států, Komise a agentury ENISA. Její působnost stanovuje čl. 11 směrnice NIS.

[348] Computer Security Incident Response Team, neboli CSIRT, provozuje v ČR sdružení CZ.NIC. Působnost sítě CSIRT upravuje čl. 12 směrnice NIS.

[349] Srov. čl. 1 odst. 2 písm. b), c), e) směrnice NIS.

[350] Srov. čl. 8 směrnice NIS, zejména odst. 4 a 5.

[351] Čl. 12 odst. 3 písm. e), f) směrnice NIS.

[352] Čl. 12 odst. 3 písm. d) směrnice NIS.

[353] CSIRT.CZ. *Zpráva o činnosti CSIRT.CZ (Národního CSIRT ČR) za rok 2020* [online], str. 10. Dostupné: https://www.csirt.cz/media/filer_public/c1/64/c1642df8-32f0-4976-9062-ac259f7a43b4/210304_csirt_vyrocni_zprava_2020.pdf [Cit. 2022-11-03]. Služba Trusted Introducer byla zřízena v roce 2000 evropskou komunitou týmů CERT/CSIRT a nabízí podporu bezpečnostním týmům při řešení bezpečnostních incidentů. Podrobněji TF-CSIRT: Trusted Introducer. *Services for Security and Incident Response Teams* [online]. Dostupné: https://www.trusted-introducer.org/services/overview/czech.html [Cit. 2022-11-03].

[354] V rovině trestního práva uvádí Koops příklad, kdy *„jediný virus napáchá v různých státech citelnou škodu, avšak trestní stíhání nezahájí žádný z příslušných orgánů činných v trestním řízení, neboť každý stát zaznamená jen nepatrnou výseč z celkově způsobené škody."* KOOPS, Bert-Jaap (ed.). *Cybercrime and jurisdiction: a global survey*. 1. vyd. The Hague: T.M.C. Asser press, 2006, str. 6. Překlad autorka.

příslušných státních orgánů.[355] Za účelem vyvarování se negativním jurisdikčním konfliktům je třeba zajistit efektivní vymahatelnost práva a posílit mezinárodní spolupráci, jíž lze řešit problematiku přípustných zásahů do státní suverenity i jurisdikční konflikty. Možnost EU uzavírat mezinárodní dohody se třetími zeměmi či mezinárodními organizacemi předpokládá čl. 218 Smlouvy o fungování EU i čl. 13 směrnice NIS. Vzhledem k suverenitě jednotlivých států obvykle nebude možné hledat řešení mimo formy mezinárodní spolupráce, které umožní vybrat nejvhodnější jurisdikci či vyžádat si právní pomoc od jiného státu.[356] Mezinárodní spolupráce v neposlední řadě snižuje i pravděpodobnost usazení definičních autorit v jurisdikci, v níž by se vyhnuly splnění určitých povinností, anebo kde by výkon správního dozoru byl méně pravděpodobný.

1.4.5.4. Tallinnský manuál

Vodítkem pro aplikaci norem mezinárodního práva v kybernetickém prostředí se stal dokument nazvaný v angličtině *Tallinn Manual on the International Law Applicable to Cyber Warfare*.[357] Jednalo se o první dokument pojednávající o aplikaci mezinárodněprávních norem v kybernetickém prostředí, a to pro případ kybernetické války. První verze Tallinnského manuálu tak pojednává o činech v kyberprostoru, které jsou v rozporu se zákazem použití síly, a o kybernetických operacích během ozbrojeného konfliktu. Díky rozšíření autorského kolektivu o další odborníky pocházející z více zemí[358] vznikla druhá verze dokumentu nazvaná *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (dále též jako „Tallinn Manual 2.0"), která pojednává již o širším spektru kybernetických aktivit: zabývá se aplikací mezinárodněprávních norem na kybernetické operace a incidenty odehrávající se na denní bázi.[359] Svojí charakteristikou jsou Tallinnské manuály dokumenty kazuistické povahy, které popisují u základních pravidel mnohé praktické situace, jež by mohly nastat; v souladu s úlohou manuálu

---

[355] TÁBOROVÁ, Alice. Op. cit., str. 35.

[356] Např. vyšetřování kybernetické trestné činnosti se zpravidla neobejde bez mezinárodní spolupráce. Podle Seitze vyžaduje přístup k digitálním důkazním prostředkům uloženým na zahraničních serverech až 80% všech případů v Německu, v nichž figuruje Internet. SEITZ, Nicolai. Op. cit., str. 25.

[357] SCHMITT, Michael N. *Tallinn manual on the international law applicable to cyber warfare: prepared by the international group of experts at the invitation of the NATO cooperative cyber defence centre of excellence*. Cambridge: Cambridge University Press, 2013.

[358] FÈVRE, Victor. Review of TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS [online]. *Politique Étrangère*, vol. 82, no. 4, 2017, str. 210–211. Dostupné: *JSTOR*, https://www.jstor.org/stable/48562377 [Cit. 2022-11-04].

[359] SCHMITT, Michael. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* [online]. 2. vydání. Cambridge: Cambridge University Press, 2017. Dostupné: https://www.cambridge.org/core/books/abs/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/law-of-international-responsibility/99E333F8578ADCC567A92BECF932E4C3 [Cit. 2022-11-04].

poskytují státům návod, jak aplikovat principy a normy mezinárodního práva veřejného na kybernetické operace.[360] Tímto návodem se státy při výkladu mezinárodních norem mohou či nemusejí řídit. Základní pravidla, která jsou tematicky rozdělena do okruhů, jsou však dostatečně obecná a do určité míry zákoník připomínají, byť jsou jednotlivá pravidla převzata z externích pramenů mezinárodního práva veřejného.

Vzhledem k nezávaznosti vyslovených pravidel nabývají Tallinnské manuály na významu silou přesvědčivosti své argumentace. Ta není zanedbatelná, neboť se na jejich vzniku podílela řada odborníků zabývajících se problematikou mezinárodního práva veřejného. V současnosti se připravuje třetí verze Tallinnského manuálu (pracovně nazvaná Tallinn Manual 3.0), vznikající v rámci odborné platformy pod patronátem NATO (*The NATO Cooperative Cyber Defence Centre of Excellence*, dále též „CCDCoE"). Třetí verze doplní původní manuály z let 2013 a 2017.[361]

Ačkoli Tallinnské manuály představují nezávazný právní dokument, někteří experti jej považují za *lex lata* kybernetického prostředí. Jiní zaujímají opačný postoj s odkazem na dominantní pozici zemí severozápadní aliance při vzniku Tallinnských manuálů. Vytýkají jim rovněž netransparentní proces přípravy, do níž nebyla zahrnuta řada dalších aktérů kyberprostoru.[362] Druhá verze Tallinn Manual 2.0 však úvodem upozorňuje, že není oficiálním dokumentem, ale jen výsledkem činnosti skupiny nezávislých expertů, a dále uvádí, že nereprezentuje postoje a názory NATO ani sponzorujících zemí.[363] Třetí verze Tallinn Manual 3.0 se snaží, alespoň částečně, uvedeným výtkám čelit. Skrze webovou stránku totiž zve k podílení se na přípravě dokumentu širokou odbornou veřejnost.[364]

Tallinn Manual 2.0, který má širší pole působnosti než první verze, se uplatní na jednání v kyberprostoru v užším slova smyslu (*cyber-to-cyber operations*). Příkladem takového jednání je kybernetický útok na státní kritickou infrastrukturu. Manuál se však nepoužije na incidenty či útoky, při nichž jsou využity tradiční zbraně, byť by se cílem útoku stal počítačový systém. Manuál je použitelný také v případech mezinárodního i vnitřního ozbrojeného konfliktu, a část pravidel (např. státní suverenita a jurisdikce) je použitelná mimo jakýkoli ozbrojený konflikt.[365]

---

[360] FÈVRE, Victor. Op. cit., str. 211.

[361] CCDOE. *The Tallinn Manual* [online]. Dostupné: https://ccdcoe.org/research/tallinn-manual/ [Cit. 2022-11-04].

[362] TANODOMDEJ Papawadee. The Tallinn Manuals and the Making of the International Law on Cyber Operations. [online] *Masaryk Journal of Law and Technology.* 2019, (13/1), str. 67 - 85. Dostupné: https://journals.muni.cz/mujlt/issue/view/992 [Cit. 2022-11-04].

[363] Tallinn Manual 2.0. Op. cit., str. 11.

[364] CCDOE. Op. cit.

[365] Tallinn Manual 2.0, str. 5.

Je jednoznačné, že princip státní suverenity, který je základem mezinárodního práva, se uplatní i v kyberprostoru. Za součást státní suverenity Tallinn Manual 2.0 považuje výkon nezávislé kontroly státu nad komunikačními kanály, úložišti a počítačovými zdroji zabezpečujícími informační systémy. Půjde o kontrolu nad „kybernetickou infrastrukturou" *(cyber infrastructure)* a s ní spojenými aktivitami na území státu. Zároveň se státy musí zdržet kybernetických operací narušujících suverenitu jiných států.[366] Porušením pravidla nebude, pokud v reakci na kybernetický útok stát zasáhne nestátního aktéra (jednotlivce, anarchistické uskupení, teroristickou skupinu, apod.).[367]

Kybernetická infrastruktura se stává předmětem vnitrostátní regulace díky územní výsosti státu. Tallinn Manual 2.0 rozeznává několik aspektů kybernetické infrastruktury: stát vykonává svrchovanou moc nad fyzickým (hardware, kabely, servery, počítače …), logickým (aplikace, data, protokoly …) i sociálním aspektem (jednotlivci a skupiny působící v kyberprostoru), a v tomto směru může stanovit technické podmínky k zabezpečení elektronických komunikací (logický aspekt) nebo kriminalizovat on-line sdílení určitého obsahu (sociální aspekt); pod státní ochranou se přitom nachází veřejná i soukromá infrastruktura.[368]

Ne každý incident však bude zásahem do suverenity státu. Tallinn Manual 2.0. klade důraz na hledisko vzniklé škody. Zásahem do státní suverenity bude útok na kybernetickou infrastrukturu nacházející se na území jiného státu, způsobí-li takový čin škodu, anebo bude-li spáchán s úmyslem donutit cizí vládu k určitým politickým krokům - v takovém případě se může jednat též o nedovolenou intervenci či nedovolené použití síly. Povinností suverénního státu je totiž zamezit, aby z jeho území docházelo ke škodlivým aktivitám v kyberprostoru.[369]

Co se jurisdikce týče, Tallinn Manual 2.0 rozlišuje teritoriální a extrateritoriální jurisdikci. Teritoriální jurisdikci stát vykonává ve vztahu ke kybernetické infrastruktuře a k osobám zapojeným do kybernetických činností (*engaged in cyber activities*) na svém území, jakož i vzhledem ke kybernetickým činnostem majícím původ na území státu, či na území tohoto státu dokonaným (*completed*), jakož i ve vztahu ke kybernetickým činnostem, které mají na státní území podstatný dopad (*having a substantial effect*).[370] Pravomoc mimo státní území (extrateritoriální jurisdikci) mohou státy vykonávat ve vztahu ke kybernetickým činům, jejichž původci jsou jeho vlastní státní

---

[366] Tallinn Manual 2.0., Rule 1 - Sovereignty, Rule 4 - Violation of sovereignty. Překlad autorka.

[367] Tamtéž, str. 18.

[368] Tamtéž.

[369] Tallinn Manual 2.0, str. 11 - 16. Překlad autorka.

[370] Tallinn Manual 2.0., Rule 9 - Territorial jurisdiction. Překlad autorka.

příslušníci nebo pokud byly spáchány na palubě plavidla či letadla registrovaného v daném státě, anebo ve vztahu ke kybernetickým činům spáchaných cizími státními příslušníky v úmyslu závažně narušit základní zájmy státu (*seriously undermine essential state interests*) či namířených proti jeho státním příslušníkům, anebo ve vztahu ke kybernetickým činům, jež představují zločiny podle mezinárodního práva a podléhají zásadě univerzality.[371]

Rozsah extrateritoriální jurisdikce nad kybernetickými aktivitami závisí na skutečnosti, zda půjde o aplikaci vnitrostátního předpisu, pravomoc národních soudů rozhodnout určitou věc, anebo o projevy moci výkonné. Aplikace vnitrostátního předpisu a pravomoc národních soudů jde obvykle ruku v ruce. Nejsou přitom výjimkou pozitivní jurisdikční konflikty, kdy je dána pravomoc soudů vícero států věc rozhodnout za aplikace vlastního vnitrostátního práva na základě státní příslušnosti původce kybernetické operace a podle místa spáchání činu. Tyto případy se zpravidla řeší formou konzultací.[372] Naproti tomu výkon státní moci vně území státu (*extraterritorial enforcement jurisdiction*) bude zpravidla možný jen se souhlasem dotčeného státu.[373]

1.4.5.5. Rozhodnutí SDEU ve věci Google vs. CNIL

Praktickým příkladem problematického působení práva v rámci virtuálního prostředí je spor mezi společností Google a francouzským dozorovým orgánem pro informatiku a svobody (*Commission nationale de l'informatique et des libertés*, dále též „CNIL"), který se dostal až k SDEU v rámci žádosti francouzské Conseil d'État (Státní rada) o posouzení předběžné otázky.[374] Ačkoli se případ netýká kybernetické bezpečnosti, nýbrž služeb informační společnosti, respektive kolize svobody šíření informací a ochrany soukromí a osobních údajů, je vhodné jej představit s ohledem na dopady, které může mít na výkon správního rozhodnutí v kyberprostoru mimo jurisdikci státu dozorujícího správního orgánu.

Veřejná správa se musí vyrovnat s existencí různých cizích správních aktů, jež mají na základě unijního práva veřejnoprávní účinky i na území domovského členského státu. Formální uznání úředního aktu jiného členského státu přitom není zapotřebí. Jev je označován jako trans-

---

[371] Tallinn Manual 2.0., Rule 10 - Extraterritorial prescriptive jurisdiction. Překlad autorka.

[372] Srov. např. čl. 22 odst. 5 Úmluvy o počítačové kriminalitě.

[373] Tallinn Manual 2.0, Rule 8 - Jurisdiction, Rule 11 - Extraterritorial enforcement jurisdiction. Překlad autorka.

[374] Rozsudek SDEU ze dne 24. 9. 2019 ve věci C-507/17, *Google LLC, právní nástupkyně Google Inc. v. Commission nationale de l'informatique et des libertés (CNIL).*

teritoriální účinky a úřední akty, jichž se týká, jsou pojmenovány jako trans-teritoriální správní akty.[375]

Žádost o předběžnou otázku byla položena ve věci sankce 100 000 eur, jíž uložila CNIL společnosti Google proto, že poté, kdy tato společnost vyhověla žádosti o odstranění odkazů, odmítla ji vztáhnout na všechny domény svého vyhledávače. Francouzský dozorový úřad konkrétně vyzval společnost Google, aby v rámci vyhovění žádosti fyzické osoby o odstranění odkazů na internetové stránky ze seznamu výsledků zobrazených po zadání jejího jména, odstranila tyto odkazy ze všech domén svého vyhledávače. CNIL nepovažovala za dostatečné opatření zvolené společností Google, a sice tzv. geo-blocking (zeměpisné blokování), které spočívalo v tom, že přístup ke sporným výsledkům zobrazujícím se po zadání jména subjektu údajů byl znemožněn pro IP adresy považované za adresy nacházející se ve státě bydliště subjektu údajů, bez ohledu na to, jakou konkrétní mutaci vyhledávače uživatel Internetu použil k vyhledávání. Conseil d'État konstatovala, že „*vzhledem k tomu, že jsou z francouzského území dostupná všechna doménová jména vyhledávače společnosti Google a tato jednotlivá doménová jména jsou vzájemně prostupná díky automatickému přesměrovávání, a vzhledem k tomu, že jsou navíc soubory cookie přítomny v jiných mutacích vyhledávače než v té, v které byly původně uloženy, musí být na tento vyhledávač, který byl ostatně předmětem jediné stížnosti u CNIL, pohlíženo pro účely aplikace zákona ze dne 6. ledna 1978 tak, že provádí jediné zpracování osobních údajů."* Dovodila proto, že ke zpracování osobních údajů vyhledávačem provozovaným společností Google dochází v provozovně usazené na francouzském území, pročež pro něj platí francouzský zákon.[376] Společnost Google rozporovala povinnost odstranit sporné odkazy bez zeměpisného omezení ze všech domén svého vyhledávače a namítala nepřiměřený zásah do svobody projevu, informací, komunikace a tisku zaručených zejména článkem 11 Listiny základních práv EU. Jádrem předběžné otázky bylo posouzení, zda vykládat právo na odstranění odkazu[377] v tom smyslu, že provozovatel vyhledávače je povinen v rámci vyhovění žádosti o odstranění odkazu vztáhnout toto odstranění na všechna doménová jména

---

[375] Podrobněji HANDRLICA, Jakub. Veřejná správa na rozcestí administrativního pluralismu. In: PAPÁČOVÁ, I. (ed). *Verejná správa na rázcestí*. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta. 2018, str. 45 - 55.

[376] Francouzský zákon obsahující požadavky směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Tato směrnice byla později nahrazena nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

[377] K podrobnostem práva na odstranění odkazu (či práva být zapomenut) srov. rozsudek SDEU ze dne 13. 5. 2014, ve věci C-131/12, *Google Spain SL a Google Inc. v. Agencia Española de Protección de Datos (AEPD) a Mario Costeja González*.

svého vyhledávače tak, aby se sporné odkazy již neobjevovaly, a to bez ohledu na místo, z něhož je zadán požadavek na vyhledávání podle jména žadatele.

SDEU zdůraznil, že pokud dochází ke zpracování osobních údajů v provozovně společnosti Google nacházející se na francouzském území (přičemž dovodil, že ano), nemůže okolnost, že je vyhledávač provozován podnikem z třetího státu, vést k tomu, že pro takové zpracování nebudou platit podmínky a záruky stanovené unijním právem.[378] Poukázal na to, že je třeba v Unii zajistit shodnou ochranu fyzických osob a zamezit rozdílům bránícím volnému pohybu osobních údajů v rámci vnitřního trhu. Zdůraznil též potřebu stanovit správcům a zpracovatelům osobních údajů povinnosti, které zajistí důsledné monitorování zpracování osobních údajů. Sankce za jejich porušení by měly být ve všech členských státech rovnocenné a spolupráce mezi dozorovými úřady účinná.[379] Skutečnost, že internetoví uživatelé mají v globalizovaném světě přístup k odkazům na informace o osobě, jejíž středisko zájmů se nachází v EU, může mít na takovou osobu přímý a podstatný dopad v samotné EU. SDEU tudíž dovodil *„pravomoc unijního normotvůrce uložit provozovateli vyhledávače v případě, že vyhoví žádosti takové osoby o odstranění odkazů, povinnost odstranit odkazy ze všech mutací svého vyhledávače."*[380]

Takovou pravomoc však nedovodil ve vztahu k třetím státům. Práva zakotvená unijní legislativou totiž nemají účinky přesahující území členských států. Společnost Google tedy nebyla shledána povinnou odstranit odkazy i v národních mutacích vyhledávače nad rámec území EU. K odstranění odkazů však mělo dojít pro všechny členské státy EU.[381] SDEU proto považoval za zásadní účinnou spolupráci dozorových úřadů dotčených členských států. Těm však zároveň ponechal zadní vrátka, když konstatoval, že *„unijní právo sice za současného stavu neukládá povinnost, aby v rámci vyhovění žádosti byly odkazy odstraněny ze všech mutací dotčeného vyhledávače, ale ani to nezakazuje. Dozorový úřad či soud členského státu proto má pravomoc poměřit právo subjektu údajů na respektování soukromého života a na ochranu jeho osobních údajů na straně jedné s právem na informace na straně druhé z pohledu vnitrostátního standardu pro ochranu základních práv (v tomto smyslu viz rozsudky ze dne 26. února 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, bod 29, a ze dne 26. února 2013, Melloni, C-399/11, EU:C:2013:107,*

---

[378] Soud přitom odkázal na bod 58 svého rozsudku ze dne 13. 5. 2014, ve věci C-131/12, *Google Spain SL a Google Inc. v. Agencia Española de Protección de Datos (AEPD) a Mario Costeja González*..

[379] Srov. rozsudek SDEU ze dne 24. 9. 2019 ve věci C-507/17, Op. cit., body 12-13, s odkazem na obecné nařízení o ochraně osobních údajů.

[380] Tamtéž, bod 58.

[381] Zároveň však Soud podotkl, že se *„zájem veřejnosti na přístupu k informacím může lišit i v jednotlivých členských státech, takže poměřování tohoto významu s právem subjektu údajů na respektování soukromého života a na ochranu osobních údajů nepovede nutně ke stejnému výsledku pro všechny členské státy"*. Tamtéž, bod 67.

bod 60), a v návaznosti na to případně provozovateli tohoto vyhledávače uložit povinnost, aby odkazy odstranil ze všech mutací uvedeného vyhledávače.“[382]

Z případu vyplývá jasný požadavek na zajištění shodné úrovně ochrany práv fyzických osob ve všech členských státech EU. K tomu má dopomoci rovnocenný systém sankcí a efektivní spolupráce dozorových správních úřadů napříč EU. Lze tak počítat s vymáháním odpovídajících povinností u nepodřízených subjektů s dopady uvnitř EU, nikoli však mimo území členských států. U správních aktů cizího členského státu se presumuje jejich správnost, přičemž zákonnost a případné vady se posuzují z hlediska právního řádu domovského státu. Tyto trans-teritoriální správní akty povedou k častější interakci exekutiv jednotlivých členských států.[383] V případě, že by dozorový správní úřad členského státu trval na splnění povinností z globálního hlediska tak, aby se požadovaný stav projevil na Internetu bez ohledu na místo, odkud se uživatel přihlásí k webu, musí to být odůvodněno testem proporcionality z pohledu vnitrostátního standardu ochrany základních práv. Právo na respektování soukromého života a ochranu osobních údajů by v takovém případě muselo převážit nad právem na informace.

[382] Tamtéž, bod 72.

[383] HANDRLICA, Jakub. Op. cit., str. 53 - 54.

2. Kyberprostor a úloha státu na zajištění informační bezpečnosti

2.1. Kybernetická bezpečnost i kybernetická obrana jako úloha státu

2.1.1. Kyberprostor a vázanost státní moci zákonem

Okolo jedné zářijové půlnoci roku 2011 informovala nizozemská TV o mimořádném zpravodajském vysílání v 1:00 hodin. Pokud byli tou dobou diváci vzhůru, spatřili na obrazovce nizozemského ministra vnitra, který jim stručně oznámil, že Internet přestal být bezpečný, ale vláda podnikla příslušné kroky a zachránila Nizozemské království i Internet. Mimořádné zpravodajství ministra vnitra se týkalo počínající aféry certifikační autority *DigiNotar*,[384] která měla být napadena íránskými hackery. V důsledku útoku byl narušen zabezpečený přenos dat mezi uživateli a webovými stránkami, neboť vznikly stovky falešných certifikátů ověřujících totožnost webových serverů. *DigiNotar* tajil kybernetický útok přes dva měsíce z obavy před negativní publicitou, útok vyšel najevo až díky zprávě německé skupiny CERT. Vlivem kybernetického útoku bylo odposlechnuto přes 300 000 IP adres využívajících několik týdnů falešný certifikát pro webovou stránku google.com.[385] Kybernetický útok na certifikační autoritu závažně narušil bezpečnost sítě Internet. Tehdejší nizozemský ministr vnitra odůvodnil zásah státu významem digitální ekonomiky a zachováním celosvětové důvěry v nizozemské služby informační společnosti. Ačkoli situace vyžadovala reaktivní opatření, zásah státní moci spočívající v převzetí kontroly nad soukromou certifikační autoritou Ministerstvem vnitra Nizozemského království postrádal zákonný základ a vzbudil značné kontroverze.[386] [387]

Obdobný postup českého ministerstva vnitra by představoval porušení ústavního principu vázanosti státní moci zákonem. Podle čl. 2 odst. 3 ústavního zákona č. 1/1993 Sb., Ústavy České republiky (dále jen „Ústava ČR"), jakož i čl. 2 odst. 2 Listiny základních práv a svobod lze státní moc uplatňovat jen v případech, v mezích a způsoby, které stanoví zákon. Zákonný podklad pro činnost státní moci v případě kybernetických útoků a ohrožení veřejných zájmů ČR je nutností. Chrání nejen zájmy státu, ale i základní práva a svobody jeho občanů.

---

[384] Certifikační autority zajišťují bezpečnou komunikaci po síti ověřením autenticity protokolu přes certifikát, čímž potvrdí, že nedošlo k narušení, pozměnění či odposlechu přenášených dat. ARNBAK, Axel, VAN EIJK, N.A.N.M. *Certificate Authority Collapse: Regulating Systemic Vulnerabilities in the HTTPS Value Chain* [online]. TRPC, 15. 8. 2012, str. 2-6. Dostupné: http://dx.doi.org/10.2139/ssrn.2031409 [Cit. 2022-11-05].

[385] Jedna IP adresa přitom může odpovídat i vícero počítačovým zařízením.

[386] ARNBAK, Axel, VAN EIJK, N.A.N.M. Op. cit., str. 12-14.

[387] Text je součástí práce autorky odevzdané v rámci XI. ročníku Studentské vědecké odborné činnosti na Právnické fakultě Univerzity Karlovy. RADEMACHEROVÁ, Kristina. *Principy a východiska kybernetické bezpečnosti de lege lata*. Op. cit., str. 6.

Nutnost reagovat na kybernetické útoky a incidenty lze očekávat v řadě veřejných politik. Z výroční zprávy monitorující výskyt kybernetických bezpečnostních incidentů v EU za rok 2019 vyplynulo, že nejvíce incidentů pocítily kybernetické infrastruktury zdravotnictví, digitálních služeb a bankovního sektoru.[388] Hlášeny jsou přitom pouze kybernetické incidenty s významným dopadem na fungování základních služeb, byť se členské státy neřídí při posouzení závažnosti incidentů jednotnými měřítky. Samotné hlášení incidentů by se mělo harmonizovat, jelikož členské státy hodnotí hrozby rozdílně a některé hlásí více incidentů oproti jiným.[389]

Výkon státní moci nesmí překročit zákonné mantinely a nelze jej obhájit toliko odkazem na účel uplatněných prostředků. Uplatněním pravidla „účel světí prostředky" by došlo k popření principu suverenity lidu vyjádřeného zejména v čl. 2 odst. 1 a 3 Ústavy ČR. Ačkoli Ústava ČR hovoří o vázanosti *státní* moci zákonem, systematickým i logickým výkladem lze dospět k širšímu pojetí ve smyslu vázanosti *veřejné* moci zákonem. Sládeček a Syllová zde odkazují k čl. 87 odst. 1 písm. d) Ústavy ČR, který umožňuje obranu proti zásahu orgánu veřejné moci do ústavně zaručených práv, nikoli toliko orgánu státní moci.[390] Státní mocí se zpravidla rozumí moc vykonávaná přímo státem (jeho orgány), přičemž jde o druh veřejné moci. Skrze propůjčení státní moci soukromoprávním subjektům či jejímu přenesení na jiné subjekty veřejného práva stát vykonává státní správu a moc i nepřímo. Veřejná moc je pojmem širším: *„Zahrnuje jak státní moc vykonávanou státními orgány (a na základě zákona namísto státu subjekty od státu odlišnými), tak další (ostatní) veřejnou moc vykonávanou nestátními subjekty, resp. jejich orgány (veřejnoprávní korporace, jimiž jsou např. územní samosprávné celky nebo profesní komory, a další soukromé subjekty)."*[391]

Princip uplatňování státní moci jen v případech, v mezích a způsoby, které stanoví zákon tak ukládá veškerým státním orgánům, ústavním činitelům i úředním osobám respektovat při výkonu vrchnostenské (veřejné) moci zákon, včetně zákona ústavního. Hmotněprávní, kompetenční i procesní podmínky pro uplatňování státní (veřejné) moci lze upravit jen zákonem. Povinnost

---

[388] NIS COOPERATION GROUP. Op. cit., str. 9.

[389] Např. Německo v důsledku své legislativy implementující směrnici NIS ukládá provozovatelům základní služby hlásit veškeré zaznamenané incidenty s dopadem na poskytovanou službu, zatímco Finsko a Irsko uplatňují určité kvalifikační požadavky k hlášení příslušných incidentů. NIS COOPERATION GROUP, Op. cit., str. 8. Dále srov. SCHMITZ-BERNDT Sandra, ANHEIER Fabian. Synergies in Cybersecurity Incident Reporting – The NIS Cooperation Group Publication 04/20 in Context [online]. *European Data Protection Law Review,* 2021, Vol. 7 (1). Dostupné: https://edpl.lexxion.eu/data/article/16999/pdf/edpl_2021_01-014.pdf [Cit. 2022-11-05].

[390] SLÁDEČEK, Vladimír, SYLLOVÁ, Jindřiška. Čl. 2 [Státní moc]. In: SLÁDEČEK, Vladimír, MIKULE, Vladimír, SUCHÁNEK, Radovan, SYLLOVÁ, Jindřiška. *Ústava České republiky*. 2. vydání. Praha: C. H. Beck, 2016, str. 32.

[391] Tamtéž, str. 31.

vykonavatelů veřejné moci řídit se zákonem však zahrnuje i závazek postupovat v souladu s podzákonnými, zejména prováděcími předpisy k zákonům, nestanoví-li Ústava jinak.[392]

Přes shora rozebraná specifika kybernetického prostředí není důvodu, aby se v něm neuplatil ústavní princip vázanosti státní moci zákonem. Tak jako by stát neměl rezignovat na ochranu svých zájmů v kyberprostoru, nesmí tak učinit ani ve vztahu k zabezpečení základních práv a svobod svých občanů. Porušení uvedených povinností může mít za následek vznik odpovědnosti státu a práva na náhradu škody způsobené nezákonným rozhodnutím nebo nesprávným úředním postupem.

2.1.2. Bezpečnost

Za účelem rozboru kybernetické bezpečnosti je třeba nejprve krátce pojednat o obecném pojmu bezpečnost. Bezpečnost vnímáme a vykládáme především ve vztahu ke konkrétnímu objektu. Definice bezpečnosti tudíž nabývá různého obsahu i významu. S pojmem se setkáváme v různých právních předpisech, počínaje ústavním zákonem č. 110/1998 Sb., o bezpečnosti České republiky, ve znění pozdějších předpisů (dále jen „ústavní zákon o bezpečnosti ČR"), přes předpisy upravující kybernetickou bezpečnost, ochranu utajovaných informací, elektronickou komunikaci, atomovou energii, až k normám věnujícím se bezpečnosti léčiv, staveb, výrobků, výkonu práce, jízdy po pozemních komunikacích, a mnoha dalším oblastem lidského života.

Smejkal, Sokol a Kodl upozorňují na relativitu a neurčitost pojmu bezpečnost, jelikož jeho obsah a výklad závisí na konkrétním vědeckém oboru a uplatňovaných principech: neurčitým právním pojmem je i bezpečnost informačních systémů, což podle zmíněných autorů může vést k riziku, že správní orgán v rámci volné (správní) úvahy nesprávně posoudí naplnění skutkové podstaty správního deliktu spočívajícího v porušení povinností ukládaných na poli bezpečnosti informačních systémů zákonem o kybernetické bezpečnosti. Upozorňují, že naplnění skutkové podstaty řady deliktů dle ZKB může být obtížně posouditelné a prokazatelné, neboť půjde o posouzení odborné otázky, zda bylo konkrétní zabezpečení při nekonečné variabilitě možností dostatečné, správné a vhodné.[393] Je pravdou, že co se rozumí kybernetickou bezpečností, v zákoně o kybernetické bezpečnosti nenajdeme. Jeho výkladová ustanovení definují pouze bezpečnost informací, kterou rozumí *„zajištění důvěrnosti, integrity a dostupnosti informací a dat."*[394] Správní

---

[392] Tamtéž, str. 34.

[393] SMEJKAL, Vladimír, SOKOL, Tomáš, KODL, Jindřich. Op. cit, str. 19 - 21.

[394] Srov. § 2 písm. c) ZKB.

orgán rozhodující o vině za přestupek na poli kybernetické bezpečnosti však není v rámci svých úvah neomezený. Státní moc je vázána zákonem, proto i zde platí obecná pravidla pro správní uvážení. Správní orgán v případech, kdy mu zákon svěřuje možnost volné úvahy, musí vždy respektovat zákonné meze, tj. ve svých úvahách nesmí vybočit z mezí a hledisek stanovených zákonem. Přitom se smí opírat pouze o premisy zjištěné v řádném procesu a celá jeho úvaha musí být v souladu s pravidly logického usuzování. Pokud správní uvážení splní tyto předpoklady, nebyl by ani soud oprávněn dovodit z týchž skutečností jiné nebo přímo opačné závěry.[395]

Rovněž Kolouch, Bašta a kol. upozorňují v monografii CyberSecurity na problematické vymezení pojmu kybernetická bezpečnost, jakož i na zrádnost přístupu, který by ji svěřoval pouze odvětví informačních a komunikačních technologií. Kybernetickou bezpečnost vnímají spíše za součást bezpečnosti a krizového managementu, když útoky využívají vedle technického přístupu i sociální inženýrství a personální i objektové zabezpečení.[396]

Obecně lze mít za to, že bezpečnost označuje stav, v něm je minimalizováno jakékoli ohrožení chráněného objektu. Podle některých autorů lze považovat za primární objekt bezpečnosti stát.[397] Z hlediska mezinárodního společenství sestávajícího ze suverénních nezávislých států, které však nejsou rovné svým postavením ani vlivem, se každý stát snaží o zachování své suverenity, tj. aby ovládal své území a vykonával veřejnou moc nad vším, co se na tomto území nachází.[398]

Český zákonodárce vyšel z komplexního pojetí bezpečnosti státu, jež v sobě spojuje zahraniční politiku, vojenskou obranu a vnitřní bezpečnost a pořádek. Bezpečnostní systém v ČR zahrnuje zejména prezidenta republiky, Parlament ČR, vládu, Bezpečnostní radu státu a její pracovní orgány, ústřední správní úřady, krajské a obecní úřady, ozbrojené síly, ozbrojené bezpečnostní sbory, zpravodajské služby, záchranné sbory, záchranné služby a havarijní služby. Odpovědnost za zajišťování bezpečnosti státu a za řízení a funkčnost celého bezpečnostního systému nese vláda jako vrcholný orgán výkonné moci.[399]

Podle důvodové zprávy k ústavnímu zákonu o bezpečnosti ČR je jejím cílem *„všestranná péče o člověka, o jeho život, o dodržování lidských práv a svobod, o ochranu majetku a životních*

---

[395] Srov. rozsudky Nejvyššího správního soudu ze dne 22. 1. 2004, č. j. 5 Azs 47/2003-48, a ze dne 27. 11. 2003, č. j. 4 Azs 27/2003-55.

[396] KOLOUCH, Jan, BAŠTA, Pavel a kol. Op. cit., str. 39 - 40.

[397] PORADA, Viktor a kol. *Bezpečnostní vědy. Úvod do teorie a metodologie*. Plzeň: Aleš Čeněk, 2017, str. 64.

[398] Podrobněji ČEPELKA, Čestmír, ŠTURMA, Pavel. *Mezinárodní právo veřejné*. Praha: Eurolex Bohemia, 2003, str. 35 a násl.

[399] MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČR. *Bezpečnostní strategie České republiky 2015* [online]. Praha, 2015, str. 23. Dostupné: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf [Cit. 2022-11-06].

jistot a o zachovávání funkcí státu jako instituce, která zajišťuje bezpečnost."[400] Krizové situace se mohou týkat rozsáhlých živelných pohrom, průmyslových havárií a dalších nehod. Vzhledem k tomuto obecnému pojetí mohou být zapříčiněny kybernetickým útokem, který se může stát důvodem pro aktivaci jednotlivých ustanovení citovaného ústavního zákona. Ačkoli se kybernetické aktivity, včetně kybernetických útoků a kyberšpionáže, objevují čím dál častěji během mezinárodních politických i válečných konfliktů, dosud se nesetkáváme s tím, že by příčinou vyhlášení stavu ohrožení státu nebo válečného stavu byl toliko kybernetický incident či kybernetický útok.[401] Například v souvislosti s ozbrojeným konfliktem mezi Ruskou federací a Ukrajinou vzrostla v únoru 2022 i hrozba kybernetických útoků a kyberšpionáže v tuzemsku. NÚKIB proto vydal dne 25. února 2022 varování podle § 12 ZKB, v němž nabádá orgány a osoby řídící se zákonem o kybernetické bezpečnosti k ostražitosti a k zabezpečení informačních systémů a jejich komponent.[402]

Ústavní zákon o bezpečnosti ČR rozumí bezpečností státu zajištění jeho svrchovanosti, územní celistvosti a demokratických základů, jakož i ochrany životů, zdraví a majetkových hodnot. Podle čl. 1 citovaného ústavního zákona jde o základní povinnost státu. Při ohrožení uvedených hodnot lze podle citovaného ústavního zákona vyhlásit nouzový stav, stav ohrožení státu, a v případech a postupem dle čl. 43 Ústavy ČR i válečný stav. Povinnosti občanů a jiných subjektů v těchto případech stanoví zákon č. 222/1999 Sb., o zajišťování obrany České republiky, ve znění pozdějších předpisů (dále jen „zákon o zajišťování obrany ČR").[403] Státní orgány, orgány územních samosprávných celků a právnické a fyzické osoby jsou povinny se podílet na zajišťování bezpečnosti ČR.[404]

---

[400] VLÁDA. Důvodová zpráva k návrhu ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky, č. 110/1998 Dz.

[401] Vymezení kybernetického incidentu a kybernetického útoku rozebírá kapitola 2.3. Narušení bezpečnosti informací, služeb a sítí.

[402] Ředitel NÚKIB Karel Řehka k tomu uvedl: *„Informace, které máme k dispozici, vedou k důvodné obavě z reálné hrozby kyberšpionáže a kybernetických útoků na významné cíle v České republice, především na strategické instituce veřejné správy, prvky kritické informační infrastruktury, informační systémy základních služeb či média."* NÚKIB. *NÚKIB v rámci preventivních kroků vydal v souvislosti s ozbrojeným konfliktem mezi Ruskou federací a Ukrajinou Varování* [online]. Dostupné: https://www.nukib.cz/cs/uredni-deska/ [Cit. 2022-11-06].

[403] SYLLOVÁ, Jindřiška. Bezpečnost státu. In: HENDRYCH, Dušan a kol. *Právnický slovník*. Op. cit.

[404] Čl. 3 ústavního zákona o bezpečnosti České republiky.

2.1.3. Kybernetická bezpečnost

2.1.3.1. Definice

Kybernetická bezpečnost je a bude proměnlivou veličinou. Pojem kybernetické bezpečnosti nabývá, shodně jako pojem bezpečnosti, různého významu, neboť se vyvíjí v čase spolu s technologickými, společenskými i politickými proměnami společnosti. Objevují se názory, podle kterých nelze kybernetickou bezpečnost přesně definovat tak, aby pojem zahrnul veškeré aspekty.[405] Nejde pouze o otázku technologie; zásadní důležitosti nabývá i lidské chování.[406] Akt EU o kybernetické bezpečnosti definuje kybernetickou bezpečnost skrze *„činnosti nezbytné k ochraně sítí a informačních systémů, jejich uživatelů a dalších osob dotčených kybernetickými hrozbami."*[407]

Výslovnou definici kybernetické bezpečnosti v ZKB nenalezneme. Přesto lze z jeho jednotlivých ustanovení pojem přiblížit. ZKB v oblasti kybernetické bezpečnosti neukládá povinnosti pouze vybraným orgánům a osobám uvedeným v § 3. Kybernetickou bezpečnost ZKB zajišťuje skrze systém popsaný v Hlavě II., a především definuje stav kybernetického nebezpečí.[408] Pojem kybernetické bezpečnosti poté lze rekonstruovat skrze povinné subjekty, činnost a její účel.

V rámci kybernetické bezpečnosti jsou určené orgány a osoby povinny zavést a provádět bezpečnostní opatření, vyhledávat a hlásit kybernetické bezpečnostní události a incidenty i provádět reaktivní a ochranná opatření uložená ústředním správním orgánem pro kybernetickou bezpečnost, jímž je NÚKIB.[409] Zjednodušeně lze říci, že optikou ZKB představuje kybernetická bezpečnost činnost vybraných orgánů a osob, jež má zamezit, aby nastalo kybernetické nebezpečí. Kybernetickým nebezpečím se slovy zákona rozumí *„stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost služeb elektronických komunikací anebo bezpečnost a integrita sítí elektronických komunikací, a tím by mohlo dojít k porušení nebo*

---

[405] ENISA. *Definition of Cybersecurity: Gaps and overlaps in standardisation* [online], 2016, str. 7 - 10. Dostupné: https://www.enisa.europa.eu/publications/definition-of-cybersecurity [Cit. 2022-11-07]. Ostatně není ani shody na způsobu psaní tohoto pojmu v angličtině, když se objevují obě podoby: *Cybersecurity* i *Cyber Security.*

[406] Srov. rec. 8 nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA (Agentuře Evropské unie pro kybernetickou bezpečnost) a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií (akt o kybernetické bezpečnosti), dále jen „akt EU o kybernetické bezpečnosti". V souvislosti s lidským chováním se lze setkat i s pojmem kybernetická hygiena, s rutinními opatřeními s cílem minimalizace bezpečnostních rizik plynoucích z kybernetických hrozeb. Tamtéž.

[407] Čl. 2 odst. 1 aktu EU o kybernetické bezpečnosti.

[408] Hlava III, § 21 odst. 1 ZKB.

[409] Srov. §§ 4, 7, 8 a 11 ZKB.

došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací."[410]

Bezpečnost sítí i informačních systémů vnímá jako zásadní i směrnice NIS. Tuto bezpečnost definuje jako *„schopnost sítí a informačních systémů odolávat s určitou spolehlivostí veškerým zásahům, které narušují dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat nebo souvisejících služeb, které tyto sítě a informační systémy nabízejí nebo které jsou jejich prostřednictvím přístupné."*[411] Z hlediska bezpečnosti tedy právo EU považuje za klíčové dostupnost, autenticitu, integritu a důvěrnost dat a služeb. Agentura EU pro bezpečnost sítí a informací (ENISA) spojuje kybernetickou bezpečnost se zabezpečenou komunikací i informacemi, bezpečným provozem, ale též s fyzickou a vojenskou (veřejnou či národní) bezpečností. Zabezpečenou komunikací je podle ENISA ochrana technické infrastruktury kybernetického systému (*cyber system*) před změnami vedoucími k činnostem nezamýšleným vlastníky, vývojáři, či uživateli systému. Bezpečnost informací definuje jako ochranu uložených nebo přenášených dat před jejich krádeží, výmazem či změnami. Bezpečností provozu chápe ochranu před úmyslným narušením pracovních postupů v rozporu s úmyslem vlastníků, vývojářů či uživatelů. Fyzická bezpečnost představuje ochranu před jakoukoli fyzickou hrozbou, která by mohla ovlivnit chod kybernetického systému. Veřejná (národní) bezpečnost zahrnuje ochranu před hrozbou pocházející mimo kyberprostor, avšak která může ohrozit fyzické či kybernetické hodnoty způsobem, že útočník získá po politické, vojenské nebo strategické stránce.[412]

Národní strategie kybernetické bezpečnosti na období let 2015 až 2020 vymezila kybernetickou bezpečnost jako *„souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v České republice, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost."*[413] Pro následující léta již upozorňuje na civilně-vojenskou spolupráci v zabezpečování kyberprostoru a skutečnost, že zajišťování kybernetické bezpečnosti ČR pouze z pozice státu není dostačující. Svůj podíl má mít i soukromá sféra, ba každý jednotlivec. Právě koordinace a spolupráce se jeví být pro období 2021 až 2025 klíčovými: *„Zajišťování kybernetické bezpečnosti zahrnuje koordinaci množství státních i nestátních subjektů takovým způsobem, aby*

---

[410] § 21 odst. 1 ZKB.

[411] Čl. 4 odst. 2 směrnice NIS.

[412] ENISA. Op. cit., str. 11 - 12.

[413] NBÚ. *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 - 2020* [online], str. 5. Dostupné: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/ [2022-11-07].

mohla ČR účinně čelit i těm nejzávažnějším a nejkomplikovanějším výzvám a hrozbám."[414] Z toho je zřejmé, že se pojem kybernetické bezpečnosti v čase vyvíjí. Očekávat lze další rozšiřování povinností k zajištění kybernetické bezpečnosti i nárůst okruhu povinných subjektů.

Kolouch, Bašta a kol. upozorňují na omezení definice uvedené v Národní strategii kybernetické bezpečnosti na období let 2015 až 2020, jež plyne z jejího zaměření na český kyberprostor s tím, že opomíjí zabezpečení zájmů občanů ČR a dalších subjektů neusídlených v ČR.[415] Takové omezení však podle mého názoru z definice nevyplývá. Definice stanoví jako cíl zajistit zabezpečený, chráněný a odolný kyberprostor v ČR, avšak nepodává se v ní, že by toho mělo být dosaženo pouze opatřeními směřujícími toliko na český kyberprostor. Definice je propojena s českým ZKB, který implementuje evropskou směrnici o kybernetické bezpečnosti sítí a informačních systémů, jejímž smyslem je zajištění bezpečného kyberprostoru v celé EU. Proto obsahuje řadu harmonizačních ustanovení a prvků spolupráce mezi členskými státy.[416]

Smejkal a kol. definici kybernetické bezpečnosti neuvádějí. Kladou však důraz na kybernetické prostředí, v němž může docházet k různým útokům. Tyto útoky dělí na: 1. kyberterorismus, je-li cílem či nástrojem teroristického útoku informační nebo telekomunikační systém; 2. kybernetickou válku, jde-li o akt nepřátelství vyvolaný cizím státem; 3. kybernetickou kriminalitu, bude-li se jednat o *„kriminalitu v klasickém smyslu coby sofistikovanější druh trestné činnosti, často prováděnou v rámci organizovaného zločinu."*[417] Tato kategorizace však nepokrývá veškeré možné případy kybernetických útoků. Není například zcela zřejmé, do jaké kategorie zařadit kybernetický útok cizího státu odehrávající se v době míru s politickými motivy, jehož podstatou by byla manipulace výsledků voleb či překažení voleb v jiném státě. Ač by takový útok naplnil patrně více skutkových podstat trestného činu, bylo by zjednodušující označit jej za kriminalitu v klasickém slova smyslu.

2.1.3.2. Akt EU o kybernetické bezpečnosti

Snaha podnítit hospodářský růst a usnadnit dosažení jednotného digitálního trhu v EU vedla k přijetí nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA (Agentuře Evropské unie pro kybernetickou bezpečnost) a o certifikaci kybernetické

---

[414] NÚKIB. *Národní strategie kybernetické bezpečnosti České republiky na období let 2021 - 2025*. Op. cit., str. 10 - 11.

[415] KOLOUCH, Jan, BAŠTA, Pavel a kol. Op. cit., str. 43.

[416] Srov. shora subkapitolu 1.3.3. Principy práva kybernetické bezpečnosti.

[417] SMEJKAL, Vladimír, SOKOL, Tomáš, KODL, Jindřich. Op. cit., str. 25 - 28.

bezpečnosti informačních a komunikačních technologií (akt o kybernetické bezpečnosti). Hlavními důvody nového nařízení bylo zajištění bezpečného kybernetického prostředí, jež by rozvíjelo jednotný digitální trh, a tím i hospodářství celé EU. Přes rostoucí počty zařízení připojených v EU k Internetu nejsou vždy využívány bezpečnostní prvky, což je podle Komise důvodem nižší kybernetické bezpečnosti a narušení důvěry v digitální produkty, služby a zařízení používané občany, organizacemi i podniky v EU.[418] S ohledem na častou přeshraniční povahu kybernetických incidentů bylo zapotřebí upravit též kompetence a opatření s cílem zabezpečit *„účinnou a koordinovanou reakci a řešení krizí na úrovni Unie."*[419]

Akt EU o kybernetické bezpečnosti cílí zejména na zajištění spolupráce, koordinace a sdílení informací mezi členskými státy a institucemi EU. Jak podotýká Birkinshaw, sdílení informací je výhodné tehdy, pokud jím lze zabránit páchání závažné trestné činnosti, zajistit výkon práva, zlepšit veřejnou správu, lépe chránit zranitelné osoby i sdílet informace za výzkumnými a statistickými účely. Problém však nastává, pokud nepanuje shoda na konkrétních důvodech, pro které mají vzniknout informační databáze, jakož i tehdy, nejsou-li data dostatečně zabezpečena.[420] Způsob sdílení informací musí současně respektovat soukromí a zajistit dostatečnou ochranu osobních údajů, jakož i transparentnost a kontrolu celého procesu analýzy, zpracování a sdílení informací.[421]

Akt EU o kybernetické bezpečnosti zřizuje evropský rámec pro certifikaci kybernetické bezpečnosti. Smyslem je mimo jiné „*vytvořit mechanismus pro zřizování systémů certifikace, které osvědčují, že produkty, služby a procesy informačních a komunikačních technologií hodnocené v souladu s takovými systémy splňují stanovené bezpečnostní požadavky, pokud jde o ochranu dostupnosti, autentičnosti, integrity nebo důvěrnosti uchovávaných, předávaných či zpracovávaných údajů nebo funkcí či služeb nabízených nebo přístupných prostřednictvím těchto produktů, služeb a procesů během celého jejich životního cyklu."*[422]

Jednotná certifikace v rámci EU by měla zajistit společnou úroveň kybernetické bezpečnosti s tím, že organizace, výrobci i poskytovatelé služeb, kteří se zabývají navrhováním a vývojem

---

[418] Srov. rec. 2 a 3 aktu EU o kybernetické bezpečnosti.

[419] Rec. 5 aktu EU o kybernetické bezpečnosti.

[420] Podrobněji BIRKINSHAW, Patrick. Op. cit., str. 4 a násl.

[421] Podrobněji ZARSKY, Tal Z. Op. cit. Kontrolu zdůrazňuje i Komise EU ve vztahu k ochraně základních práv v době digitalizace. KOMISE EU. *2021 annual report on the application of the Charter of fundamental rights* [online]. Dostupné: https://ec.europa.eu/info/files/2021-annual-report-application-charter-fundamental-rights_en [Cit. 2022-11-08].

[422] EUR-LEX. *Akt EU o kybernetické bezpečnosti: Shrnutí dokumentů* [online]. Dostupné https://eur-lex.europa.eu/legal-content/CS/LSU/?qid=1652275836404&uri=CELEX%3A32019R0881 [Cit. 2022-11-08].

produktů a služeb ICT, by měli zajišťovat bezpečnostní opatření ihned od počátečních fází vývoje. Postup lze označit anglickým termínem *security by design*.[423] Zabezpečení hlavních protokolů a infrastruktury otevřeného Internetu lze považovat za globální veřejný statek, v jehož ochraně by měla hrát klíčovou úlohu agentura ENISA. Nařízení stanovuje cíle, úkoly a organizační strukturu agentury ENISA, která by měla *„podpořit bezpečnost veřejného jádra otevřeného internetu a stabilitu jeho fungování, včetně klíčových protokolů (zejména DNS, BGP, a IPv6), provozu systému doménových jmen (včetně provozu všech domén na vrcholné úrovni) a provozu root zone."*[424] V praxi by měla agentura ENISA mimo jiné zajišťovat jednotné provádění právních předpisů EU (zejména směrnice NIS), nabízet členským státům podporu, rozvoj a školení v oblasti kybernetické bezpečnosti, a podněcovat spolupráci mezi veřejným a soukromým sektorem. V rámci členských států je na základě čl. 58 aktu EU o kybernetické bezpečnosti činný vždy jeden nebo více vnitrostátních orgánů certifikace kybernetické bezpečnosti. Citovaný článek nařízení vstoupil v platnost 28. 6. 2021.[425] Certifikační správní orgány by měly mít dostatečnou pravomoc k provádění dohledu a prosazování požadovaných bezpečnostních pravidel. Čl. 58 odst. 1 aktu EU o kybernetické bezpečnosti přitom umožňuje přenést odpovědnost v rámci certifikace kybernetické bezpečnosti i na správní orgán jiného členského státu, pokud by s tím dotyčný členský stát souhlasil. Orgánem certifikace kybernetické bezpečnosti v ČR se stal NÚKIB a jeho pravomoc tak byla rozšířena o rozhodování o žádostech o autorizaci subjektu posuzování shody a o pozastavení vykonatelnosti, o změně nebo o zrušení rozhodnutí o autorizaci.[426]

Můžeme předpokládat, že unijní certifikační schémata kybernetické bezpečnosti ovlivní trh s ICT produkty, službami a procesy, a to důrazem na bezpečnější řešení. Správně nastavená bezpečnostní pravidla a podmínky pro získání osvědčení by měla přispět ke zvýšení dostupnosti, integrity i důvěrnosti informací. Využití evropské certifikace kybernetické bezpečnosti je dobrovolné, ledaže by povinnost certifikace stanovilo vnitrostátní nebo unijní právo.[427] Vzhledem k dlouhodobějšímu trendu kladoucímu důraz na kybernetickou bezpečnost však lze do budoucna očekávat stanovení případů, kdy bude vnitrostátní právo certifikaci vyžadovat.

---

[423] Podrobněji srov. níže subkapitolu 2.1.3.5. Akční plán k Národní strategii kybernetické bezpečnosti 2021-2025.

[424] Rec. 23 aktu EU o kybernetické bezpečnosti.

[425] Čl. 69 odst. 2 aktu EU o kybernetické bezpečnosti.

[426] Projednávání původního sněmovního tisku 1100 nebylo v minulém volebním období dokončeno. Současný vládní návrh, který je projednáván v Poslanecké sněmovně, obsahuje oproti předchozímu pouze adaptační právní úpravu. C. H. BECK. Certifikace kybernetické bezpečnosti. *Právní zpravodaj*, 8. 2. 2022. Dostupné: beck-online.cz [Cit. 2022-11-08].

[427] Srov. Rec. 91 aktu EU o kybernetické bezpečnosti.

2.1.3.3 Nařízení o Evropské síti a centru kompetencí pro kybernetickou bezpečnost

S cílem zvýšit kompetence členských států v oblasti kybernetické bezpečnosti, a tím i konkurenceschopnost průmyslu EU, došlo k přijetí nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center (dále jen „nařízení o kompetenčním centru").

Smyslem nařízení o kompetenčním centru, které platí od 28. 6. 2021, je vybudovat v EU odbornou akademickou, výzkumnou i průmyslově orientovanou komunitu pro podporu technologií v oblasti kybernetické bezpečnosti.[428] Kromě zřízení Evropského centra kompetencí pro kybernetickou bezpečnost, jehož sídlem byla zvolena rumunská Bukurešť,[429] mají v členských státech vzniknout národní koordinační centra, jimž stanovilo nařízení o kompetenčním centru pravidla fungování. Tato vnitrostátní centra by měla pro členský stát působit nejen ve smyslu podpory výzkumu, technologického pokroku a vzdělávání v oblasti kybernetické bezpečnosti, nýbrž by se měla stát i místem praktického využití znalostí díky poskytování technické pomoci v projektech řízených Evropským centrem kompetencí. Vnitrostátní centra by měla dále nabízet odborné znalosti, spolupracovat na zahraničních projektech a podílet se na výzkumných činnostech podporovaných evropskými granty. Podle nařízení o kompetenčním centru se má jednat o *„subjekt veřejného sektoru, nebo subjekt ve většinovém vlastnictví členského státu, který vykonává funkce veřejné správy podle vnitrostátních právních přepisů, včetně prostřednictvím přenesení pravomoci"*.[430] Tento subjekt musí být rovněž schopen plnit cíle nařízení, tj. disponovat odbornými výzkumnými a technologickými znalostmi v oblasti kybernetické bezpečnosti (případně k nim mít přístup), jakož i efektivně spolupracovat a koordinovat svou činnost s agenturou ENISA i s průmyslem, veřejným sektorem, akademickou obcí, výzkumnou komunitou a občany.[431] V ČR zajišťuje vznik národního koordinačního centra NÚKIB.[432]

---

[428] Čl. 3 nařízení o kompetenčním centru.

[429] RADA EU. *Výběr sídla Evropského centra kompetencí pro kybernetickou bezpečnost* [online]. Dostupné: https://www.consilium.europa.eu/cs/policies/cybersecurity/seat-selection-cybersecurity-centre/ [Cit. 2022-10-16].

[430] Čl. 6 odst. 5 nařízení o kompetenčním centru.

[431] Tamtéž.

[432] NÚKIB. *Národní výzkum a vývoj* [online]. Dostupné: https://nukib.cz/cs/kyberneticka-bezpecnost/vyzkum/narodni-vyzkum-a-vyvoj/ [Cit. 2022-10-17].

Komunita budovaná na základě nařízení o kompetenčním centru připomíná do určité míry instituci podobnou Akademii věd, avšak na úrovni EU a orientovanou na kybernetickou bezpečnost. Zdá se však, že předním důvodem k přijetí nařízení o kompetenčním centru byla především snaha podpořit podniky a průmysl v odvětví kybernetické bezpečnosti. To by současně mělo vést i k ekonomickému rozvoji a vyššímu zabezpečení podniků před kybernetickými hrozbami v rámci EU. Nařízení o kompetenčním centru má totiž reagovat na zvyšující se výskyt kybernetických hrozeb a bezpečnostních incidentů lepším zabezpečením informačních a komunikačních sítí a systémů v EU, což má zásadní význam pro evropskou společnost i hospodářství. Současně si klade za cíl změnit v oblasti kybernetické bezpečnosti závislost EU na neevropských dodavatelích a zajistit, aby si EU *„udržela a rozvíjela důležité výzkumné a technologické kapacity v oblasti kybernetické bezpečnosti, aby mohla zabezpečit sítě a informační systémy občanů a podniků, a zejména chránit kritické sítě a informační systémy a poskytovat klíčové služby v oblasti kybernetické bezpečnosti."*[433] Důraz na bezpečné dodavatelské řetězce v oblasti ICT se ukazuje v současnosti jako klíčový požadavek i s ohledem na geopolitickou situaci v Evropě.[434]

Kybernetické hrozby definuje nařízení o kompetenčním centru poměrně široce jako jakoukoliv potenciální okolnost, událost nebo čin, které by mohly poškodit, narušit nebo jinak nepříznivě ovlivnit sítě a informační systémy, jejich uživatele a další osoby.[435] Díky zvýšení důvěry a bezpečnosti, včetně důvěrnosti, integrity a dostupnosti údajů, má dojít i ke zvýšení globální konkurenceschopnosti EU v oblasti kybernetické bezpečnosti. Přínosem by měla být i lepší bezpečnost kritické infrastruktury. Pravomocí členských států z oblastí veřejné bezpečnosti, obrany, národní bezpečnosti a trestního práva, se však nařízení o kompetenčním centru nedotýká. Upravuje především organizační a finanční aspekty fungování Evropského centra kompetencí a vnitrostátních koordinačních center.

---

[433] Rec. 6 nařízení o kompetenčním centru.

[434] Viz prohlášení předsedkyně Komise EU Ursuly von der Leyen při zahájení Prague Cyber Security konference v listopadu 2022: *„Bezpečná digitální budoucnost vyžaduje nejen silnou kybernetickou obranu, ale mnohem víc. Vyžaduje zabezpečenou infrastrukturu, spolehlivé partnery a odolné dodavatelské řetězce. A na tom Evropa pracuje.*" NÚKIB. *V Praze proběhla prestižní Prague Cyber Security Conference* [online], 4. 11. 2022. Dostupné: https://nukib.cz/cs/infoservis/aktuality/1903-v-praze-probehla-prestizni-prague-cyber-security-conference/ [Cit. 2022-11-08].

[435] Čl. 2 bod 4) nařízení o kompetenčním centru.

2.1.3.4. Národní strategie kybernetické bezpečnosti 2021-2025

Za funkčnost bezpečnostního systému ČR odpovídá vláda jako vrcholný orgán moci výkonné. NÚKIB jako gestor kybernetické bezpečnosti v ČR a ústřední orgán státní správy[436] pro oblast kybernetické bezpečnosti, ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany, připravuje na pětiletá období Národní strategie kybernetické bezpečnosti. Tyto strategie jsou určeny především pro bezpečnostní složky státu a další subjekty veřejné správy při zajišťování kybernetické bezpečnosti státu[437] a jsou konkretizovány Akčním plánem kybernetické bezpečnosti České republiky.[438]

Podle Národní strategie kybernetické bezpečnosti České republiky na období let 2021 - 2025 (dále též jen „Strategie") dochází k nárůstu intenzity využívání kyberprostoru při prosazování zahraničně-politických zájmů států. Zejména státní instituce v ČR jsou dlouhodobě cílem kybernetické špionáže. Roste i riziko průmyslové špionáže v podnicích, akademické a výzkumné sféře, a to s cílem oslabit konkurenceschopnost ČR. Strategie hovoří dále o nárůstu významu kyberprostoru při vojenských operacích. Důraz klade na schopnost ČR adaptovat se proměnlivému bezpečnostnímu prostředí, přičemž uvádí: *„v kyberprostoru proto bude ČR vystupovat na vládní úrovni asertivně a rozhodně. Sebevědomým, zodpovědným přístupem ke kybernetické bezpečnosti na národní úrovni bude ČR posilovat svou prosperitu a navíc bude i nadále silným spojencem pro své partnery na mezinárodní úrovni."*[439]

Vedle NÚKIB (který plní úkoly vládního CERT) a sdružení CZ.NIC (jež provozuje národní CERT) se podílí na zajištění kybernetické bezpečnosti ČR z hlediska zahraniční politiky i Ministerstvo zahraničních věcí a zpravodajské služby. Bezpečnostní informační služba (dále jen „BIS"), Vojenské zpravodajství (dále jen „VZ") a Úřad pro zahraniční styky a informace (dále jen „ÚZSI") získávají a analyzují klíčové informace, přičemž VZ odpovídá i za kybernetickou obranu ČR. Na té se zároveň podílí Armáda ČR, a sice Velitelství kybernetických sil a informačních operací. Prevenci a postih kybernetické kriminality zajišťuje Policie ČR, především Národní centrála proti organizovanému zločinu Služby kriminální policie a vyšetřování.[440] Zajišťování

---

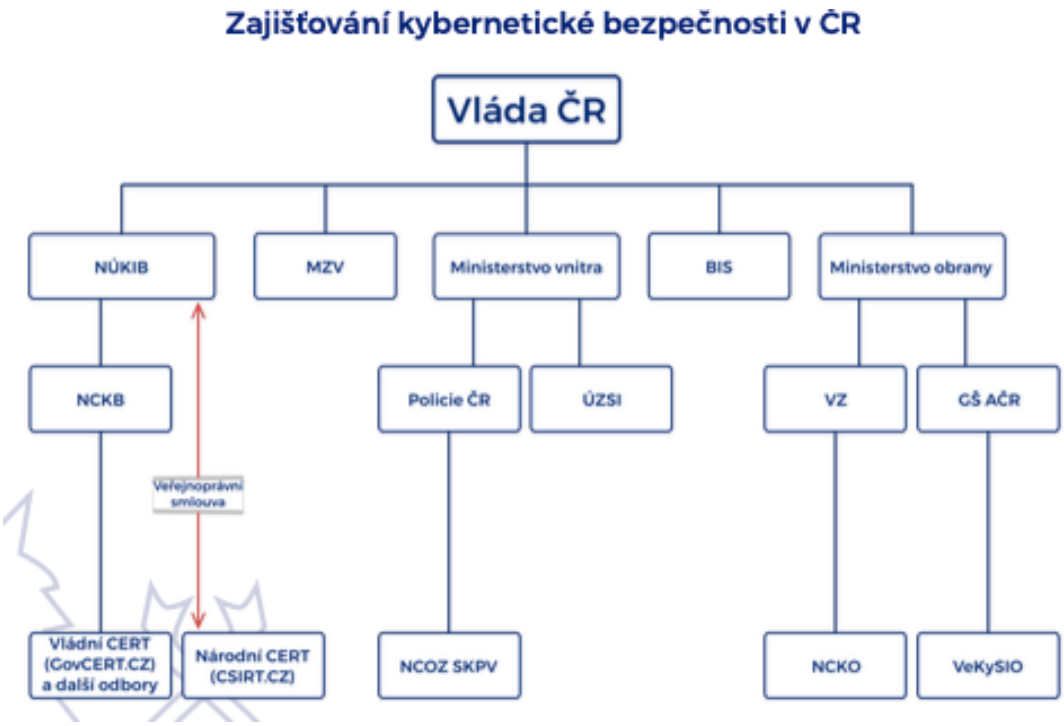
[436] Srov. § 2 zákona České národní rady č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění pozdějších předpisů.

[437] NÚKIB. *Národní strategie kybernetické bezpečnosti České republiky na období let 2021 - 2025*. Op. cit., str. 3.

[438] Tamtéž, str. 4.

[439] Tamtéž, str. 10.

[440] Tamtéž, str. 5 - 8.



kybernetické bezpečnosti tudíž představuje komplexní systém, na němž se podílí vedle NÚKIB vícero orgánů státní správy, jak dokládá i následující schéma:

Zdroj: NÚKIB. *Národní strategie kybernetické bezpečnosti České republiky na období let 2021 - 2025* [online], str. 8. Dostupné: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/ [Cit. 2022-03-05].

Další ústřední správní úřady, správní orgány i soukromé subjekty ovlivňují kybernetickou bezpečnost v rámci své působnosti a odpovídají za zajištění souladu svých činností s právními předpisy. S ohledem na komplexnost a vzájemnou provázanost systému zajištění kybernetické bezpečnosti v ČR lze odkázat na příměr Sira Arthura Conana Doyla, vložený do úst doktora Watsona, a sice že každý řetěz je silný právě jen tolik jako jeho nejslabší článek.[441] Vzájemná spolupráce, sdílení informací i koordinace zabezpečení se proto jeví z hlediska zájmů ČR klíčová.

Strategie rozeznává vzájemnou provázanost a zranitelnost bezpečnostních infrastruktur (zmiňuje „kaskádový" efekt). Proto považuje za stěžejní chránit a zabezpečit povinné subjekty podle ZKB, o nichž hovoří jako o *„stěžejním pilíř[i] kybernetické, potažmo národní bezpečnosti"*.[442] Zvláště důležitá je kybernetická bezpečnost průmyslových řídících a SCADA systémů[443] a cloudových funkcí. Význam je přisouzen i aktivní mezinárodní spolupráci na atribuci škodlivých aktivit v kyberprostoru konkrétním aktérům a jednotné komunikaci navenek, s cílem zamezit zneužití informačních mezer k manipulacím, podrývání důvěry v schopnosti státu a šíření strachu mezi obyvateli.[444] Otázkou zůstává, jakým způsobem tak ČR hodlá činit a zda reakce, kdy

[441] DOYLE, Arthur Conan. *Údolí strachu* [online]. 1. vyd. Praha : Městská knihovna v Praze, 2012, str. 9. Dostupné: <http://web2.mlp.cz/koweb/00/03/34/76/87/udoli_strachu.pdf> [Cit. 2022-11-08].

[442] NÚKIB. *Národní strategie kybernetické bezpečnosti České republiky na období let 2021 - 2025*. Op. cit., str. 11.

[443] Anglická zkratka SCADA, tj. *Supervisory Control and Data Aquisition*, označuje průmyslové systémy dispečerského řízení a sběru dat, díky nimž lze centrálně monitorovat a ovládat jiná technická zařízení.

[444] NÚKIB. *Národní strategie kybernetické bezpečnosti České republiky na období let 2021 - 2025*. Op. cit., str. 12 - 13.

vláda „doporučí" blokování v českém prostředí dlouze působících dezinformačních webů, odpovídá proklamované strategii.[445]

Vedle podpory dostatečných technických i personálních kapacit má být cílem ČR rovněž účinná mezinárodní spolupráce a aktivní prosazování národních zájmů a bezpečnosti ČR v rámci mezinárodních společenství, jako je EU, NATO, OBSE, OSN i OECD. S vybranými spojenci hodlá ČR nadále rozvíjet úzkou bilaterální spolupráci s cílem sdílet strategické informace a společné postupy proti nepřátelským aktivitám cizích mocností, ale i posílit mezinárodní justiční spolupráci v trestním řízení a vymahatelnost práva. Přitom se počítá i s nestátními „škůdci" a s preventivními opatřeními v kyberprostoru proti škodlivému jednání státních i nestátních aktérů. Vzhledem k globálnímu charakteru hrozeb v kyberprostoru ČR hodlá pomáhat s navyšováním odolnosti kybernetické bezpečnosti i v rozvojových zemích.[446]

Ve vztahu k veřejné správě Strategie poukazuje na probíhající digitalizaci veřejné správy a s tím související nutnost zajistit v infrastrukturách od počátku kybernetickou bezpečnost. Kromě bezpečnosti informačních kanálů veřejné správy je zdůrazněna i nutnost garantovat dostupnost a plynulost služeb.[447] Dalším aspektem má být podpora a investice do vzdělávání a kvalifikované pracovní síly. Orgány státní správy by proto měly investovat do náboru stávajících talentů a vytvářet odpovídající pracovní podmínky. Strategie výslovně uvádí: *„Státní správa musí být konkurenceschopná na vysoce konkurenčním trhu práce v oblasti kybernetické bezpečnosti. Musí vytvořit takové pracovní prostředí, které motivuje stávající talenty k rozhodnutí pracovat pro státní organizace, potažmo bezpečnostní složky státu."*[448] Platové podmínky upravené nařízením vlády č. 341/2017, o platových poměrech zaměstnanců ve veřejných službách a správě, v platném znění, však nejsou schopny odměnám v soukromé sféře konkurovat, a to tím spíše ve velkých městech, kde správní úřady sídlí.

---

[445] V souvislosti s probíhající válkou na Ukrajině a agresí Ruské federace došlo k zablokování dezinformačních webů (např. Protiproud) na základě rozhodnutí soukromého sdružení CZ.NIC i v důsledku stanoviska vlády ČR. DIMUN, Petr. *O blokování „dezinformačních" webů vláda nerozhodla, chybí zákonná úprava* [online]. Česká justice, 3. března 2022. Dostupné: https://www.ceska-justice.cz/2022/03/o-blokovani-dezinformacnich-webu-vlada-nerozhodla-chybi-zakonna-uprava/ [Cit. 2022-11-08].

[446] NÚKIB. *Národní strategie kybernetické bezpečnosti České republiky na období let 2021 - 2025.* Op. cit., str. 16 - 17. V rámci posílení mezinárodní spolupráce i neformálních vztahů, ale i úrovně technické expertízy, pořádá NÚKIB řadu kybernetických cvičení, kde dochází k simulaci krizových situací. Podrobněji NÚKIB. *Kybernetická cvičení* [online]. Dostupné: https://www.nukib.cz/cs/kyberneticka-bezpecnost/cviceni/kyberneticka-cviceni/ [Cit. 2022-11-08].

[447] NÚKIB. *Národní strategie kybernetické bezpečnosti České republiky na období let 2021 - 2025.* Op. cit., str. 18.

[448] Tamtéž, str. 20.

2.1.3.5. Akční plán k Národní strategii kybernetické bezpečnosti 2021 - 2025

Konkrétní úkoly vytčené v souladu s cíli uvedenými ve Strategii stanoví Akční plán k Národní strategii kybernetické bezpečnosti ČR na období let 2021 až 2025 (dále jen „Akční plán").[449] Na zajištění úkolů v rámci kybernetické bezpečnosti se podílí široká škála orgánů státní správy. Jejich výčet stanoví vláda, která Akční plán schvaluje svým usnesením. Mezi subjekty odpovědnými za plnění jednotlivých úkolů patří kromě NÚKIB další ústřední orgány státní správy; z ministerstev to jsou Ministerstvo obrany, Ministerstvo vnitra, Ministerstvo zahraničních věcí, Ministerstvo průmyslu a obchodu, Ministerstvo financí, Ministerstvo zdravotnictví, Ministerstvo spravedlnosti, Ministerstvo pro místní rozvoj, Ministerstvo školství, mládeže a tělovýchovy, Ministerstvo dopravy a Ministerstvo práce a sociálních věcí. Z dalších ústředních správních úřadů to jsou Národní bezpečnostní úřad, Státní úřad pro jadernou bezpečnost, Úřad pro ochranu osobních údajů a Český telekomunikační úřad. Odpovědnými subjekty jsou dále Úřad vlády ČR a Vládní zmocněnec pro IT a digitalizaci, Policie ČR, Nejvyšší i Vrchní státní zastupitelství, Celní správa, Generální inspekce bezpečnostních sborů, Vězeňská služba, Justiční akademie, Úřad pro civilní letectví, Generální ředitelství Hasičského záchranného sboru, Český institut pro akreditaci, Technologická agentura ČR i Technologické centrum Akademie věd ČR, Česká rozvojová agentura, Armáda ČR, Vojenské zpravodajství, Bezpečnostní a informační služba i Úřad pro zahraniční styky a informace.

Řada úkolů si klade za cíl zajistit vzájemnou spolupráci jednotlivých odpovědných subjektů a sjednocení jejich postupů. Například k zabezpečení národní kybernetické bezpečnosti se navrhuje zamezit tuzemskému působení vysoce rizikových dodavatelů v systémech regulovaných ZKB i obecně na úrovni realizace telekomunikačních sítí nových generací. Kteří dodavatelé jsou pro kybernetickou bezpečnost vysoce riziková, má navrhnout NÚKIB ve spolupráci s Ministerstvem průmyslu a obchodu, Ministerstvem vnitra a Ministerstvem zahraničních věcí, a ve spolupráci s Českým telekomunikačním úřadem i zpravodajskými službami. Pro zabezpečení případného rychlého obstarání technických a programových prostředků k nasazení protiopatření a k provádění reaktivních a ochranných opatření Akční plán ukládá Ministerstvu vnitra, NÚKIB a Ministerstvu pro místní rozvoj zpracovat analýzu právních možností operativního nákupu prostředků.

Spolupráce má být zajišťována na mezinárodní úrovni, zejména v rámci NATO a EU. Spolupráce má být posílena i v rámci středoevropského a východoevropského regionu a oblasti západního Balkánu. Akční plán počítá i s vysíláním tzv. kyberatašé a národních expertů do zahraničí

[449] NÚKIB. *Akční plán k Národní strategii kybernetické bezpečnosti ČR na období let 2021 až 2025* [online]. Dostupné: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/ [Cit. 2022-11-08].

k prohloubení spolupráce s klíčovými partnery, což mají být zejména členské státy EU, USA, Izrael, Jižní Korea, či Austrálie. Objevuje se dokonce spojení „aktivní kybernetická diplomacie", jejímž prostřednictvím má ČR přispívat k prosazování stávajícího mezinárodního práva a nezávazných norem upravujících odpovědné chování států v kyberprostoru.[450] V rámci mezinárodního prostředí se má ČR profilovat z hlediska kybernetické bezpečnosti i obrany jako aktivní stát s expertní kapacitou. Vedle pořádání mezinárodních cvičení a konferencí v oblasti kybernetické bezpečnosti jde též o monitoring a rozvoj právní úpravy, výměnu informací a sdílení zkušeností, či posílení kapacit třetích zemí v rámci zahraniční rozvojové spolupráce a ekonomické diplomacie.

Akční plán se věnuje i zajištění odolné veřejné správy. Odpovědné subjekty státní správy mají zajistit přístup *security by design*.[451] *Security by design* charakterizuje programátorskou architekturu, jež se snaží předcházet problémům se zabezpečením. Obvykle se zmiňují tři hlavní důvody narušení bezpečnosti počítačového programu: škodlivý úmysl (*malice*), hloupost (*mistake*) a nešťastná náhoda (*mischance*); průvodními jevy může být zničení či ztráta dat, únik informací i podvodné jednání.[452] Jde o vytváření software, který je od samého základu navržen bezpečně a jeho znalost nemá vést ke zneužití programátorských chyb. Rovněž má dojít ke sdílení zkušeností a spolupráci na bezpečném rozvoji tzv. Smart Cities v ČR[453] i k jednotné kontrole systémů e-Governmentu skrze Vládní dohledové centrum. Zavádění moderních informačních a komunikačních technologií do řízení obcí a měst, např. do odpadového hospodářství, dopravy či energetiky, si klade za cíl zlepšit kvalitu bydlení v daném místě díky snaze o zlepšení ekonomických a energetických procesů i životního prostředí. Nelze však opomenout související nároky na zabezpečení moderních IT systémů, která budou řídit v chytrých městech nejrůznější procesy.

Ve vztahu ke kybernetické obraně zmiňuje Akční plán působení Armády ČR a Vojenského zpravodajství. Současný Akční plán v bodě 23 rozvádí oprávnění Vojenského zpravodajství poměrně obecně: *„Pokračovat v posilování systému kybernetické obrany prostřednictvím budování schopností NCKO jako součásti VZ se zaměřením na logistické, personální a finanční zabezpečení,*

---

[450] NÚKIB. *Akční plán k Národní strategii kybernetické bezpečnosti ČR na období let 2021 až 2025*. Op. cit., str. 13, bod 70.

[451] Tamtéž, str. 15.

[452] WOODS, Eoin. *Secure by Design - the Architect's Guide to Security Design Principles* [online]. GOTO 2016. Dostupné: https://www.youtube.com/watch?v=4qN3JBGd1g8 [Cit. 2022-11-08].

[453] Koncept Smart Cities, neboli „chytrých měst", značí přístup k chytřejšímu řízení měst, obcí, regionů a života v nich prostřednictvím zavádění moderních technologií. Podrobněji MMR. *Jak využít chytrá řešení ve vašem městě?* [online]. Dostupné: https://mmr.cz/cs/microsites/sc/smart-cities [Cit. 2022-11-08].

ale i další aspekty důležité pro jeho efektivní fungování."[454] Oprávnění Vojenského zpravodajství v této oblasti se stalo předmětem kritiky, když pro předchozí období let 2015 - 2020 Akční plán předpokládal vznik Národního centra kybernetických sil zajišťujícího kybernetickou obranu ČR v případě hybridního konfliktu i provádění vojenských operací v kyberprostoru na podporu zahraničních misí v rámci NATO i EU. Nebylo však zřejmé, na základě jakého podkladu se tak mělo dít, respektive objevovala se kritika, že se tak stalo bez zákonného podkladu v rozporu s principem enumerativnosti veřejnoprávních pretencí dle čl. 2 odst. 3 Ústavy ČR.[455] V následujícím textu bude pojednáno o uvedeném oprávnění Vojenského zpravodajství.

2.1.4. Kybernetická obrana

2.1.4.1. Definice

Zatímco kybernetická bezpečnost si klade za cíl zajistit odolné informační systémy a sítě, jež jsou klíčové pro fungování státu, respektive pro jeho zásadní společenské a ekonomické činnosti, kybernetická obrana má aktivně reagovat na případné ohrožení státu. Vláda ČR se roku 2015 rozhodla svěřit kybernetickou obranu Vojenskému zpravodajství, v jehož rámci vzniklo Národní centrum kybernetických sil, následně přejmenované na Národní centrum kybernetických operací („NCKO").[456] Ministerstvo obrany k tomu na svých webových stránkách uvedlo: *„Kybernetické síly budou tedy sloužit potřebám armády a souviset striktně s její činností, kdežto Národní centrum kybernetických operací je institucí určenou ke komplexnímu zajišťování kybernetické obrany České republiky. … Kybernetická obrana, kterou má v gesci Vojenské zpravodajství, je samostatnou oblastí širšího konceptu kybernetické bezpečnosti a zároveň oblastí širšího konceptu zajištění obrany státu. Jejím úkolem je v případě potřeby aktivně působit v kybernetickém prostoru proti útočníkům. Specifikem kybernetické obrany je skutečnost, že bude prováděna jak v případě vyhlášení mimořádných stavů, především formou součinnosti s ostatními složkami zajišťujícími obranu ČR, tak i nepřetržitě mimo tyto stavy."*[457]

Zákonný podklad pro činnosti Vojenského zpravodajství při zajišťování kybernetické obrany ČR skýtá čtvrtá část zákona č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších

---

[454] NÚKIB. *Akční plán k Národní strategii kybernetické bezpečnosti ČR na období let 2021 až 2025.* Op. cit., str. 6.

[455] SMEJKAL, Vladimír, SOKOL, Tomáš, KODL, Jindřich. Op. cit., str. 31 - 32.

[456] MO. *Národní centrum kybernetických operací vypracovalo strategii kybernetické obrany ČR* [online], 6. 8. 2018. Dostupné: https://mocr.army.cz/informacni-servis/zpravodajstvi/narodni-centrum-kybernetickych-operaci-vypracovalo-strategii-kyberneticke-obrany-cr-201906/ [Cit. 2022-11-09].

[457] Tamtéž.

předpisů (dále jen „ZVZ"). Zmíněná část čtvrtá, tj. ustanovení §§ 16a až 16n, se dostala do ZVZ teprve přijetím zákona č. 150/2021 Sb., kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, a některé další zákony. Tato novela ZVZ nabyla účinnosti 1. 7. 2021. Vojenské zpravodajství však bylo na poli kybernetické obrany ČR činné již před tímto datem, což je patrné nejen z webu Ministerstva obrany, ale i z Akčního plánu z let 2015 - 2020, který uváděl činnost Národního centra kybernetických sil od počátku roku 2016.[458] Podle informací uvedených na webu Ministerstva obrany mělo dojít ke svěření kybernetické obrany Vojenskému zpravodajství na základě rozhodnutí vlády z roku 2015. Zmíněné rozhodnutí přitom nelze mezi zveřejněnými dokumenty z jednání vlády dohledat.[459] Nezbytné podmínky pro realizaci úkolů stanovených v Akčním plánu k Národní strategii kybernetické bezpečnosti ČR na období let 2015 až 2020 tudíž byly uzákoněny až na základě novely z roku 2021, tj. teprve po skončení platnosti zmíněného akčního plánu. Současně se zdá, že před zmíněnou novelizací bylo Národní centrum kybernetických sil činné, aniž by dané pravomoci byly Vojenskému zpravodajství zákonem svěřeny.

2.1.4.2. Zákonná pravomoc Vojenského zpravodajství - detekce, vyhodnocení i reakce na kybernetické útoky a hrozby

Čl. 3 odst. 2 ústavního zákona o bezpečnosti ČR ukládá státním orgánům povinnost podílet se na zajišťování bezpečnosti ČR; rozsah povinností a další podrobnosti má stanovit zákon. Podmínky zajišťování bezpečnosti ČR v kybernetickém prostoru nyní upravuje též ZVZ. Počínaje 1. červencem 2021 se Vojenské zpravodajství, a to nad rámec své zpravodajské činnosti a narozdíl od ostatních zpravodajských služeb, podílí přímo také na kybernetické obraně ČR. Na webu Vojenského zpravodajství se uvádí: *„Obrana je soubor opatření chránící stát a jeho občany před vnějším napadením. Kybernetický prostor je prostor informací. Takže jak už samotný název instituce napovídá, v případě „Vojenského zpravodajství" jsou naplněny základní požadavky, tedy že se jedná o řešení obranných / vojenských skutečností na poli informací. Národní centrum kybernetických operací, které Vojenské zpravodajství v souvislosti s tímto novým vládním úkolem buduje, plní jen dílčí roli na zajištění celkové bezpečnosti státu a občanů v kybernetickém prostoru.*

[458] NÚKIB. *Akční plán k Národní strategii kybernetické bezpečnosti ČR na období let 2015 až 2020.* Op. cit., str. 15.

[459] Mezi dokumenty zveřejněnými z jednání vlády v roce 2015 se nachází sice usnesení č. 79 ze dne 4. 2. 2015, jímž vláda schválila Bezpečnostní strategii České republiky 2015, v níž se hovoří o hrozbě kybernetických útoků a Národní strategii kybernetické bezpečnosti na období let 2015 až 2020, to však pouze v obecných termínech. Pravomoci Vojenského zpravodajství v něm nejsou zmiňovány vůbec. Srov. dokumenty z jednání vlády v archivu Úřadu vlády ČR dostupné v Aplikaci ODok: VLÁDA. *Jednání vlády - archiv* [online]. Aplikace ODok. Dostupné: https://apps.odok.cz/djv-agenda-list?year=2022 [Cit. 2022-11-09].

Nové kompetence směřují výhradně proti nejzávažnějším útokům v podstatě vojenského charakteru, které mají původ v zahraničí. A to na ty, na které bude potřeba reagovat okamžitě."[460] Ve vztahu k zákonnému podkladu svěřených pravomocí se uvádí, že *„[n]ovela zákona o Vojenském zpravodajství dovršila svěření vládního úkolu podílet se na kybernetické obraně Vojenskému zpravodajství a ukotvila kybernetickou obranu v českém právním systému."*[461] Jestliže měla vláda svým rozhodnutím svěřit kybernetickou obranu Vojenskému zpravodajství již v roce 2015, pak přijetí příslušné zákonné úpravy teprve o 6 let později je podstatně opožděným „dovršením" svěření zmíněného vládního úkolu. Není zřejmé, jakým způsobem bylo v tomto mezidobí vyhověno podmínce vázanosti státní moci zákonem ve smyslu čl. 2 odst. 3 Ústavy ČR, podle něhož lze státní moc uplatňovat jen v případech, v mezích a způsoby, které stanoví zákon.

Vojenské zpravodajství je ozbrojenou zpravodajskou službou ČR, jejíž činnost, postavení a působnost upravuje kromě ZVZ i zákon č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů (dále jen „zákon o zpravodajských službách"). K plnění svých úkolů využívá zpravodajské prostředky, jimiž jsou zpravodajská technika, krycí doklady, krycí prostředky a sledování osob a věcí.[462] Ve vztahu ke kyberprostoru nabývá zvláštního významu zejména zpravodajská technika, tj. při konkrétní činnosti využívané technické prostředky a zařízení, zejména elektronické, fototechnické, chemické, fyzikálně-chemické, radiotechnické, optické, mechanické anebo jejich soubory, používané utajovaným způsobem, pokud je jimi zasahováno do základních práv a svobod.[463] Její použití je možné pouze po předchozím písemném povolení předsedy senátu Vrchního soudu v Praze, s respektem k principu subsidiarity i proporcionality.[464] Použití zpravodajské techniky může Vojenské zpravodajství zabezpečit i pro potřeby jiných oprávněných orgánů, jako je Bezpečnostní informační služba či Policie ČR.

Činnost, kterou se Vojenské zpravodajství přímo podílí na zajišťování obrany ČR v kyberprostoru, stanoví § 16a ZVZ. Jde o detekci a vyhodnocování kybernetických útoků a hrozeb i jejich odvracení. Vojenské zpravodajství se přitom zaměřuje jen na kybernetické útoky a hrozby, které mají původ v zahraničí a směřují proti důležitým zájmům státu, jejichž zajišťování je

---

[460] VZ. *Novela zákona o vojenském zpravodajství* [online]. Dostupné: https://www.vzcr.cz/novela-zakona-o-vojenskem-zpravodajstvi-151 [Cit. 2022-11-09].

[461] Tamtéž.

[462] § 7 a násl. ZVZ. Vojenské zpravodajství je dále podle §§ 6 a 16 ZVZ oprávněno při plnění svých úkolů využívat i dobrovolné spolupráce osob.

[463] § 8 odst. 1 ZVZ.

[464] Tedy za předpokladu, že by odhalování nebo dokumentování činností, pro něž má být použita, bylo jiným způsobem neúčinné nebo podstatně ztížené anebo v daném případě nemožné. Použití nesmí rovněž zasahovat do práv a svobod nad nezbytně nutnou míru. Srov. § 9 ZVZ.

předmětem obrany ČR podle zákona o zajišťování obrany ČR.[465] Zmíněné kybernetické útoky a hrozby Vojenské zpravodajství vyhledává na základě ukazatelů, které si vyhodnotí jako skutečnosti ohrožující důležité zájmy státu v kybernetickém prostoru na základě dat a informací z vlastní zpravodajské činnosti i od ostatních zpravodajských služeb, NÚKIB a dalších orgánů.

K detekci stanovených útoků a hrozeb může Vojenské zpravodajství využít svých vlastních nástrojů umístěných na určených bodech veřejných komunikačních sítí, pokud to vyžaduje důležitý zájem obrany státu. Přednostně má však využívat spolupráce s provozovateli veřejných sítí a služeb.[466] Ti mají na základě dohody uzavřené s Vojenským zpravodajstvím vyhledávat na základě poskytnutých informací kybernetické útoky či hrozby.

ZVZ tedy stanoví podmínky pro uzavření subordinační veřejnoprávní smlouvy ve smyslu správního řádu. Dohoda o spolupráci s provozovatelem veřejných sítí a služeb musí být písemná, objem předávaných metadat nesmí překročit zákonem stanovený rozsah, a musí obsahovat technické a organizační podmínky nezbytné pro realizaci detekce, způsob předávání metadat o zachyceném útoku nebo hrozbě a způsob určení výše efektivně vynaložených nákladů.[467] Bližší podmínky pro sjednání veřejnoprávní smlouvy - dohody o spolupráci, však ZVZ neuvádí. Lze předpokládat, že konkrétní podoba dohod bude odvislá od typu vyhledávaných informací VZ. Kontrolou uzavíraných dohod o spolupráci by se jistě měl zabývat inspektor pro kybernetickou obranu, což je nová funkce vytvořená shora citovanou novelou ZVZ.[468] Inspektor pro kybernetickou obranu, ač je formálně součástí Vojenského zpravodajství, je podřízen přímo ministrovi obrany. Ve své kontrolní činnosti by tak měl být do značné míry nezávislý. V jaké míře tomu bude, ukáže čas.

V případě nebezpečí z prodlení si může Vojenské zpravodajství vyžádat informace i bez předem uzavřené písemné dohody s provozovateli veřejných sítí a služeb, to však pouze pomocí ukazatelů v rozsahu bezpečnostních opatření, které tento provozovatel již sám prováděl.[469]

---

[465] Podle § 2 odst. 1 zákona o zajišťování obrany ČR je obrana státu souhrnem opatření k zajištění svrchovanosti, územní celistvosti, principů demokracie a právního státu, ochrany života obyvatel a jejich majetku před vnějším napadením, a zahrnuje výstavbu účinného systému obrany státu, přípravu a použití odpovídajících sil a prostředků a účast v kolektivním obranném systému.

[466] Tedy s právnickou nebo podnikající fyzickou osobou zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací. Srov. § 16b odst. 2 ZVZ.

[467] § 16b ZVZ.

[468] Prvním inspektorem pro kybernetickou obranu byl jmenován dne 6. 4. 2022 Jan Vacek. SEDLÁK, Jan. *Vláda jmenovala inspektora kybernetické obrany, bude hlídat Vojenské zpravodajství* [online]. Lupa.cz, 7. 4. 2022. Dostupné: https://www.lupa.cz/aktuality/vlada-jmenovala-inspektora-kyberneticke-obrany-bude-hlidat-vojenske-zpravodajstvi/ [Cit. 2022-11-09].

[469] § 16c ZVZ.

Umístit vlastní nástroj detekce smí Vojenské zpravodajství teprve na základě rozhodnutí Ministerstva obrany ve zvláštním řízení, které bude vydáno poté, kdy Vojenské zpravodajství navrhne ministerstvu opatření k zajištění detekce, vyhodnocení a reakce na kybernetické útoky a hrozby.[470] Podkladem uvedeného správního rozhodnutí budou dokumenty předložené Vojenským zpravodajstvím - vedle zmíněných nutných opatření k zajištění jeho činnosti i posouzení bezpečnostních rizik spojených s připojením nástroje detekce. Ministerstvo obrany před vydáním rozhodnutí posoudí, zda umístění detekce kybernetického útoku či hrozby vyžaduje důležitý zájem obrany státu a zda je v souladu se zákonem stanovenými principy subsidiarity - tedy zda nelze dosáhnout cíle již na základě dohody o spolupráci s provozovateli veřejné sítě či služby. Rovněž by mělo posoudit naplnění principu proporcionality. Rozsah zaznamenávaných metadat nesmí vést k detekci nad zákonem stanovený rámec vymezený v § 16d odst. 2 ZVZ, a způsob provádění detekce musí zachovávat důvěrnost komunikace i integritu a dostupnost veřejných komunikačních sítí a služeb elektronických komunikací.

V případě kladného zhodnocení Ministerstvo obrany uloží svým rozhodnutím právnické nebo podnikající fyzické osobě zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinnost zřídit a zabezpečit rozhraní pro připojení nástrojů detekce v určeném bodě veřejné komunikační sítě a povinnost strpět jejich umístění a provozování. Detekce však smí být provozována pouze po dobu stanovenou v tomto rozhodnutí. Tato doba nesmí překročit 12 měsíců (na návrh Vojenského zpravodajství ji lze prodloužit nejdéle o 6 měsíců). Rozklad proti rozhodnutí ministerstva nemá odkladný účinek. Využití detekce pro odposlech a záznam telekomunikačního provozu nebo k aktivnímu zásahu zákon Vojenskému zpravodajství výslovně zakazuje.[471]

ZVZ dovoluje Vojenskému zpravodajství reagovat na zjištěnou kybernetickou hrozbu nebo útok dvojím způsobem. Buď předáním zjištěných informací státním orgánům příslušným k provedení konkrétního opatření k odvrácení takové hrozby, anebo v případě nebezpečí z prodlení vlastním aktivním zásahem.

Aktivní zásah Vojenského zpravodajství k odvrácení kybernetického útoku či hrozby musí splnit zákonem kumulativně stanovené podmínky: ve značném rozsahu musí být ohroženy důležité zájmy státu, kybernetický útok nebo hrozba musí trvat či bezprostředně hrozit, nelze je odvrátit v součinnosti s ozbrojenými silami ČR, a aktivní zásah je jediným možným účinným způsobem jejich

---

[470] Srov. § 16e odst. 3 ZVZ.

[471] § 16d odst. 3 ZVZ.

odvrácení.[472] Svými podmínkami tak aktivní zásah v kybernetickém prostoru připomíná meze nutné obrany stanovené trestním zákoníkem. Odvrácení nebezpečí musí splňovat podmínku subsidiarity, avšak nikoli proporcionality, když musí být dostatečně účinné a jevit se jako jediné možné účinné opatření k odvrácení útoku či hrozby.

Před provedením aktivního zásahu je Vojenské zpravodajství povinno vyžádat si souhlas ministra obrany; neobdrží-li jej, zásah neprovede. Ministra obrany rovněž informuje o provedení aktivního zásahu bezodkladně po jeho provedení a o zahájení aktivního zásahu bezodkladně informuje vládu, NÚKIB a ostatní zpravodajské služby.[473] Okolnosti, důvody a průběh každého provedeného aktivního zásahu Vojenským zpravodajstvím musejí být dokumentovány.[474] Aktivní zásah je tedy koncipován jako krajní řešení a okolnosti, které k němu vedly, musí být zpětně přezkoumatelné.

2.1.4.3. Kontrola výkonu činnosti Vojenského zpravodajství v oblasti kybernetické obrany státu

Vojenské zpravodajství jako ozbrojená zpravodajská služba ČR a součást moci výkonné podléhá kontrole vlády, která je vrcholným orgánem výkonné moci. Určitou kontrolu vykonává i prezident republiky, který je ve smyslu čl. 63 písm. c) Ústavy ČR vrchním velitelem ozbrojených sil. Vláda i prezident republiky ukládají zpravodajským službám úkoly v mezích jejich působnosti, přičemž prezident republiky tak činí s vědomím vlády.[475] Proto i ZVZ ukládá Vojenskému zpravodajství povinnost předkládat prezidentu republiky a vládě prostřednictvím ministra obrany jednou ročně podrobnou zprávu o činnostech a opatřeních na zajišťování obrany státu v kybernetickém prostoru. Ministra obrany má Vojenské zpravodajství písemně informovat o plnění stanovených úkolů pololetně.[476]

Dozor nad mocí vládní i výkonnou je oprávněn provádět i Parlament ČR, jehož kontrolní funkce byly po roce 1989 postupně opět rozšiřovány.[477] Obecný způsob provádění parlamentní kontroly je upraven v jednacím řádu Poslanecké sněmovny, který umožňuje Poslanecké sněmovně

---

[472] § 16g odst. 1 ZVZ.

[473] § 16g odst. 2 až 4 ZVZ.

[474] § 16h odst. 2 ZVZ.

[475] § 8 odst. 4 zákona o zpravodajských službách.

[476] § 16i ZVZ.

[477] HENDRYCH, Dušan a kol. Op. cit., str. 501.

zřídit pro vyšetření věci veřejného zájmu vyšetřovací komisi.[478] Zvláštní zákony pak upravují specifické případy parlamentní kontroly. Poslanecká sněmovna tak vykonává kontrolu činnosti zpravodajských služeb zejména prostřednictvím svých k tomuto účelu zřízených zvláštních kontrolních orgánů.[479] Činnost Vojenského zpravodajství, kterou se podílí na zajišťování obrany státu v kybernetickém prostoru, podléhá právě této kontrole.

Kontrolu zpravodajských služeb v oboru jejich působnosti na území ČR, včetně kontroly dodržování základních práv a svobod, vykonává i Orgán nezávislé kontroly zpravodajských služeb České republiky (dále jen „Orgán nezávislé kontroly"),[480] a to na základě podnětu některého ze zvláštních kontrolních orgánů. Orgán nezávislé kontroly se skládá z pěti členů, kteří jsou na návrh vlády voleni Poslaneckou sněmovnou na dobu pěti let a splňují zákonem stanovené podmínky pro výkon této veřejné funkce.[481] Kontrola je zákonem koncipována jako nezávislá na zájmech politických stran a politických hnutí, a také jako nestranná. Orgán nezávislé kontroly je při výkonu své kontrolní činnosti oprávněn požadovat od zpravodajské služby všechny potřebné související informace o její činnosti, ledaže by tím mohlo dojít k ohrožení účelu probíhající akce či bezpečnosti osob. Nemá však pravomoc přijmout opatření k odstranění zjištěných pochybení. Zjištění o nezákonné činnosti nebo protiprávním zásahu do základních práv a svobod může jen uveřejnit a navrhnout řediteli zpravodajské služby, předsedovi vlády nebo příslušnému členu vlády, aby přijali opatření nezbytná k odstranění zjištěných nedostatků. Každé podezření ze spáchání trestného činu příslušníkem zpravodajské služby, které Orgán nezávislé kontroly zjistí při prováděné kontrole, je rovněž povinen oznámit nejvyššímu státnímu zástupci.[482]

Činnost zpravodajských služeb je oblastí, v níž mohou být vysoce ohroženy základní lidská práva a svobody. Zákon o zpravodajských službách i ZVZ proto výslovně upravují jejich zvláštní parlamentní kontrolu. Neponechává se tak pouze na rozhodnutí Poslanecké sněmovny, zda zřídí ve smyslu § 48 Jednacího řádu PS vyšetřovací komisi, uzná-li za vhodné vyšetřit konkrétní činnost Vojenského zpravodajství na poli kybernetické obrany. Místo toho má fungovat permanentní kontrolní orgán Poslanecké sněmovny kontrolující zpravodajské služby, včetně činnosti Vojenského zpravodajství zajišťujícího obranu státu v kybernetickém prostoru. Soulad opatření zajišťujících

---

[478] Zákon č. 90/1995 Sb., o jednacím řádu Poslanecké sněmovny, ve znění pozdějších předpisů (dále jen „Jednací řád PS").

[479] § 12 odst. 1 a 2 zákona o zpravodajských službách.

[480] § 12 odst. 1 zákona o zpravodajských službách.

[481] Kromě bezpečnostní prověrky pro stupeň utajení Přísně tajné jde o minimální věk 40 let, české občanství a podmínky vylučující střet zájmů. Podrobněji § 12e zákona o zpravodajských službách.

[482] Srov. § 12g zákona o zpravodajských službách.

kybernetickou obranu státu se zákonem, zejména dodržování principu proporcionality a zachování důvěrnosti elektronických komunikací a služeb ve vztahu k občanům, lze jistě vždy hodnotit jako věc veřejného zájmu. Protože kontrolní orgán slouží k naplnění kontrolní funkce Poslanecké sněmovny, nikoli k prošetření individuálních stížností jednotlivců, nelze jej považovat za orgán nezávislé právní kontroly.[483] V případě nezákonného zásahu do veřejného subjektivního práva by se však jednotlivec mohl domáhat právní ochrany u nezávislého soudu. V úvahu by přicházela žaloba na ochranu před nezákonným zásahem správního orgánu ve smyslu § 82 a násl. s. ř. s.

Dalším možným nástrojem parlamentní kontroly je také právo každého poslance v souladu s čl. 53 Ústavy ČR interpelovat ministra obrany jako člena vlády ohledně přijatých opatření na zajištění kybernetické obrany státu. Kontrolním nástrojem poslanců je též využití citačního práva: usnese-li se na tom Poslanecká sněmovna, musí se ministr obrany na základě čl. 38 odst. 2 Ústavy ČR dostavit osobně na její schůzi a zodpovědět příslušné otázky stran kybernetické obrany; v případě obdobného požadavku výboru, komise či vyšetřovací komise Poslanecké sněmovny se může nechat zastoupit i jiným členem vlády nebo svým náměstkem, není-li výslovně jeho účast vyžadována.

Novela ZVZ upravila dále i nový institut inspektora kybernetické obrany. Na rozdíl od Orgánu nezávislé kontroly a kontrolních orgánů Poslanecké sněmovny podléhá exekutivě. Inspektor kybernetické obrany je jmenován a odvoláván vládou na návrh ministra obrany. Je buď vojákem z povolání či zaměstnancem zařazeným ve Vojenském zpravodajství, podřízen je však přímo ministrovi obrany. Zákon tedy počítá s podřízením inspektora kybernetické obrany členu vlády. Je proto otázkou, do jaké míry bude výkon kontroly v jeho podání fakticky nezávislý na politických podmínkách, byť tuto nezávislost přímo stanoví ZVZ.[484] Orgán nezávislé kontroly, který je administrativně navázán na Parlament ČR,[485] tedy na moc zákonodárnou, se proto jeví jako vhodnější podoba kontrolního mechanismu ve vztahu k výkonu pravomocí Vojenského zpravodajství, které je podřízeno moci výkonné. Lze tedy předpokládat, že zásadní úlohou inspektora kybernetické obrany bude spíše komunikace s osobami zajišťujícími veřejnou komunikační síť nebo poskytujícími veřejně dostupnou službu elektronických komunikací v případě jejich stížností či obav z ohrožení práv ze strany Vojenského zpravodajství.[486]

---

[483] HENDRYCH, Dušan a kol. Op. cit., str. 504.

[484] Srov. § 16k odst. 5 ZVZ.

[485] Srov. § 12e odst. 1 či § 12i zákona o zpravodajských službách.

[486] Srov. § 16l odst. 2 ZVZ.

2.2. Pojmové znaky bezpečnosti informací a dat

Informace, data a informační systémy chráníme především před neoprávněným přístupem k nim a před prováděním jejich změn během zpracování, přenosu nebo zálohování informací. Zásadní je též zabránit, aby došlo k odepření služeb oprávněným uživatelům. Z hlediska bezpečnosti informací a dat je proto klíčové zajistit jejich důvěrnost, integritu a dostupnost. Takto je bezpečnost informací uchopena nejen v zákoně o kybernetické bezpečnosti,[487] ale i v Úmluvě o počítačové kriminalitě, která ukládá smluvním stranám povinnost stíhat trestné činy proti důvěrnosti, integritě a použitelnosti (v anglickém originálním znění *availability*, tedy dostupnosti) počítačových dat a systémů.[488] Různé státy přistupují k zabezpečení počítačových dat a informačních systémů rozdílně, proto stál za přijetím Úmluvy o počítačové kriminalitě požadavek reagovat na takřka neomezené přeshraniční proudění počítačových dat alespoň sjednocením skutkových podstat trestných činů, spolu s usnadněním jejich vyšetřování.[489] Nižší míra bezpečnosti informací může vést ke ztrátě či změně dat, ke zneužití osobních údajů, ke vzniku majetkové i nemajetkové újmy i k ohrožení státních zájmů; v neposlední řadě ovlivňuje též postoj obyvatel státu k veřejné moci. Lze totiž oprávněně očekávat, že práva a svobody občanů stát zabezpečí i ve virtuální sféře.

Definice kybernetické bezpečnosti založená na důvěrnosti (*confidentiality*), integritě či celistvosti (*integrity*) a dostupnosti (*availability*) dat patří mezi ty klíčové a v praxi obvykle užívané.[490] Kolouch, Bašta a kol. vztahují uvedenou triádu „CIA"[491] i na data a počítačové systémy jako další prvky kybernetické bezpečnosti.[492] Proti tomuto přístupu nelze ničeho namítat. Pojem bezpečnost informací ovšem zdůrazňuje skutečnost, že data chráníme předně pro jejich informační potenciál.[493]

---

[487] Podle § 2 písm. c) ZKB se bezpečností informací rozumí zajištění důvěrnosti, integrity a dostupnosti informací a dat.

[488] Srov. Část 1, oddíl 1 Úmluvy o počítačové kriminalitě.

[489] ČR ratifikovala Úmluvu o počítačové kriminalitě 22. 8. 2013, v platnost vstoupila 1. 12. 2013. Jde o první mezinárodní smlouvu řešící trestné činy spáchané v internetovém prostředí a je otevřena k ratifikaci i nečlenským státům Rady Evropy.

[490] ENISA. Op. cit., str. 13. Překlad autorka.

[491] Jde o zkratku podle počátečních písmen anglických termínů.

[492] KOLOUCH, Jan, BAŠTA, Pavel a kol. Op. cit., str. 45 - 48.

[493] O rozdílech mezi daty a informacemi a o jednotlivých pojmech bylo pojednáno shora v podkapitole 1.1.2. Základní pojmy - počítač, data, informace, kyberprostor, Internet.

2.2.1. Důvěrnost informací a dat

Právní systémy různých států se obvykle snaží zajistit ochranu informací a informačních systémů před neoprávněným přístupem k nim, ať již z důvodu respektování soukromí a rodinného života, ochrany osobních údajů, obchodního tajemství, či jiných oprávněných zájmů. Zajištění důvěrnosti informací a dat je i prevencí neoprávněných změn v datech. Důvěrnost a integrita (celistvost) informací a dat jsou úzce spjaty.

Důvěrností informací a dat lze rozumět skutečnost, že k nim získají přístup jen osoby (systémy, subjekty) k tomu oprávněné. Rovněž to znamená, že nikdo nepovolaný nemůže zachytit tok dat, tj. „odposlechnout" komunikaci mezi počítačovými systémy a narušit tím důvěrný přenos informací. Narušením důvěrnosti informací je především neoprávněný přístup k počítačovému systému nebo jeho části. Zpravidla bývá považován za trestný, *„pokud je spáchán porušením bezpečnostních opatření, s úmyslem získat počítačová data nebo s jiným nečestným úmyslem, nebo ve vztahu k počítačovému systému, který je spojen s jiným počítačovým systémem."*[494]

Kromě narušení důvěrnosti představuje neoprávněný přístup k informacím též hrozbu pro integritu a dostupnost informací a dat, neboť může ztížit využití počítačových systémů a sítí jejich oprávněnými uživateli, vést ke změnám či ztrátě dat a k vysokým nákladům vynaloženým na jejich znovuzískání. Nezákonný přístup k informacím a datům může být i prostředkem ke spáchání závažnější trestné činnosti, kterou je padělání, podvod, vydírání apod. Přístup může být získán k hardware a fyzickým komponentům počítače, k uloženým datům, k adresářům či k metadatům, přičemž nezáleží, zda je přístupu docíleno skrze veřejnou či soukromou komunikační síť. Neoprávněnost přístupu spočívá v absenci souhlasu vlastníka či jiné osoby oprávněné udělit souhlas s přístupem do systému či jeho části, např. za účelem provedení zkoušky jeho zabezpečení. O neoprávněný přístup se však nebude jednat v případě počítačového systému volně přístupného veřejnosti (*open access by the public*) - takový přístup bude vždy po právu. Mezi další případy přístupu v souladu s právem může patřit výkon státní moci v souladu se zákonem za účelem ochrany veřejného pořádku, bezpečnosti státu či postihu trestné činnosti.[495]

Narušením důvěrnosti informací a dat je i nezákonný odposlech. Úmluva o počítačové kriminalitě ukládá stíhat jako trestný *„úmyslný, neoprávněný, technickými prostředky provedený odposlech neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci,*

---

[494] Srov. čl. 2 Úmluvy o počítačové kriminalitě. ČR učinila v souladu s čl. 2 a čl. 40 Úmluvy o počítačové kriminalitě výhradu, dle níž nastane trestní odpovědnost za činy popsané v čl. 2 Úmluvy při narušení bezpečnostních opatření s cílem získat neoprávněný přístup k celému počítačovému systému nebo jeho části.

[495] RADA EVROPY. *Explanatory Report - ETS 185 - Cybercrime (Convention)* [online], body 38 a 44 - 47. Dostupné: https://rm.coe.int/16800cce5b [Cit. 2022-11-09].

včetně elektromagnetického vyzařování z počítačového systému přenášejícího taková počítačová data."[496] Jedná se o stejné porušení práva na soukromí jako v případě klasického odposlechu telefonního hovoru či porušení listovního tajemství. Způsob přenosu elektronických dat není rozhodující. Z hlediska trestnosti však Úmluva o počítačové kriminalitě cílí pouze na odposlechy provedené technickými prostředky, tj. s pomocí technických zařízení připevněných k přenosovým linkám či zařízením pro sběr a záznam bezdrátové komunikace, počítaje v to nejrůznější software. Ochrana je poskytována neveřejnému přenosu - je nerozhodné, jsou-li přenášené informace a data jinak veřejně dostupné.[497] Samotné „proudění" elektronických dat má zůstat nenarušeno, má-li být zajištěna jejich důvěrnost.

S pojmem důvěrnost informací a služeb, které *„zpracovává nebo poskytuje informační a komunikační systém"*, pracuje i vyhláška NÚKIB č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „vyhláška o kybernetické bezpečnosti"). Tyto informace a služby označuje jako aktiva. Povinným osobám ukládá přistupovat k aktivům s ohledem na jejich důležitost, jež má být stanovena pomocí hledisek důvěrnosti, integrity a dostupnosti. Obdobně dělí i kybernetické bezpečnostní incidenty podle skutečnosti, zda narušují důvěrnost, integritu nebo dostupnost informací a služeb, případně zda jde o kombinaci narušení uvedených oblastí.[498]

Jak nahlížet na důvěrnost informací a služeb uvádí Stupnice pro hodnocení důvěrnosti v tabulce Přílohy č. 1 vyhlášky o kybernetické bezpečnosti. Informace a služby rozděluje z hlediska hodnocení jejich důvěrnosti do čtyř úrovní: nízká, střední, vysoká a kritická. Požadavky na ochranu mají vzestupnou tendenci: zatímco u veřejně přístupných informací (nízká úroveň důvěrnosti) nejsou žádné, u informací, jež představují veřejně nepřístupné know-how (střední úroveň důvěrnosti), mají být využity prostředky pro řízení přístupu, přičemž požadavky jsou i u jejich likvidace. Pokud informace a služby nejsou veřejně přístupné a právní předpisy nebo jiné předpisy či smluvní ujednání vyžadují jejich ochranu (vysoká úroveň důvěrnosti), mají být pro ochranu důvěrnosti využívány již prostředky zajišťující řízení i zaznamenávání přístupu, a přenos informací má být chráněn pomocí kryptografie. U veřejně nepřístupných informací a služeb vyžadujících nadstandardní míru ochrany nad rámec vysoké úrovně důvěrnosti (kritická úroveň důvěrnosti) má

---

[496] Čl. 3 Úmluvy o počítačové kriminalitě.

[497] RADA EVROPY. Op. cit., body 51 - 54.

[498] Srov. 2 písm. g), § 4 písm. b), e), § 31 odst. 3 vyhlášky o kybernetické bezpečnosti a dále její přílohu č. 1.

být nad rámec předchozích opatření využita i ochrana před zneužitím informací a služeb ze strany administrátorů.

Důvěrnost informací lze hodnotit i na základě zákona o ochraně utajovaných informací. Utajovanou informací je informace, *„jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné, a která je uvedena v seznamu utajovaných informací",* přičemž podoba ani nosič informace nejsou rozhodující.[499] V souvislosti s povahou újmy zájmu ČR, která může být vyzrazením utajované informace neoprávněné osobě způsobena, je informace klasifikována jedním ze čtyř stupňů utajení: přísně tajné, tajné, důvěrné a vyhrazené.[500] Ústředním orgánem státní správy pro ochranu utajovaných skutečností se stal 1. 8. 1998 Národní bezpečnostní úřad, jenž se v souvislosti s přijetím zákona o ochraně utajovaných informací označuje od roku 2006 jako ústřední orgán státní správy ochrany utajovaných informací.[501]

Bezpečnost informačních a komunikačních systémů nakládajících s utajovanými informacemi upravuje Hlava VI. zákona o ochraně utajovaných informací. Nakládat s utajovanými informacemi lze pouze v informačních systémech, které byly certifikovány NÚKIB a písemně schváleny do provozu odpovědnou osobou nebo jí pověřenou osobou.[502] NÚKIB schvaluje i projekt bezpečnosti provozu komunikačního systému,[503] neboť do působnosti NÚKIB spadá i bezpečnost informačních a komunikačních systémů a kryptografická ochrana utajovaných informací. V jejím rámci NÚKIB vykonává nejen legislativní a metodickou činnost, ale i kontrolu, vede správní řízení a ukládá správní tresty za porušení povinností při ochraně utajovaných informací.[504] Posuzování bezpečnosti informačních systémů je složitá problematika vzhledem k různorodosti informačních systémů a rychlému rozvoji ICT.[505] Požadavky na informační i komunikační systémy nakládající s

---

[499] § 2 písm. a) zákona o ochraně utajovaných informací. Zájem ČR je koncipován v písm. b) téhož ustanovení široce jako zachování její ústavnosti, svrchovanosti a územní celistvosti, zajištění vnitřního pořádku a bezpečnosti, mezinárodních závazků a obrany, ochrana ekonomiky a ochrana života nebo zdraví fyzických osob.

[500] § 4 zákona o ochraně utajovaných informací. Pojem újmy zájmu ČR je rozveden v § 3 zákona o ochraně utajovaných informací.

[501] Před 1. 8. 1998, kdy vstoupil v účinnost zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, byl výkon státní správy v dané oblasti svěřen Komisi pro ochranu státního tajemství a Federálnímu ministerstvu vnitra, resp. od 1.1.1993 Ministerstvu vnitra ČR. Blíže k vývoji institucionální ochrany utajovaných informací v ČR viz PAVELKA, Ivan. Institucionální zajištění ochrany utajovaných informací v ČR. *Správní právo*, č. 3/2018.

[502] Srov. § 34 odst. 1 až 4 zákona o ochraně utajovaných informací.

[503] § 35 odst. 2 zákona o ochraně utajovaných informací.

[504] Tato působnost NÚKIB se však nevztahuje na činnost zpravodajských služeb ani Ministerstva vnitra, plní-li úkoly podle zákona o ochraně utajovaných informací. Podrobněji k úkolům a pravomoci NÚKIB i NBÚ v oblasti ochrany utajovaných informací PAVELKA, Ivan. Op. cit.

[505] Srov. Metodiku k certifikaci informačních systémů č. 1/2005/02/is Nbu ve znění účinném od 30. 4. 2005, bod 5.

utajovanými informacemi, provádění certifikace a schvalování projektů bezpečnosti jsou uvedeny ve vyhlášce Národního bezpečnostního úřadu č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor (dále jen „vyhláška o bezpečnosti ICT"). V ní najdeme i vysvětlení pojmu důvěrnost utajované informace: jde o *„vlastnost, která znemožňuje odhalení utajované informace neoprávněné osobě"*.[506] Na základě žádosti o certifikaci vypracuje NÚKIB seznam podkladů pro ověření způsobilosti informačního systému. Certifikaci informačního systému provede posouzením podkladů předložených žadatelem a provedením dodatečných testů za spoluúčasti žadatele, případně i dodavatele (pokud je informační systém budován jinou organizací).[507] Výsledkem posouzení je vydání certifikační zprávy, která případně obsahuje kromě podmínek provozu informačního systému a jeho popisu i identifikaci přijatelných rizik souvisejících s jeho provozem.[508] Certifikace se vydává na dobu určitou, a v případě žádosti o opakovanou certifikaci, neexistují-li nová rizika, NÚKIB vydává certifikát již na základě existující bezpečnostní dokumentace informačního systému a provedené kontroly bezpečnosti informačního systému.[509]

Na certifikaci informačního systému lze nahlížet jako na doklad ve smyslu § 151 správního řádu opravňující nakládat v informačním systému s utajovanými informacemi. Proces posuzování informačního systému je řízením o žádosti žadatele, a je-li žádosti vyhověno, přiznává certifikace právo nakládat v informačním systému s utajovanými informacemi. Pravomoc NÚKIB provádět ve smyslu § 137a písm. e) zákona o ochraně utajovaných informací certifikaci informačního systému či schvalovat projekt bezpečnosti komunikačního systému, je patrně svým charakterem správním řízením, v němž lze místo písemného vyhotovení rozhodnutí vydat doklad - certifikační zprávu, jež je ve své podstatě konstitutivním rozhodnutím. Pokud by nebylo žádosti o certifikaci vyhověno, postup podle § 151 správního řádu se neuplatní, ale musí být vydáno rozhodnutí podle § 67 a násl. správního řádu.[510]

---

[506] § 2 písm. i) vyhlášky o bezpečnosti ICT.

[507] § 24 odst. 6 vyhlášky o bezpečnosti ICT. Podrobněji srov. Metodiku k certifikaci informačních systémů č. 1/2005/02/ is Nbu ve znění účinném od 30. 4. 2005.

[508] § 25 vyhlášky o bezpečnosti ICT. Certifikační zpráva obsahuje podle písm. d) téhož ustanovení i typy změn informačního systému, které vyžadují provedení doplňujícího hodnocení informačního systému.

[509] § 26 odst. 2 vyhlášky o bezpečnosti ICT.

[510] JEMELKA, Luboš, PONDĚLÍČKOVÁ, Klára, BOHADLO, David. § 151 [Vydání dokladu]. In: JEMELKA, Luboš, PONDĚLÍČKOVÁ, Klára, BOHADLO, David. *Správní řád*. 6. vydání. Praha: C. H. Beck, 2019, str. 805.

V oblasti ochrany utajovaných informací se projevuje spolupráce příslušných správních orgánů. Národní bezpečnostní úřad jako ústřední správní úřad primárně kontroluje, zda v oblasti ochrany utajovaných informací a bezpečnostní způsobilosti dodržují orgány státu, právnické osoby, podnikající fyzické osoby a fyzické osoby právní předpisy. Jelikož je však NÚKIB příslušným orgánem státní správy pro oblast ochrany utajovaných informací v informačních a komunikačních systémech, bude k výkonu kontroly přizván též zástupce NÚKIB.[511]

2.2.2. Integrita (celistvost) informací a dat

Integrita zaručuje autenticitu dat, tj. skutečnost, že nedošlo k neoprávněným změnám dat a tím pádem ani z nich vyplývajících informací.[512] Podstatou integrity je, že do daných dat (i počítačového systému) nemohl zasáhnout nikdo neoprávněný; integrita jako vlastnost dat tudíž zaručuje jejich neporušenost.[513] Integrita dat rovněž označuje jejich platnost, konzistenci a přesnost, integrita systému vylučuje manipulace a nezamýšlené změny, ať již ze strany autorizovaných či neautorizovaných uživatelů.[514] Na integritu můžeme nahlížet i jako na celistvost dat. Zjednodušeně lze říci, že jsou-li data celistvá (tj. je zachována jejich integrita), jsou tím, čím se zdají být - ať již z hlediska svého původu či obsahu. Kdo se seznámí s daty, jejichž integrita je zaručena, získá i požadované informace; pokud nikoli, není chyba zpravidla na straně dat, nýbrž u recipienta informací.

---

[511] Srov. § 33a, § 136 odst. 1, § 137 písm. b), § 137a písm. e), § 143 odst. 6 zákona o ochraně utajovaných informací. V praxi též mohou vyvstat problémy při přezkumu správního rozhodnutí, které je založeno na důkazech tvořených utajovanými informacemi. Podle § 17 odst. 3 správního řádu jsou uchovávány odděleně mimo spis záznamy obsahující utajované informace, tudíž není možné, aby se adresát rozhodnutí s těmito podklady seznámil, neboť by tím došlo ke zmaření účelu jejich utajení. Jde o konflikt mezi procesními právy účastníka správního řízení a právem na spravedlivý proces, jehož součástí je i právo seznámit se s důvody rozhodnutí, vyjádřit se k provedeným důkazům a právo na účinný prostředek nápravy. Podrobněji SLÁDEKOVÁ, Stanislava. Když je v sázce národní bezpečnost. Ohrožení bezpečnosti státu jako důvod pro neudělení pobytového oprávnění cizinci, se zaměřením na krátkodobá víza. In: POŘÍZEK, Pavel, JÍLEK, Dalibor. *Ročenka uprchlického a cizineckého práva 2018: ročenku tvoří příspěvky, které zazněly na vědeckém semináři konaném ve dnech 20. a 21. září 2018 v Kanceláři veřejného ochránce práv - Současné otázky a odpovědi uprchlického a cizineckého práva, a další odborné příspěvky, které souvisí s tématem uprchlického a cizineckého práva* [online]. Brno: Kancelář veřejného ochránce práv ve spolupráci s Wolters Kluwer ČR, 2019, str. 19-43. Soud je v těchto případech garantem práva na spravedlivý proces výrazněji než v jiných (sporných) řízeních a postup veřejné správy aktivně přezkoumává s ohledem na relevanci utajovaných informací ze všech možných hledisek. O povaze utajovaných informací jako důkazního prostředku ve správním řízení pojednávají např. rozsudky Nejvyššího správního soudu ze dne 25. 11. 2011, č. j. 7 As 31/2011-101, ze dne 21. 12. 2012, č. j. 7 As 117/2012-28, nebo rozsudek Krajského soudu v Hradci Králové, pobočka v Pardubicích ze dne 22. 2. 2021, č. j. 52 A 86/2020-69.

[512] Lze se setkat i s názorem, který považuje autenticitu za další vlastnost vedle integrity počítačových dat či informačního systému. Ve snaze pokrýt zcela informační bezpečnost rozšiřuje triádu CIA o autenticitu, držbu či kontrolu dat a jejich využitelnost. Blíže PENDER-BEY, Georgie. *The Parkerian Hexad: The CIA Triad Model Expanded* [online]. Dostupné: http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf [Cit. 2022-11-10].

[513] KOLOUCH, Jan, BAŠTA, Pavel a kol. Op. cit., str. 53.

[514] JIRÁSEK, Petr, NOVÁK, Luděk, POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti* [online]. 3. aktualizované vydání. Praha: AFCEA, 2015, str. 59. Dostupné: https://afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf [Cit. 2022-11-10].

Úmluva o počítačové kriminalitě obsahuje skutkovou podstatu nazvanou „zasahování do dat" (*data interference*), jejíž podstatou je úmyslné neoprávněné poškození, vymazání, snížení kvality, pozměnění nebo potlačení počítačových dat.[515] Důvodová zpráva k Úmluvě o počítačové kriminalitě upozorňuje, že k pozměnění dat a narušení počítačového systému a programu dochází obvykle vlivem malware. Cílem citované skutkové podstaty je zajistit počítačovým datům obdobnou ochranu jako v případě ochrany fyzických objektů před úmyslným poškozením nebo zničením tak, aby byla zaručena funkčnost a použitelnost počítačových dat a software. Jsou-li data potlačena, nebudou dostupná oprávněným uživatelům, případně nebudou využitelná.[516]

Integrita dat úzce souvisí se zajištěním jejich dostupnosti. Úmluva o počítačové kriminalitě tudíž v další skutkové podstatě nazvané jako „zasahování do systému" (*system interference*) chrání nejen integritu, ale i dostupnost informací a dat požadavkem kriminalizovat úmyslné *„neoprávněné závažné omezení funkčnosti počítačového systému vkládáním, přenášením, poškozením, vymazáním, snížením kvality, pozměněním nebo potlačením počítačových dat."*[517]

Vyhláška o kybernetické bezpečnosti nabízí v Příloze č. 1 v Tabulce 2 Stupnici pro hodnocení integrity. Neohrozí-li narušení integrity informací a služeb oprávněné zájmy povinné osoby, nevyžaduje se ani žádná ochrana. V případě vyšších úrovní důležitosti informací a služeb (střední, vysoká a kritická) se postupně vyžadují ochranné prvky - od standardních nástrojů jako je omezení přístupových práv pro zápis, přes speciální nástroje jako je sledování historie provedených změn a záznamů identity osob provádějících změnu, až ke kryptografickým prostředkům chránícím přenos a aplikaci jednoznačné identifikace osob provádějících změny, např. skrze digitální podpis.

2.2.3. Dostupnost informací a dat

Dostupnost informací a dat značí spolehlivou možnost jejich využití v případě potřeby. Skutečnost, že data jsou dostupná, především znamená, že jsou použitelná, jak naznačuje i Úmluva o počítačové kriminalitě.[518] Výkladový slovník kybernetické bezpečnosti definuje dostupnost jako

[515] Čl. 4 odst. 1 Úmluvy o počítačové kriminalitě.

[516] RADA EVROPY. Op. cit., body 60 - 61.

[517] Čl. 5 Úmluvy o počítačové kriminalitě.

[518] Viz Oddíl 1 Úmluvy o počítačové kriminalitě - Trestné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů.

vlastnost přístupnosti a použitelnosti na žádost oprávněné osoby.[519] Běžným nástrojem zabezpečení dostupnosti může být např. firewall, který zabezpečuje síťový provoz.[520]

Dostupnost dat nelze směšovat s jejich vlastnictvím, držbou či kontrolou. Není-li možné přečíst data uložená na pevném nosiči, protože nosič byl zničen a je nefunkční, případně nejsou-li známé přístupové údaje k datům uloženým v cloudovém úložišti, jsou taková data uživateli k ničemu, byť je stále jejich vlastníkem.

Smyslem dostupnosti informací a dat je zaručení funkčnosti počítačového systému (je-li něco dostupné a použitelné, bude to plnit svoji funkci). Jak bylo shora naznačeno, dostupnost úzce souvisí se zajištěním integrity dat a informací. Například Úmluva o počítačové kriminalitě vychází z premisy, podle níž nebude-li do dat a počítačového systému zasahováno, tj. bude-li zachována jejich integrita, zůstanou tato data a systémy oprávněnému uživateli také dostupné a použitelné.

Vyhláška o kybernetické bezpečnosti člení v Příloze č. 1 v Tabulce 3 důležitost informací a služeb podle následků narušení jejich dostupnosti opět do čtyř úrovní, jako tomu je u hodnocení důvěrnosti a integrity. Pokud lze běžně tolerovat i delší časové období (cca do týdne), během něhož nejsou informace či služby dostupné, jde o úroveň nízkou - dostupnost v ní může být zabezpečena jen pomocí běžného zálohování dat. Pokud by narušení dostupnosti nemělo přesáhnout pracovní den (střední úroveň), měla by být zajištěna i obnova dat. O vysokou úroveň důležitosti půjde tehdy, pokud by i několikahodinové narušení dostupnosti informací a služeb znamenalo přímé ohrožení oprávněných zájmů osob. Dostupnost na vysoké úrovni proto má být chráněna pomocí záložních systémů a může být podmíněna i zásahy obsluhy či výměnou technických aktiv. Nelze-li vůbec připustit narušení dostupnosti informace či služeb, půjde o kritickou úroveň důležitosti, která vyžaduje automatizovanou ochranu pomocí záložních systémů a obnovy poskytování služeb. Příkladem kriticky důležitých informací a služeb by mohl být zdravotní sektor, v jehož rámci nelze s ohledem na ochranu života a zdraví osob připustit žádné narušení dostupnosti informací a služeb.[521]

---

[519] JIRÁSEK, Petr, NOVÁK, Luděk, POŽÁR, Josef. Op. cit., str. 43.

[520] K možnosti zabezpečení srov. např. PENDER-BEY, Georgie. Op. cit., str. 16.

[521] Lze si představit probíhající operaci prováděnou pomocí speciálních počítačových zobrazovacích metod (např. laparoskopicky) nebo po určitou dobu trvající napojení pacienta na mimotělní oběh zabezpečovaný přístroji, umožňující po určitou dobu zcela nahradit normální činnost jeho srdce a plic.

2.3. Narušení bezpečnosti informací, služeb a sítí

Smyslem informační bezpečnosti by mělo být především zajištění důvěrnosti, integrity (celistvosti) a dostupnosti informací.[522] Shodně definuje bezpečnost informací i zákon o kybernetické bezpečnosti.[523] Zajištěním informační bezpečnosti v kybernetickém prostředí dojde i k lepšímu zabezpečení informačních systémů a služeb, jakož i sítí elektronických komunikací.

V oblasti kybernetické bezpečnosti se běžně setkáme s řadou různých pojmů, které mají podobný význam, případně mají být vykládány dokonce i totožně. S ohledem na různé autory i překladatele z cizího jazyka však dochází k použití jiné terminologie. Objevují se termíny jako kybernetická hrozba, kybernetický incident, kybernetický útok, kybernetická událost, kybernetický konflikt, apod. Přehled a terminologii jednotlivých pojmů uvádí např. Kolouch, Bašta a kol. v monografii CyberSecurity.[524] Na tomto místě však postačí podat přehled základních zákonných definic a blíže se zabývat pouze kybernetickým útokem.

Dále se text věnuje příkladům narušení důvěrnosti, celistvosti a dostupnosti informací a dat, včetně stručného rozboru případu Stuxnet - kybernetického útoku na počítačové zařízení v íránské jaderné elektrárně. Závěrem je uveden přehled vybraných právních předpisů a norem dotýkajících se bezpečnosti informací v kyberprostoru.

2.3.1. Kybernetická bezpečnostní událost a incident

Česká právní úprava obsahuje zákonné definice kybernetické bezpečnostní události i incidentu. ZKB definuje kybernetickou bezpečnostní událost jako *„událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací."*[525] Synonymem této zákonné definice se proto může stát i pojem kybernetická hrozba. Tu ZKB přímo nedefinuje, byť na několika místech zmiňuje hrozbu v oblasti kybernetické bezpečnosti. Hrozba v oblasti kybernetické bezpečnosti je podle ZKB důvodem pro výkon správní pravomoci - konkrétního opatření k zabezpečení informačních systémů nebo služeb a sítí elektronických komunikací, tj. pro vydání varování, reaktivního opatření nebo ochranného opatření.[526] Konkrétní příklady kybernetických hrozeb

---

[522] Obdobně ŠULC, Vladimír. Op. cit., str. 6.

[523] Srov. § 2 písm. c) ZKB.

[524] KOLOUCH, Jan, BAŠTA, Pavel a kol. Op. cit., str. 73 a násl.

[525] § 7 odst. 2 ZKB.

[526] § 11 ZKB.

nalezneme ve vyhlášce o kybernetické bezpečnosti, která nabízí i stupnici pro hodnocení hrozeb.[527] Jde například o různé druhy škodlivého kódu (malware), o zneužití identity, zneužití oprávnění uživateli či administrátory, sabotáž atd.

Kybernetickým bezpečnostním incidentem je *„narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události."*[528] Narozdíl od kybernetické hrozby nebo kybernetické bezpečnostní události představuje kybernetický bezpečnostní incident již faktické narušení bezpečnosti informací, služeb nebo sítí. Jeho příčiny mohou být různé, patří mezi ně úmyslné i nedbalostní jednání člověka, přírodní jev, či pouhá náhoda. Tím se kybernetický bezpečnostní incident odlišuje od útoku, za nímž nakonec vždy stojí úmyslné jednání jedné nebo více osob.

NÚKIB ve své klasifikaci kybernetických incidentů, kterou zveřejňuje každý měsíc na webových stránkách, vychází z taxonomie ENISA. Kybernetické incidenty dělí podle způsobu spáchání nebo chráněného objektu do následujících kategorií: dostupnost, informační bezpečnost, podvod, škodlivý kód, průnik, pokus o průnik, sběr informací, urážlivý obsah a ostatní.[529] ENISA uvádí navíc dvě kategorie - zranitelnost (*vulnerable*) a testování (*test*).[530]

2.3.2. Kybernetický útok

Podobně jako není shody na všeobecně přijímané definici kyberprostoru,[531] těžko bychom nalezli jednotný pohled na to, co je přesně kybernetický útok. Různé komunity kladou důraz na odlišné aspekty: zatímco armáda se zdráhá označit kybernetický útok za použití síly, orgány činné v trestním řízení chápou útok především jako násilný trestný čin.[532] ZKB pojem kybernetického útoku nedefinuje. Termín se používá ve spojení s útoky vedenými na hodnoty ve virtuálním prostředí *„za účelem narušení, znepřístupnění zničení či ovládnutí počítačového prostředí či infrastruktury nebo*

---

[527] Srov. Přílohu č. 2 Tab. 1 a Přílohu č. 3 vyhlášky o kybernetické bezpečnosti.

[528] § 7 odst. 2 ZKB.

[529] Srov. např. NÚKIB. *Kybernetické incidenty pohledem NÚKIB: červen 2022* [online], str. 3. Dostupné: https://www.nukib.cz/download/publikace/vyzkum/NUKIB_incidenty-2022-06.pdf [Cit. 2022-11-10]. NÚKIB. *Kybernetické incidenty pohledem NÚKIB: říjen 2022* [online], str. 3. Dostupné: https://www.nukib.cz/download/publikace/vyzkum/2022-10.pdf [Cit. 2022-11-10].

[530] ENISA. *Reference Incident Classification Taxonomy: Task Force Status and Way Forward* [online]. January 2018, str. 9. Dostupné: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy [Cit. 2022-11-10]. Překlad autorka.

[531] ENISA. *Definition of Cybersecurity: Gaps and overlaps in standardisation* [online]. Op. cit., str. 25.

[532] KLIMBURG, Alexander (ed). *National Cyber Security Framework Manual, NATO CCD COE Publication* [online]. Tallinn 2012, str. 18. Dostupné: https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf [Cit. 2022-11-10].

zničení integrity dat či odcizení kontrolovaných informací"[533] i obecně ve spojení se všemi útoky, které nějakým způsobem využijí informační a komunikační technologie. NATO považuje kybernetické útoky za součást hybridní války a silnou a flexibilní kybernetickou obranu za jeden z klíčových úkolů při zajišťování kolektivní obrany.[534] Rozšíření působnosti na čtvrtou doménu - kyberprostor, odůvodňuje významem kybernetického prostředí v moderních bezpečnostních konfliktech.[535]

Zatímco Německo kybernetický útok považuje za útok vedený díky informačním technologiím v kyberprostoru proti jednomu či více počítačovým systémům, a to v úmyslu poškodit jejich důvěrnost, integritu či dostupnost,[536] americká Committee on National Security Systems označuje kybernetický útok jako jakékoli škodlivé jednání s cílem shromáždit, narušit, odmítnout, znehodnotit či zničit zdroje informačního systému nebo informace samotné.[537] Velká Británie klade důraz na čtyři různé způsoby kybernetického útoku: elektronický útok, sabotáž dodavatelského řetězce, manipulace s radiovým spektrem a narušení nechráněných elektronických zařízení skrze vysokovýkonnou radiovou frekvenci.[538]

Výkladový slovník kybernetické bezpečnosti chápe obecný útok jako *„pokus o zničení, vystavení hrozbě, změnu, vyřazení z činnosti, zcizení aktiva nebo získání neoprávněného přístupu k aktivu nebo uskutečnění neoprávněného použití aktiva",*[539] přičemž aktivum je ve slovníku vymezeno jako *„cokoliv, co má hodnotu pro jednotlivce, organizaci nebo veřejnou správu."*[540]

---

[533] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Managing Information Security Risk: Organization, Mission, and Information System View* [online]. March 2011, str. B-3. Dostupné: https://csrc.nist.gov/publications/detail/sp/800-39/final [Cit. 2022-11-10]. Překlad autorka.

[534] Podrobněji NATO. *Cyber defence* Op. cit.

[535] K tomuto kroku došlo po útocích na estonskou infrastrukturu roku 2007. Ačkoli členské státy Severoatlantické aliance zodpovídají za bezpečnost národních informačních a komunikačních sítí, musí zaručit jejich kompatibilitu navzájem mezi sebou, jakož i s infrastrukturou NATO. V rámci NATO je posílena výměna informací a vzájemná pomoc při prevenci, odražení i nápravě následků kybernetických útoků. Na žádost členského státu NATO posílí obranu kyberprostoru, což umožní koordinovanou obranu kyberprostoru a případnou odezvu na kybernetický útok. Mezi CERT pracovišti EU i NATO má probíhat oboustranná výměna informací a osvědčených postupů při řešení bezpečnostních incidentů. Objevují se však výtky, že jde o zbytečnou duplikaci obranných postupů v rámci EU a NATO. Srov. NATO. *NATO Summit Guide, Warsaw 8 - 9 2016.* Op. cit., str. 128. AWAN, Imran, BLAKEMORE, Brian (eds.). Op. cit., str. 166.

[536] KLIMBURG, Alexander (ed). Op. cit., str. 18.

[537] CNSS. *Committee on National Security Systems (CNSS) Glossary* [online]. April 6, 2015, str. 8. Dostupné: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf [Cit. 2022-11-10]. Překlad autorka. Kybernetickou bezpečnost pak chápe jako ochranu před zničením (a uvedení do původního stavu) počítačů, elektronických komunikačních systémů i služeb, drátové komunikace, elektronické komunikace, včetně informací zde obsažených, a zajišťující jejich dostupnost, integritu, autenticitu, důvěrnost a funkčnost. Tamtéž, str. 40. Překlad autorka.

[538] KLIMBURG, Alexander (ed). Op. cit., str. 18.

[539] JIRÁSEK, Petr, NOVÁK, Luděk, POŽÁR, Josef. Op. cit., str. 121.

[540] Tamtéž, str. 17.

Kladem této definice je její obecnost, neboť není navázána na kybernetické prostředí, anebo na využití informačních a výpočetních technologií. Zvláštní se naopak jeví vymezení útoku pouze jako pokusu, ledaže by autoři definice zamýšleli útok tím spíše vztáhnout i na dokonaný čin. Nedostatečné se rovněž může jevit i omezení chráněných hodnot pouze na ty s významem pro jednotlivce, organizaci a veřejnou správu. Kybernetický útok je ve Výkladovém slovníku kybernetické bezpečnosti označen následovně: „*Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.*"[541] Zde se jeví omezení pouze na IT infrastrukturu jako nedostatečné. K útoku např. může dojít i podvedením oprávněného uživatele, který následně sám provede škodlivou operaci (typicky při phishingu), přičemž takový útok nebude veden přímo na IT infrastrukturu. Definice se zdá nevyhovující i ve vztahu k omezení na citlivé či strategicky důležité informace, neboť útočník může cílit i na jiné informace či obecně data, případně nemusí chtít vůbec informace získat, ale jen způsobit škodu (např. zničit či znehodnotit funkční zařízení či program).

Aby byl incident považován za útok, musí být zpravidla veden úmyslně,[542] případně dokonce s určitým záměrem. Požadavek (škodlivého) úmyslu se zdá univerzálním v soukromé i veřejné sféře. Úmluva o počítačové kriminalitě udává požadavek úmyslného jednání ve vztahu ke všem skutkovým podstatám trestných činů, ať trestným činům proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů, trestných činů souvisejících s počítačem, trestných činů souvisejících s obsahem nebo trestných činů týkajících se porušení autorského práva a práv souvisejících s právem autorským.[543] Lze se setkat s pojetím kybernetického útoku jako jakéhokoli škodlivého úmyslného pokusu jednotlivce či organizace o narušení informačního systému, obvykle s cílem získat prospěch,[544] nebo jako jakéhokoli neoprávněného útočného jednání vůči počítačovému informačnímu systému, síti či infrastruktuře, nebo vůči osobním počítačovým zařízením, potenciálně se škodlivým úmyslem.[545] Útočník bývá popisován jako jednotlivec, organizace, skupina, společnost; útok může být přičitatelný též státu. Dokonce se můžeme setkat i s

---

[541] Tamtéž, str. 71.

[542] Srov. též KOLOUCH, Jan, BAŠTA, Pavel a kol. Op. cit., str. 82.

[543] Srov. Oddíly 1 až 4, Část 1 Úmluvy o počítačové kriminalitě. Ve vztahu k trestným činům týkajícím se porušení autorského práva a práv souvisejících s právem autorským, se hovoří o „záměru".

[544] CISCO. *What is a Cyberattack?* [online]. Dostupné: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html [Cit. 2022-11-10].

[545] WIKIPEDIA : The Free Encyclopedia. *Cyberattack* [online]. St. Petersburg (Florida) : Wikimedia Foundation, 2001-. Anglická verze. Dostupné: https://en.wikipedia.org/wiki/Cyberattack [Cit. 2022-11-10].

„neživým" útočníkem ve smyslu škodlivého procesu.[546] Takový přístup však nelze považovat za správný, jelikož i za škodlivým programem (procesem) je v případě útoku vždy lidský faktor v podobě konkrétního programátora, skupiny hackerů apod. Pokud by šlo o proces ve smyslu události, nejednalo by se o útok.

Zatímco vymezení kybernetické bezpečnosti reaguje i na incidenty neúmyslné či náhodné povahy, kybernetický útok bývá ze své podstaty veden úmyslně, zpravidla se záměrem způsobit škodu či získat neoprávněný prospěch (případně oboje). Míří na informační a komunikační systém a související hodnoty. Obsahově proto zahrnuje širokou škálu jednání. Uveďme dokument NATO zmiňující kybernetické hrozby (*cyber threats*) povahy politické, technologické, právní, ekonomické, manažerské i vojenské.[547] S tím souvisí i široké pole pro uplatnění reakce na kybernetický útok z hlediska mezinárodně - bezpečnostních vztahů, v jejichž rámci může být zvoleno také reaktivní opatření zcela mimo kyberprostor.[548]

Ve vztahu k triádě CIA, tj. zabezpečení důvěrnosti, integrity a dostupnosti informací a dat, lze rozlišit různé typy kybernetických útoků. Odvíjejí se od motivace útočníků, kteří obvykle cílí na krádež informací a dat (naruší důvěrnost dat), jejich změnu například za podvodnými účely (naruší integritu neboli celistvost dat), či chtějí zamezit přístupu k informacím oprávněnému uživateli, například s cílem získat finanční prospěch (naruší dostupnost dat).[549]

2.3.3. Narušení důvěrnosti a celistvosti informací a dat

2.3.3.1 Příklady

Kybernetický útok na důvěrnost informací a dat představuje úmyslné neoprávněné získání přístupu k datům, obvykle s cílem získání informací bez oprávnění. Neoprávněný přístup k datům dále vytváří příležitost pro narušení celistvosti dat, tj. k zásahům do jejich integrity. V důsledku narušení integrity dat může být narušena i hodnota informace (změněn informační potenciál dat), data se mohou stát nečitelnými, mohou být potlačena, změněna, vymazána, atp. Kybernetický útok na celistvost dat tak může být úzce provázán i s narušením dostupnosti dat a informací.

---

[546] Tamtéž.

[547] NATO. *National Cyber Security Framework Manual.* Op. cit.

[548] Tamtéž, str. 83.

[549] Srov. KOLOUCH, Jan. Op. cit., str. 185. Autor odkazuje na: SCHNEIER, Bruce. *The Internet of Things Will Turn Large - Scale Hacks into a Real World Disasters* [online]. Vice, 25. 7. 2016. Dostupné: https://www.vice.com/en/article/qkjzwp/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster [Cit. 2022-11-10].

Ke značné části bezpečnostních incidentů přispívá neznalost či nedostatečná obezřetnost uživatelů počítačových systémů. Šulc upozorňuje na časté využívání sociálního inženýrství, jelikož nejslabším článkem informační bezpečnosti ve veřejném i soukromém sektoru bývají zaměstnanci, kteří obvykle vykazují (shodně jako jejich vedoucí pracovníci) nízké bezpečnostní povědomí.[550] Sociální inženýrství definuje jako techniku *„ovlivňování, přesvědčování a manipulace s lidmi"*, přičemž útočníci téměř vždy využívají kombinace sociálního inženýrství a programovacích technik zneužívajících známé zranitelnosti (tzv. exploitů).[551]

Důvěrnost může být typicky narušena prostřednictvím škodlivého počítačového programu - malware[552] v podobě spyware. Spyware je počítačový program, který dovede splnit „špionážní" cíle útočníka, neboť bez vědomí a souhlasu oprávněného uživatele počítačového systému získává přístup k datům, která následně sdílí s počítačovým systémem ovládaným útočníkem. Může sledovat fyzickou polohu uživatele napadeného počítačového systému, jím navštěvované webové stránky, dokonce jej zvládne díky nevyžádanému zapnutí kamery a mikrofonu též odposlouchávat a nahrávat.[553] Spyware může rovněž obsahovat další nástroje ovládající činnost uživatele[554] a může se nacházet i v běžně dostupných a šířených programech, vyvinutých k plnění řádných funkcí počítače a požadavků jeho uživatele.[555]

Podobného ražení jako spyware je i škodlivý program označovaný jako Trojský kůň. Trojské koně jsou vybaveny skrytými funkcemi, o nichž jejich uživatelé neví - odtud název odkazující na bájný příběh z Trojské války o dobytí města Tróji Řeky pomocí lsti.[556] Kolouch upozorňuje, že v případě své aktivace může Trojský kůň zapříčinit nejen výmaz, blokaci, modifikaci, kopírování dat, či bránit obvyklému fungování počítačového systému a sítí, ale dovede i otevřít komunikační porty napadeného počítačového systému bez vědomí jeho uživatele; v posledním případě jde o tzv.

---

[550] ŠULC, Vladimír. Op. cit., str. 30.

[551] Tamtéž, str. 31.

[552] Jako malware lze označit počítačový program, který je využit ke škodlivé činnosti, jakou je obvykle narušení běžné funkce počítačového systému, případně s úmyslem získat neoprávněný přístup k počítačovému systému. Má mnoho podob, přičemž jeden druh malware může vykonávat i více škodlivých činností najednou. KOLOUCH, Jan. Op. cit., str. 204. Podrobněji k jednotlivým druhům malware tamtéž, str. 205 a násl.

[553] ŠULC, Vladimír. Op. cit., str. 36.

[554] KOLOUCH, Jan. Op. cit., str. 207.

[555] Tamtéž. Spyware bývá často využíván k získání marketingových informací o uživatelích daného programu, s cílem získat data o jejich aktivitách, preferencích apod., s čímž uživatel „nevědomky" předem souhlasil přijetím smluvních podmínek daného produktu. Tématu získání dat za marketingovými účely díky souhlasu udělenému v nepřehledných uživatelských podmínkách počítačových aplikací se věnuje např. dokument z roku 2013 s názvem Souhlasím s podmínkami od amerického režiséra Cullena Hobacka.

[556] HOMÉR. *Ílias*. 9. vydání. Praha: Odeon 1980.

backdoor programy usnadňující přímé ovládnutí napadeného počítače, které mohou být spojeny i se zneužitím skenovacích programů umožňujících zjistit využívané komunikační porty a jejich vhodnost vedení útoku skrze ně.[557] Trojské koně tím pádem mohou být nástrojem k narušení důvěrnosti i integrity informací a dat.

K narušení důvěrnosti informací a dat může být též zneužit tzv. keystroke logger, počítačový program zaznamenávající konkrétní stisky kláves na napadeném počítači, který umožňuje například získání citlivých přístupových údajů.[558] Poté, kdy útočník získá neoprávněně přístup do aplikace přihlášením se namísto oprávněného uživatele, může narušit také celistvost informací a dat.

Neoprávněný přístup k aplikacím, uživatelským účtům nejrůznějšího charakteru, bankovním informacích a dalším citlivým údajům, získávají útočníci rovněž skrze tzv. phishing. Jde o podvod spáchaný díky předstírání klamavých údajů s cílem vylákat z uživatele citlivé údaje, které jsou následně zneužity k dosažení finančního zisku. Podstatou phishingových útoků je tedy spíše sociální inženýrství.[559] Virtuální prostředí však umožňuje jednoduché rozesílání podvodných zpráv širokému okruhu potenciálních obětí, což obvykle vede k násobení neoprávněného zisku.[560]

Důvěrnost informací a dat lze narušit též skrze tzv. sniffing, nelegální odposlech dat procházejících počítačovou sítí při komunikaci mezi poskytovanou službou a počítačovým systémem; je však třeba jej odlišit od bezpečnostního monitoringu nestandardních projevů na síti správcem sítě, což se děje po právu a slouží k zachycení anomálií, a tím i k odhalení počítačového systému napadeného malwarem.[561]

K sofistikovaným útokům proti počítačovým systémům a sítím jsou využívány i tzv. botnety, sítě infikovaných počítačů umožňujících automatizovanou trestnou činnost.[562] Jejich podstatu shrnuje také Kolouch: *„Z pohledu práva je možné konstatovat, že botnety představují celé sítě infikovaných počítačových systémů, nad kterými do určité míry neoprávněně převzala kontrolu třetí osoba, a to bez vědomí oprávněných uživatelů."*[563] Botnet je tvořen velkým množstvím IP adres infikovaných malwarem, které mohou být ovládány skrze počítačovou síť administrátorem, aniž by

---

[557] KOLOUCH, Jan. Op. cit., str. 208 - 209.

[558] Tamtéž, str. 210.

[559] WALL, David. Op. cit., str. 49.

[560] Konkrétní případy phishingu rozebírá KOLOUCH, Jan. Op. cit., str. 246 an.

[561] Tamtéž, str. 294.

[562] WALL, David. Op. cit., str. 150 a násl.

[563] KOLOUCH, Jan. Op. cit., str. 203.

o tom jejich majitelé (či oprávnění uživatelé) věděli.[564] Na černém trhu jsou botnety ceněnou komoditou.[565] Spolu s černým trhem provozovaným na síti Darknet a teroristickými útoky je existence botnetů důvodem vzájemných jednání suverénních států o spolupráci při potírání těchto nežádoucích jevů.

Někteří nahlížejí na případy počítačové kriminality páchané skrze botnet jako na specifickou formu organizovaného zločinu.[566] Ačkoli lze souhlasit s tím, že botnet představuje koordinovanou, organizovanou, efektivní a nebezpečnou formu páchání počítačové trestné činnosti v prostředí globálních počítačových sítí, ovládán je zpravidla jediným administrátorem, nikoli organizovanou skupinou více osob. Z tohoto důvodu nelze botnet vztáhnout pod definici organizovaného zločinu tak, jak jej pojímá např. mezinárodní úmluva OSN proti nadnárodnímu organizovanému zločinu.[567]

2.3.4. Narušení dostupnosti informací a dat

2.3.4.1. Příklady

Kybernetický útok na dostupnost informací a dat představuje úmyslné znemožnění či bránění oprávněným uživatelům použít potřebná data a informace (tedy i aplikace, služby, databáze, apod.). Typicky půjde o útoky označované jako DoS (*Denial of Service*, neboli odepření služby) a DDoS (*Distributed Denial of Service*, neboli distribuované odepření služby), jejichž cílem je vyřazení počítačového zařízení z chodu nebo významné omezení jeho fungování.[568] Podstatou jsou řízené útoky značného množství počítačů pomocí přístupových požadavků na konkrétní místo v síti, což následně způsobí její přetížení. Dalším způsobem útoku je zahlcení počítačového systému opakujícími se požadavky na úkony, načež dojde k nápadnému zpomalení služby nebo až k její

---

[564] Tamtéž, str. 193 a násl.

[565] Průměrná cena za 24hodinový pronájem botnetu v roce 2010 činila 67 USD. Srov. DANCHEV, Dancho. *Study finds the average price for renting a botnet* [online]. ZDNet, 26. 5. 2010. Dostupné: http://www.zdnet.com/article/study-finds-the-average-price-for-renting-a-botnet/ [Cit. 2022-11-11].

[566] CHANG, Lennon Y. C. *Cybercrime in the Greater China Region: Regulatory Response and Crime Prevention across the Taiwan Strait* [online]. Edward Elgar, 2012. Dostupné: https://www.researchgate.net/publication/301693009_Cybercrime_in_the_Greater_China_Region_Regulatory_Response_and_Crime_Prevention_across_the_Taiwan_Strait [Cit. 2022-11-11].

[567] Sdělení č. 75/2013 Sb. m. s., Ministerstva zahraničních věcí o sjednání Úmluvy Organizace spojených národů ze dne 15. listopadu 2000 proti nadnárodnímu organizovanému zločinu.
Čl. 2 písm. a) této úmluvy definuje organizovanou zločineckou skupinu jako *„strukturovanou skupinu tří nebo více osob, existující po určité časové období a jednající ve vzájemné shodě s cílem spáchat jeden či více závažných trestných činů nebo trestných činů stanovených v souladu s touto Úmluvou, aby získala, přímo či nepřímo, finanční nebo jiný hmotný prospěch."*

[568] U DoS je jediný zdroj útoku, kterému je snazší se ubránit blokováním provozu z něj. U DDoS se nachází zdroje útoku na více různých místech zpravidla odlišné polohy, což vede k jejich náročnějšímu odhalení a blokování. Dalším druhem útoku je DRDoS, které využívá chyby v operačních systémech a rozesílání odpovědí na fiktivní DoS. KOLOUCH, Jan. Op. cit., str. 296 - 297.

nedostupnosti.[569] Kromě znemožnění přístupu oprávněným uživatelům k službě dochází k zablokování webové stránky nebo i serveru. Podíl kybernetických útoků narušujících dostupnost informací a dat způsobených DoS/DDoS útoky nebo sabotážemi meziročně stoupá; v červnu 2022 tvořily 75% všech NÚKIB zaznamenaných kybernetických bezpečnostních incidentů.[570] V říjnu 2022 došlo k mimořádnému nárůstu zaznamenaných útoků na dostupnost (DoS, DDoS útoky nebo sabotáže), které tvořily 74% všech NÚKIB zaznamenaných kybernetických bezpečnostních incidentů (až na jediný případ šlo pouze o DDoS útoky) a jejich počet téměř vyrovnal souhrnný počet všech útoků tohoto typu za celý rok 2022.[571]

NÚKIB popisuje kybernetický útok typu DoS jako *„kybernetický útok, který má za cíl omezit nebo vyřadit služby počítačových systémů. Zpravidla se jedná buď o generování velkého množství podvržených požadavků s cílem zahltit systém a/nebo přenosovou cestu nebo jde o sofistikovaný útok na slabá místa v cílovém systému a/nebo přenosové cestě"* a útok DDoS označuje za *„kybernetický útok typu DoS, který probíhá najednou koordinovaně z mnoha uzlů sítě."*[572] NÚKIB zdůrazňuje úlohu sledování systémů i síťového provozu a při zachycení anomálií a potvrzení, že jde o útok, doporučuje kontaktovat neprodleně poskytovatele internetového připojení a příslušný bezpečnostní tým CERT/CSIRT. Jeho role je však především koordinační, neboť za bezpečnost odpovídá vždy konkrétní správce subjektu, který se stal předmětem útoku.[573]

O DDoS útocích se zmiňuje i Úmluva o počítačové kriminalitě v čl. 5 jako o „zasahování do systému" (srov. shora). Z hlediska české trestněprávní úpravy dopadá na taková jednání skutková podstata trestného činu poškození a ohrožení provozu obecně prospěšného zařízení v úmyslné i nedbalostní formě ve smyslu § 276 a § 277 trestního zákoníku. Výkladové ustanovení § 132 trestního zákoníku řadí mezi obecně prospěšná zařízení také zařízení a sítě elektronických komunikací. Může se jednat o server využívaný širokou veřejností, jehož užívání bude znemožněno právě DDoS útoky. DDoS útoky bývají typicky páchány tzv. automatizovaně, prostřednictvím

---

[569] KOLOUCH, Jan. Op. cit., str. 296.

[570] NÚKIB. *Kybernetické incidenty pohledem NÚKIB: červen 2022.* Op. cit., str. 3.

[571] NÚKIB. *Kybernetické incidenty pohledem NÚKIB: říjen 2022*. Op. cit., str. 3-4. Podle NÚKIB byla jednou z příčin skupina Anonymous Russia útočící proti českým subjektům. Tamtéž, str. 4.

[572] NÚKIB. *DoS / DDoS útoky: Doporučení pro případ napadení DDoS útokem - jak se zachovat a jak postupovat* [online]. Dostupné: https://nukib.cz/download/publikace/doporuceni/Doporuceni_DDoS.pdf [Cit. 2022-11-11].

[573] Tamtéž, str. 2.

napadených počítačů, které byly infikovány za pomoci spamu a sociálního inženýrství.[574] Počítač napadený malwarem se může obvykle stát i součástí tzv. botnetu a bez vědomí majitele či oprávněného uživatele být zneužíván k automatizované trestné činnosti.

Příkladem kybernetického útoku ve formě DDoS, který mířil na zamezení dostupnosti informací a dat jsou útoky na estonskou státní infrastrukturu, k nimž došlo v roce 2007. V evropské geografické oblasti se útoky staly milníkem v přístupu ke kybernetické bezpečnosti a byly jedním z důvodů, proč NATO zahrnulo kybernetickou obranu mezi klíčové úkoly kolektivní obrany členů aliance. Roku 2007 došlo v Tallinnu, hlavním městě Estonska, jež má historicky dlouhodobě vyhraněné vztahy s Ruskem,[575] k odstranění ruského válečného pomníku. Následně se staly webové stránky estonské vlády i další estonské webové stránky vybraných politických stran, médií či finančních institucí, terčem několikatýdenních kybernetických útoků, které je vyřadily z provozu. Estonsko obvinilo z útoků Rusko a zaměřilo se na posílení odolnosti svých významných informačních infrastruktur a sítí. Dnes sídlí v Tallinnu centrum NATO pro kybernetickou bezpečnost a Estonsko se úrovní své kybernetické obrany řadí k nejlépe zabezpečeným státům světa.[576]

Odlišným případem omezení dostupnosti služeb na principu DDoS útoku jsou situace, kdy dojde k hromadným či opakovaným požadavkům na přihlášení se k poskytované službě ze strany velkého množství uživatelů, kteří tak činí ze svých počítačů vědomě. Mohou mít právě v úmyslu přetížit danou webovou stránku v důsledku opětovného přihlašování se. V takovém případě není výjimkou vzájemná předchozí domluva na zadávání přístupových požadavků ve smluvený čas. K podobným útokům docházelo v roce 2012 v souvislosti s protesty proti ACTA.[577] Jeden z prostředků k naplánování okamžiku přetížení služby - ke stažení volně dostupnou aplikaci LOIC (*Low Orbit Ion Cannon*) testující vytížení sítě, poskytlo hnutí Anonymous.[578] Hackerské hnutí Anonymous je známé svým zapojením do politických i válečných incidentů a formou DDoS útočí proti webovým stránkám vybraných společností. Roku 2011 například hnutí podporovalo rebely

---

[574] Spamem označujeme obvykle nevyžádanou elektronickou poštu reklamního charakteru. Spam není sám o sobě škodlivý, může však v příloze obsahovat soubor se škodlivým programem (tzn. malware), který napáchá škodu. Za sociální inženýrství lze označit jednání útočníka, který podvodnými způsoby vyláká z oběti citlivá data, často přístupové údaje či osobní data nutná k přihlášení se na účet a k provedení operací finančního charakteru.

[575] Srov. např. SUBRENAT, Jean-Jacques. *Estonia: identity and independence*. New York: Rodopi, 2004.

[576] PAVLIKOVÁ, Miroslava. Op. cit.

[577] Z anglického Anti-Counterfeiting Trade Agreement, neboli Obchodní dohoda proti padělatelství. V ČR byl proces ratifikace této mezinárodní smlouvy pozastaven. VLÁDA. *Vláda pozastavuje ratifikaci dohody ACTA* [online]. Vláda ČR, 6. 2. 2012. Dostupné: https://www.vlada.cz/cz/media-centrum/aktualne/vlada-pozastavuje-ratifikaci-dohody-acta-92694/ [Cit. 2022-11-11].

[578] KOLOUCH, Jan. Op. cit., str. 299.

proti plukovníku Kaddáfímu v libyjské občanské válce. Ve své kampani hnutí označilo Internet za další prostředí boje proti diktatuře libyjského vůdce a poskytovatele připojení k Internetu vyzvalo k ukončení spolupráce s plukovníkem Kaddáfím.[579] Dne 27. 2. 2022, několik dní po napadení Ukrajiny Ruskem, hnutí Anonymous zveřejnilo video, v němž oznamuje ruskému prezidentu Vladimiru Putinovi, že za ruskou agresi vůči Ukrajině bude čelit nevídaným kyberútokům z celého světa.[580] Několik dní poté hnutí na svém twitterovém účtu uvedlo: *„Od vyhlášení kybernetické války zločineckému režimu Kremlu hnutí Anonymous nabouralo přes 2500 webových stránek ruské a běloruské vlády, státních médií, bank, nemocnic, letišť, společností a proruských hackerských skupin",* přičemž nejčastějším nástrojem byly právě útoky typu DDoS.[581] Pomocí útoků DDoS byly vyřazeny z provozu weby Kremlu, ruské vlády a ruského ministerstva obrany, či stanice RT, dříve známé jako Russia Today, která podle hnutí šíří prokremelskou propagandu.[582] Existují ovšem i proruské (resp. prokremelské) skupiny označující se za součást hnutí Anonymous.[583] Kromě politických aktivit a cílů se hnutí Anonymous dlouhodobě zaměřuje i na potlačení šíření dětské pornografie na Internetu. V dubnu 2013 dočasně vyřadilo z provozu řadu webových stránek šířících materiál dětské pornografie.[584] Ověřit objektivitu uvedených zpráv ovšem bývá obtížné, neboť hackerská uskupení obvykle úspěšnost svých kybernetických útoků spíše zveličují, zatímco jejich cíle je negují a dopady útoku bagatelizují.

Dalším způsobem zamezení dostupnosti informací a dat může být použití malware, tedy škodlivého počítačového programu, který naruší běžný chod počítačového zařízení. Malware může mít mnoho podob a je schopen instalace do nejrůznějších počítačových zařízení, včetně mobilních telefonů a chytrých domácích spotřebičů (viz koncept *Internet of Things*). Narušit dostupnost informací a dat může např. adware, program zobrazující reklamy, a to za předpokladu zahlcení obrazovky obrovským množstvím nevyžádaných reklamních oken do té míry, že znemožní další práci na počítači. Nebezpečnější podobu malware blokujícího data však mohou představovat viry.

---

[579] BROADHURST, Roderic, GRABOSKY, Peter, ALAZAB, Mamoun, BOUHOURS, Brigitte, CHON, Steve, DA, Chen. Crime in Cyberspace: Offenders and the Role of Organized Crime Groups [online]. *Australian National University Cybercrime Observatory,* 2013, str. 7. Dostupné: http://ssrn.com/abstract=2211842 [Cit. 2022-11-11].

[580] IDNES. *Čekejte kyberútok, vzkázali Anonymous Putinovi* [online]. 27. 2. 2022. Dostupné: https://tv.idnes.cz/zahranicni/rusko-ukrajina-anonymous-kyberutok-hrozba-putin-vladimir.V220227_104405_idnestv_vojt [Cit. 2022-11-11].

[581] FIŠER, Miloslav. *Kybernetická válka: Anonymous napadli 2500 ruských a běloruských cílů* [online]. novinky.cz, 4. 3. 2022. Dostupné: https://www.novinky.cz/valka-na-ukrajine/clanek/kyberneticka-valka-anonymous-napadli-2500-ruskych-a-beloruskych-cilu-40389280 [Cit. 2022-11-11].

[582] Tamtéž.

[583] NÚKIB. *Kybernetické incidenty pohledem NÚKIB: říjen 2022*. Op. cit., str. 4.

[584] Tamtéž, str. 4 - 5.

Kolouch upozorňuje na existenci velkého množství různých virů, jejichž cílem je ničit, případně osídlit co největší počet počítačových systémů, které mají být následně zneužity k útoku. Projevem některých virů je zahlcení počítačového systému, změna či zničení dat i celého systému. K výmazu, blokaci a změnám dat mohou být využíváni i Trojští koně, tj. počítačové programy se skrytými funkcemi.[585]

K zahlcení počítačového systému mohou přispět i počítačoví červi, kteří se dovedou rychle šířit po síti narozdíl od počítačových virů samostatně bez napojení na jiný program, přičemž dovedou vyhledávat nedostatky v zabezpečení počítačových programů a systémů.[586]

Specifickým typem malware je ransomware - vyděračský škodlivý počítačový program, který brání oprávněnému uživateli v obvyklém užívání počítačového systému do doby, než zaplatí výkupné.[587] Formou ransomware byl v lednu 2022 veden kybernetický útok hackerské skupiny bojující proti režimu běloruského prezidenta Alexandra Lukašenka. Útočníci zašifrovali systémy veřejného železničního dopravce, čímž způsobili rozsáhlé zpoždění spojů. Klíč k dešifrování nabídli za propuštění 50 politických vězňů s potřebou lékařské pomoci. V neděli 27. 2. 2022 zaútočili běloruští „kyberpartizáni" na běloruskou železnici opětovně a formou útoku DDoS (srov. výše) vyřadili 90% sítě a vybavení dopravce mimo provoz.[588]

Způsoby, jimiž se malware šíří počítačovými sítěmi a systémy, jsou mnohé. Nejčastěji k jeho šíření dochází s určitým přičiněním nepoučeného nebo podvedeného uživatele počítače.[589]

2.3.4.2. Exkurz - Stuxnet

Roku 2010 se na veřejnosti objevila aféra ohledně počítačového červu Stuxnet, který byl původně vyvinutý za účelem vzdálené kontroly a ovládání průmyslových systémů dispečerského řízení dat, známých pod anglickou zkratkou SCADA (*Supervisory Control and Data Aquisition*). Broadhurst a kol. uvádějí, že byl komplexní počítačový program vyvinut v rámci utajené spolupráce tajných služeb Izraele a USA, s cílem překazit íránský nukleární program. Vlády obou států

---

[585] KOLOUCH, Jan. Op. cit., str. 207 - 208. Maskovat výskyt škodlivého programu dovede nástroj zvaný rootkit. Podrobněji k němu srov. tamtéž, str. 209 a násl.

[586] Tamtéž, str. 208.

[587] Kolouch uvádí dva typy ransomware: první omezí fungování celého počítačového systému bez jakékoli možnosti jeho dalšího využití, druhý ponechá systém funkční, avšak znepřístupní uživateli jeho data. Podrobněji k ransomware a vývoji jeho forem KOLOUCH, Jan. Op. cit., str. 221 a násl.

[588] MAGDOŇOVÁ, Jana, ANDRLE, Vít. *Hackeři zaútočili na běloruské železnice. Výrazně zpomalili přesun ruské vojenské techniky k Ukrajině* [online]. irozhlas.cz, 6. 3. 2022. Dostupné: https://www.irozhlas.cz/zpravy-svet/hackeri-kyberneticky-partizan-ukrajina-belorusko-vlaky_2203061205_ban [Cit. 2022-11-11].

[589] Podrobněji se jednotlivým cestám šíření malware věnuje Kolouch. KOLOUCH, Jan. Op. cit., str. 211 a násl.

existenci operace i vzájemnou spolupráci na ní popírají. Malware byl instalován do SCADA systému jaderného zařízení na obohacování uranu v íránském Natanzu a skrze jeho vzdálenou kontrolu bylo zničeno několik centrifug zařízení. Důsledkem uvedeného útoku došlo i ke zpomalení íránského jaderného programu. K odhalení Stuxnetu nakonec přispěla programátorská chyba.[590]

Forenzní analýza po útoku odhalila, že škodlivý program byl vyvinut díky detailním informacím o nastavení počítačových systémů v Natanzu. Útočníci patrně spolupracovali s osobou pohybující se uvnitř jaderného zařízení, která jim poskytla klíčové informace. Díky interním informacím byl kód počítačového červa před zahájením útoku několikrát přizpůsoben, aby bylo zaručeno, že dojde k účinku pouze při nálezu specifické konfigurace počítačového zařízení i podmínek v počítačové síti. První verzi Stuxnetu bylo proto možné označit za cílený útok zaměřený na jedinou síť, navržený s cílem samostatného šíření na další počítačové systémy pouze uvnitř této sítě.[591] Při druhém opakování však útočníci infikovali počítačové systémy externích dodavatelů elektrárny, vlivem čehož došlo k rozšíření malware i mimo zařízení v Natanzu, když se šířil i do počítačových zařízení jiných zákazníků externích dodavatelů elektrárny (patrně skrze vyměnitelná media). Tím se však Stuxnet „utrhl ze řetězu". Následným šířením po sítích a skrze internetové kanály nakazil v konečném důsledku přes 100 000 počítačových systémů po celém světě. Vlivem specifického naprogramování, jež ukládalo působit pouze v prostředí počítačových systémů Natanzu, však Stuxnet nezpůsobil nekontrolovatelné škody, byť došlo k jeho nekontrolovatelnému rozšíření i mimo počítačové systémy v Natanzu.[592]

Uvedená charakteristika Stuxnetu vede některé autory k závěru, že z hlediska aplikace mezinárodního práva byl Stuxnet v souladu s doktrínou cíleného útoku.[593] Jakékoli případné škody v civilní oblasti, způsobené mimo počítačové systémy a sítě elektrárny v Natanzu, by patrně bylo možné označit za způsobené neúmyslně.

Stuxnet lze vnímat jako jednu z nejrozsáhlejších sabotáží provedených pomocí ICT nástrojů. Před Stuxnetem nebylo obvyklé preventivně zabezpečovat průmyslové řídící systémy, neboť mnozí se domnívali, že již jejich samotným izolováním od globálních počítačových sítí bude dosaženo

---

[590] BROADHURST, Roderic, GRABOSKY, Peter, ALAZAB, Mamoun, BOUHOURS, Brigitte, CHON, Steve, DA, Chen. Op. cit., str. 5.

[591] KAMINSKA, Monica, BROEDERS, Dennis, CRISTIANO, Fabio. Limiting Viral Spread: Automated Cyber Operations and the Principles of Distinction and Discrimination in the Grey Zone [online]. *13th International Conference on Cyber Conflict: 'Going Viral'*, 30. 5. 2021, str. 69 - 70. Dostupné: https://ssrn.com/abstract=3856623 [Cit. 2022-11-11].

[592] Tamtéž.

[593] Tamtéž, str. 71.

kýžené ochrany. Případ Stuxnet však upozornil širokou veřejnost, že také počítačová zařízení, která nejsou připojená ke globální síti, bude zapotřebí zabezpečit před kybernetickými útoky.[594]

2.3.5. Přehled vybraných právních předpisů a norem

Problematika bezpečnosti informací a dat je komplexní téma, jehož se dotýká řada právních předpisů. Kybernetickou bezpečnost sice v českém právním prostředí upravuje poměrně celistvě zákon o kybernetické bezpečnosti, pro oblast však mohou být důležité i některé právní předpisy a dokumenty z oblasti mezinárodního práva. Může se jednat jak o vyhlášené mezinárodní smlouvy, jimiž je stát vázán a které mají přednost před vnitrostátními předpisy, tak o dokumenty charakteru soft law či o nejrůznější standardy a normy, které mohou soukromé i veřejné subjekty převzít za své. Kromě stručnějšího rozboru ZKB pojednává následující text proto též o dalších právních předpisech a nezávazných normách, které mohou být z hlediska českého kyberprostoru zásadní.[595]

2.3.5.1. Úmluva o počítačové kriminalitě

Z hlediska vyhlášených mezinárodních smluv, s jejichž ratifikací vyslovil Parlament ČR souhlas, jimiž je ČR vázána a jsou tak součástí jejího právního řádu (čl. 10 Ústavy ČR), a současně se dotýkají problematiky bezpečnosti informací a dat, zaujímá zásadní postavení Úmluva o počítačové kriminalitě. Ve smyslu čl. 10 Ústavy ČR je její podstatnou vlastností aplikační přednost před zákonem: stanoví-li Úmluva o počítačové kriminalitě něco jiného než zákon, použije se úmluva.

Jak bylo zdůrazněno výše, Úmluva o počítačové kriminalitě chrání dostupnost informací a dat i jejich důvěrnost a integritu (celistvost). Kategorie jsou vzájemně provázané: zachování integrity dat a počítačových systémů je podmínkou jejich použitelnosti, a tím i dostupnosti informací a služeb. Sjednocením, či alespoň podstatnou harmonizací skutkových podstat trestných činů proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů dle Oddílu 1 Kapitoly II Úmluva o počítačové kriminalitě vytváří podmínky pro postih počítačové trestné činnosti ze strany

---

[594] KASPERSKY. Stuxnet: Victims Zero [online]. *Kaspersky Daily*, 18. 11. 2014. Dostupné: https://www.kaspersky.com/blog/stuxnet-victims-zero/6775/ [Cit. 2022-11-11].

[595] Nejedná se nicméně o vyčerpávající přehled všech možných pramenů práva. Ten by závisel na konkrétním řešeném problému (např. problematika odpovědnosti z hlediska soukromoprávní či veřejnoprávní úpravy, existence mezinárodního prvku, atd.) a přesahuje již prostor této práce.

vnitrostátních orgánů činných v trestním řízení, včetně podmínek mezinárodní spolupráce při vyšetřování.[596]

Důvěrnost, integrita a dostupnost informací a dat je chráněna povinností smluvních stran stíhat jako trestné činy tzv. nezákonný přístup i nezákonný odposlech. Čl. 2 Úmluvy o počítačové kriminalitě definuje nezákonný přístup následovně: *„Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů byl trestným činem, pokud je spáchán úmyslně, neoprávněný přístup k celému počítačovému systému nebo jeho jakékoli části. Strana může stanovit, že bude považovat tento čin za trestný, jen pokud je spáchán porušením bezpečnostních opatření, s úmyslem získat počítačová data nebo s jiným nečestným úmyslem, nebo ve vztahu k počítačovému systému, který je spojen s jiným počítačovým systémem."*

Nezákonný přístup je obecným trestným činem chránícím všechny složky bezpečnosti informací - jejich důvěrnost, integritu i dostupnost. Principiálně by jakékoli neoprávněné narušení počítačového systému či dat mělo být protiprávním, neboť může omezit činnost oprávněných uživatelů, způsobit změnu či poškození dat, což si vyžádá vysoké náklady na jejich obnovu, způsobit únik citlivých údajů, včetně hesel a klíčových informací o počítačovém systému, přičemž může také podnítit páchání další trestné činnosti.[597] Nezákonný přístup rovněž může představovat narušení soukromého a rodinného života uživatele napadeného počítačového zařízení.

Úmluva o počítačové kriminalitě ponechala na smluvních stranách, zda budou považovat za trestný i čin, jímž nebude porušeno žádné bezpečnostní opatření, případně čin spáchaný bez konkrétního škodlivého úmyslu (obmyslu). ČR přistoupila ke kriminalizaci neoprávněného přístupu k počítačovému systému nebo k jeho části, překoná-li pachatel současně bezpečnostní opatření.[598] Pokud by pachatel nepřekonal žádné bezpečnostní opatření, vyžaduje český trestní zákoník k trestnosti činu, aby pachatel svým jednáním naplnil zároveň další kvalifikační okolnosti: aby neoprávněně užil uložená data, neoprávněně je vymazal nebo zničil, poškodil, změnil, potlačil, snížil jejich kvalitu, atd.[599]

Ochranou důvěrnosti se zabývá i čl. 3 Úmluvy o počítačové kriminalitě, který upravuje tzv. nezákonný odposlech. Stanoví povinnost smluvním stranám přijmout „*taková legislativní a jiná*

---

[596] RADA EVROPY. Op. cit., bod 16.

[597] Tamtéž, bod 44.

[598] Srov. základní skutkovou podstatu v § 230 odst. 1 trestního zákoníku.

[599] Viz další základní skutková podstata v § 230 odst. 2 trestního zákoníku. Podrobněji kybernetické trestné činy, včetně trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací, rozebírá KOLOUCH, Jan. Op. cit., str. 338 an.

opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů byl trestným činem úmyslný, neoprávněný, technickými prostředky provedený odposlech neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému přenášejícího taková počítačová data. Strana může stanovit, že bude považovat tento čin za trestný, jen pokud je spáchán s nečestným úmyslem, nebo ve vztahu k počítačovému systému, který je spojen s jiným počítačovým systémem."

Citovaná skutková podstata chrání soukromí datové komunikace. Vztahuje se na veškerý přenos elektronických dat, bez ohledu na použité médium či technologické zařízení. Nezákonný odposlech dat lze postavit na roveň nezákonnému prostorovému odposlechu či odposlechu telefonické konverzace, jež jsou známy z offline světa. Úprava klade důraz na ochranu soukromí, jak stanoví i čl. 8 Evropské úmluvy o ochraně základních lidských práv a svobod (dále jen „EÚLP").[600]

Dostupnost informací a dat je chráněna požadavkem postihu zasahování do dat ve smyslu čl. 4 Úmluvy o počítačové kriminalitě, jenž ukládá smluvním stranám přijmout *„taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů bylo trestným činem, pokud je spácháno úmyslně, neoprávněné poškození, vymazání, snížení kvality, pozměnění nebo potlačení počítačových dat*."[601] Smluvní strany úmluvy si nicméně mohou vyhradit právo stanovit, že budou považovat popsané jednání za trestné pouze pokud způsobí závažnou škodu.[602] K tomu ze strany ČR nedošlo a k trestnosti se tudíž nevyžaduje vznik škody.

Podle výkladových ustanovení jsou poškození a snížení kvality počítačových dat vzájemně se přesahující pojmy znamenající především negativní změny v celistvosti a informačním potenciálu počítačových dat a programů. Pozměnění dat je modifikací existujících dat, např. v důsledku škodlivých počítačových programů (viry, Trojské koně apod.); výmaz dat je postaven na roveň zničení fyzické věci, zatímco potlačení dat má označovat jakékoli jednání, které zamezí, aby data byla dostupná osobě s přístupem k počítači nebo nosiči dat.[603]

Rozlišit vymazání dat od jejich potlačení může být obtížné, neboť data se mohou osobě s uživatelskými znalostmi jevit jako smazaná, ač mohou být (částečně) na nosiči stále dostupná. Jak se lze dočíst i v řadě popularizačních článků na webu, výmaz dat z pevného disku či jiného

---

[600] RADA EVROPY. Op. cit., bod 51. Podrobněji k pojmům technické prostředky a neveřejný přenos srov. tamtéž, body 53 a 54.

[601] Čl. 4 odst. 1 Úmluvy o počítačové kriminalitě.

[602] Čl. 4 odst. 2 Úmluvy o počítačové kriminalitě.

[603] RADA EVROPY. Op. cit., bod 61.

paměťového média obvykle pouze odstraní cestu k vymazaným datům, ta však stále existují v nezměněné podobě - došlo toliko k odstranění cesty, kterou by viděl operační systém tak, aby data zobrazil uživateli.[604] Mnohé z dostupných programů na výmaz dat uložených na paměťových médiích staví na několikanásobném přepsání původních dat náhodnými daty, šance na obnovu původních dat však může stále existovat. Spolehlivou se jeví až metoda demagnetizace, která v případě magnetických paměťových médií trvale odstraní data působením silného magnetického pole, anebo přímo fyzická likvidace paměťového média.[605]

Aby bylo jednání popsané v čl. 4 odst. 1 Úmluvy o počítačové kriminalitě trestné, musí pachatel jednat úmyslně a bez oprávnění. Oprávněná likvidace či potlačení dat, např. v důsledku splnění požadavků na jejich výmaz, při rekonfiguraci operačního systému či vlivem testování zabezpečení počítačového systému, kdy k jednání dochází se souhlasem majitele či oprávněného uživatele, není protiprávní, a tudíž ani trestné.[606]

Dostupnost informací a dat je chráněna rovněž požadavkem stíhat tzv. zasahování do systému ve smyslu čl. 5 Úmluvy o počítačové kriminalitě. Smluvním stranám je zde uloženo přijmout *„taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů bylo trestným činem, pokud je spácháno úmyslně, neoprávněné závažné omezení funkčnosti počítačového systému vkládáním, přenášením, poškozením, vymazáním, snížením kvality, pozměněním nebo potlačením počítačových dat."*[607]

Důvodová zpráva k Úmluvě o počítačové kriminalitě uvádí, že zmíněné ustanovení dopadá na počítačovou sabotáž, tj. úmyslné bránění oprávněnému užívání počítačových systémů, včetně telekomunikačních zařízení, skrze ovlivňování počítačových dat. Omezení funkčnosti počítačového systému musí být závažné, aby bylo trestně postižitelné, přičemž hranice závažnosti je ponechána na vnitrostátní právní úpravě, ustanovení má však typicky dopadat na útoky typu DDoS či spáchané pomocí malware, které podstatně zpomalí či zcela zamezí fungování systému. Díky neutrální formulaci však ustanovení chrání řadu funkcí. Dopadá i na zasílání spamu s cílem blokovat komunikační funkce systému.[608]

---

[604] VOŘÍŠEK, Lukáš. *Obyčejné smazání nestačí, data dokáže obnovit kdokoli: Jak bezpečně smazat soubory a zničit pevný disk?* [online]. inSmart.cz, 7. 6. 2019. Dostupné: https://insmart.cz/jak-trvale-smazat-data/ [Cit. 2022-11-12].

[605] Tamtéž.

[606] RADA EVROPY. Op. cit., body 62 - 63.

[607] Čl. 5 Úmluvy o počítačové kriminalitě.

[608] RADA EVROPY. Op. cit., body 65 - 67.

Současně Úmluva o počítačové kriminalitě stanoví požadavek kriminalizovat jednání, které může být materiálně přípravou k trestné činnosti popsané shora. Čl. 6 odst. 1 písm. a) ukládá stíhat úmyslnou a neoprávněnou výrobu, prodej, opatření za účelem použití, dovoz, distribuci nebo jiné zpřístupnění zařízení, včetně počítačového programu, vytvořeného nebo přizpůsobeného zejména za účelem spáchání trestného činu zasahování do dat nebo trestného činu zasahování do systému. Stejně má být stíhána výroba, prodej, opatření za účelem použití, dovoz, distribuce nebo jiné zpřístupnění počítačového hesla, přístupového kódu nebo podobných dat, pomocí nichž lze získat přístup do celého počítačového systému nebo do jakékoli jeho části s tím úmyslem, že jej bude použito pro účely spáchání trestného činu zasahování do dat nebo trestného činu zasahování do systému.[609] Kriminalizováno má být i pouhé držení shora vyjmenovaných položek s úmyslem spáchání trestného činu zasahování do dat nebo trestného činu zasahování do systému.[610] Úmluva však připouští výhradu z uvedeného požadavku kriminalizace za podmínky, že se taková výhrada nebude týkat prodeje, distribuce nebo jiného zpřístupnění počítačového hesla, přístupového kódu nebo dat, pomocí nichž lze získat přístup do počítačového systému nebo jeho části.[611] Takovou výhradu ČR neučinila.

Vznik citovaného čl. 6 Úmluvy o počítačové kriminalitě provázely rozsáhlé debaty o tom, zda stanovit jako trestné držení jakýchkoli zařízení, která by mohla být využita k páchání trestné činnosti proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů (*dual-use devices*), anebo pouze těch zařízení přímo či výslovně určených k jejímu páchání. Oba přístupy byly nakonec odmítnuty s ohledem na příliš obtížné prokazování. Řešením se stal přístup založený na prokazování subjektivní stránky trestného činu - držení zařízení právě v úmyslu spáchat počítačový trestný čin.[612] Otázkou je, zda by nebylo jednodušší prokazovat držení počítačového programu specificky určeného např. k vedení útoku DDoS, než úmysl takový útok spáchat.

2.3.5.2. Opatření pro budování důvěry v kyberprostoru

Specifickým nástrojem pro prevenci konfliktů v kyberprostoru a udržení míru v mezinárodním prostředí jsou opatření pro budování důvěry v kyberprostoru (*Confidence Building Measures for Cyberspace*). Ačkoli nejde o právně závazné dokumenty, jakým byla právě zmíněná

---

[609] Čl. 6 odst. 1 písm. a) body i, ii. Úmluvy o počítačové kriminalitě.

[610] Čl. 6 odst. 1 písm. b) Úmluvy o počítačové kriminalitě.

[611] Čl. 6 odst. 3 Úmluvy o počítačové kriminalitě.

[612] RADA EVROPY. Op. cit., bod 73.

Úmluva o počítačové kriminalitě, představují opatření praktický politický nástroj, který se snaží za pomoci pravidel krizového managementu mezi jednotlivými státy předejít válečnému konfliktu, k němuž by jinak mohlo dojít z důvodu chybně vnímaného rizika nebo nesprávného odhadu krizové situace.[613] Přitom právě politická prohlášení států lze v rámci mezinárodních vztahů vnímat jako mocný nástroj pro rozvoj obecných principů mezinárodního práva, jež jsou pro státy již obecně závazné.[614]

Již od 90. let 20. století se objevují debaty o úmluvě, která by omezila riziko vzniku kybernetického konfliktu v mezinárodním prostředí, nicméně právě důraz na tento smluvní instrument se neukázal jako vhodný k zajištění bezpečnosti.[615] Ruská federace navrhla v roce 1998 jako první přijetí mezinárodní úmluvy zamezující zneužití kyberprostoru pro vojenské účely, avšak využití tradičních mechanismů kontrolujících použití zbraní v kyberprostoru se nejevilo pravděpodobným.[616] Naopak, následný vývoj ukázal, že řada států (včetně Ruské federace) běžně využívá kyberprostor jako další doménu pro prosazování svých cílů, nejen v rámci vojenských konfliktů.[617]

Proti přijetí závazné mezinárodní úmluvy rovněž stojí skutečnost, že jakákoli kontrola výskytu škodlivých počítačových programů v kyberprostoru je velmi obtížná, neboť by znamenala souhlas států s monitoringem všech počítačových zařízení, včetně vládních nebo využívaných zpravodajskými službami; problematická je i atribuce kybernetického útoku a zneužívání malware ze strany nestátních aktérů.[618] Právně nezávazné nástroje, jakými jsou opatření pro budování důvěry, proto nalézají v oblasti kyberprostoru uplatnění.

Obecný smysl a úlohu těchto opatření vyjádřila Konzultační skupina komise OSN pro odzbrojení v roce 1988 především jako posílení mezinárodního míru a bezpečnosti za pomoci zamezení všem válkám, odstranění příležitostí ke vzniku vzájemné nedůvěry, strachu a neporozumění ve vztahu k vojenským aktivitám a vojenským záměrům jiných států, jakož i snahu

---

[613] ZIOLKOWSKI, Katharina. *Confidence Building Measures for Cyberspace - Legal Implications* [online]. Tallinn: NATO CCD COE, 2013, str. 5. Dostupné: https://ccdcoe.org/uploads/2018/10/CBMs.pdf [Cit. 2022-11-12].

[614] Tamtéž.

[615] LEWIS, James Andrew. *Confidence-building and international agreement in cybersecurity* [online]. Disarmament forum, str. 52. Dostupné: https://citizenlab.ca/cybernorms2012/Lewis2011.pdf [Cit. 2022-11-12].

[616] ZIOLKOWSKI, Katharina. Op. cit., str. 8.

[617] Srov. shora popsané kybernetické útoky na estonské vládní webové stránky v roce 2007 či v rámci probíhajícího válečného konfliktu na Ukrajině.

[618] ZIOLKOWSKI, Katharina. Op. cit., str. 9.

zamezit vojenským střetům a přípravám na válečný konflikt, a snížení rizika překvapivých útoků a náhodného vypuknutí války.[619]

Na půdě OSN se od roku 2004 zabývá problematikou informační bezpečnosti uskupení vládních expertů (*Groups of Governmental Experts, GGE*). Výsledkem jejich činnosti jsou doporučení a zprávy přijaté Valným shromážděním OSN. Usnesením 70/237, jímž byla přijata zpráva GGE za rok 2015, vyzvalo Valné shromáždění členské státy, aby se při používání informačních a komunikačních technologií řídily právě zprávou GGE z roku 2015.[620] Mezi klíčová doporučení členským státům zpráva řadí dbát při využívání ICT obecných principů mezinárodního práva, zejména respektovat státní suverenitu, řešit spory mírovými prostředky a nezasahovat do vnitřních záležitostí jiných států. Existující mezinárodněprávní závazky jsou poplatné i pro ICT a státy jsou povinny je při využívání ICT dodržovat, stejně jako dbát ochrany lidských práv a základních svobod. Konkrétním a zásadním požadavkem Valného shromáždění je především zákaz *„zneužívat zástupčí metody k páchání protiprávních činů podle mezinárodního práva"* i povinnost zajistit, „*aby jejich území nebylo k páchání takových činů zneužíváno nestátními subjekty."*[621]

Příkladem bilaterálních opatření pro budování důvěry v kyberprostoru byly bilaterální dohody mezi Ruskou federací a USA z června 2013. Na jejich základě vznikl mimo jiné komunikační kanál a prostor pro sdílení informací mezi CERT týmy obou zemí i přímá komunikační linka mezi středisky pro snižování jaderného rizika v obou zemích; dále byla zřízena přímá zabezpečená hlasová linka mezi americkým a ruským orgánem pro kybernetickou bezpečnost.[622] V současné době však považuje USA aktivity vlády Ruské federace za hrozbu pro svou národní bezpečnost, zahraniční politiku a ekonomiku, neboť prezident Joe Biden vyhlásil v USA stav národní pohotovosti mimo jiné *„s ohledem na úsilí o narušení průběhu svobodných a spravedlivých demokratických voleb a demokratických institucí v USA a jejich spojencích a partnerech, zapojení se do škodlivých kybernetických aktivit proti USA i proti jejich spojencům a*

---

[619] UN GA. *Special Report of the Disarmament Commission to the General Assembly at its Third Special Session Devoted to Disarmament*, UN Doc A/S-15/3 (28 May 1988) 28-33 (endorsed by UNGA Res 43/78H, 7 December 1988). Citace dle ZIOLKOWSKI, Katharina. Op. cit., str. 13.

[620] UN OFFICE FOR DISARMAMENT AFFAIRS. *Developments in the field of information and telecommunications in the context of international security* [online]. Dostupné: https://www.un.org/disarmament/ict-security/ [Cit. 2022-11-12].

[621] UN OFFICE FOR DISARMAMENT AFFAIRS. *Fact Sheet: Developments in the Field of Information and Telecommunications in the Context of International Security* [online]. July 2019, str. 2. Dostupné: https://front.un-arm.org/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf [Cit. 2022-11-12]. Překlad autorka.

[622] ZIOLKOWSKI, Katharina. Op. cit., str. 22.

partnerům, včetně jejich usnadňování …".[623] V současné době se tudíž patrně obě země zmíněnými bilaterálními dohodami neřídí.

Můžeme se setkat i s jednostrannými prohlášeními, které mohou být podkladem opatření pro budování důvěry v kyberprostoru mezi dvěma i více státy, neboť informují o pozici dané země. Například Německo se vyslovilo pro přijetí opatření pro zvýšení transparentnosti a stability spočívající ve výměně informací o platném mezinárodním právu, organizačních strukturách, strategiích a doktrínách v kyberprostoru, a v podpoře krizových komunikačních kanálů, CERT a společných kybernetických cvičeních.[624]

Rovněž Evropská komise vyjádřila svůj postoj ke kyberprostoru, na nějž lze pohlížet jako na jednostranné prohlášení EU o přijatých politických pozicích ve vztahu ke kyberprostoru. Ve Strategii kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor[625] se uvádí, že základní hodnoty EU platí i v digitálním světě a stejné právní předpisy a normy, které se uplatňují v jiných oblastech každodenního života, považuje EU za platné i v kybernetické oblasti. Týká se to především základních práv a svobod a právních závazků zakotvených v Mezinárodním paktu o občanských a politických právech, Evropské úmluvě o lidských právech a Listině základních práv Evropské unie. Jakékoliv sdílení informací pro účely kybernetické bezpečnosti, jde-li o osobní údaje, by mělo být v souladu s právními předpisy EU o ochraně údajů a mělo by plně zohledňovat práva jednotlivců v této oblasti.

V rámci mezinárodní politiky týkající se kyberprostoru se EU vyslovila pro podporu spolupráce s mezinárodními organizacemi a dalšími partnery i se soukromým sektorem a občanskou společností. Klíčovou hodnotou má být otevřený a svobodný Internet, vysoká úroveň ochrany osobních údajů, bezpečný kyberprostor a boj proti kriminalitě. V otázkách mezinárodní bezpečnosti EU podporuje rozvoj opatření k budování důvěry v oblasti kybernetické bezpečnosti s cílem zvýšit transparentnost a snížit riziko chybné interpretace chování státu. Vytvoření nových mezinárodních právních nástrojů týkajících se kybernetiky nepovažuje za nutné. Obecným vzorem vnitrostátních právních předpisů o kyberkriminalitě a základem pro mezinárodní spolupráci se má stát budapešťská Úmluva o počítačové kriminalitě. Projeví-li se v kyberprostoru ozbrojený konflikt,

---

[623] THE WHITE HOUSE. *Notice on the Continuation Of The National Emergency With Respect To Specified Harmful Foreign Activities Of The Government Of The Russian Federation* [online]. April 13, 2022, Statements and Releases. Dostupné: https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/13/notice-on-the-continuation-of-the-national-emergency-with-respect-to-specified-harmful-foreign-activities-of-the-government-of-the-russian-federation/ [Cit. 2022-11-12]. Překlad autorka.

[624] ZIOLKOWSKI, Katharina. Op. cit., str. 23 - 24.

[625] EVROPSKÁ KOMISE. *Společné sdělení Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů. Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor /* JOIN/2013/01 final */* . Dokument 52013JC0001.

vyslovila se EU pro uplatnění mezinárodního humanitárního práva a právních předpisů z oblasti lidských práv.[626]

2.3.5.3. Tallinn Manual 2.0

Druhá verze Tallinnských manuálů obsahuje rozsáhlý soubor pravidel pojednávajících o kybernetických operacích a incidentech odehrávajících se na denní bázi. Z nich lze vybrat několik pravidel dotýkajících se narušení důvěrnosti, celistvosti či dostupnosti informací a dat. Následující text je založen na překladu uvedených pravidel Tallinn Manual 2.0 autorkou této práce. Podrobnější rozbor pravidel Tallinn Manual 2.0 obsahuje dále kapitola 2.4. disertační práce pojednávající o kybernetických operacích a mezinárodní odpovědnosti státu.

Podle Tallinn Manual 2.0 bude jakýkoli kybernetický útok narušující shora uvedenou triádu porušením principu suverenity státu ve smyslu pravidla č. 4, neboť stát nesmí provádět kybernetické operace porušující suverenitu jiného státu. Výjimkou je situace, kdy by takovou operaci schválila Rada bezpečnosti OSN nebo pokud by se jednalo o výkon práva státu na sebeobranu. Zákaz porušení suverenity zavazuje pouze státy, ne však nestátní aktéry, ledaže by jejich činy bylo možné přičíst některému státu. Činy nestátních aktérů, jež nelze přičíst žádnému státu, po právu však nejsou a budou postižitelné podle vnitrostátního práva napadeného státu.[627] Takový stát ovšem bude oprávněn v souladu s mezinárodním právem reagovat na kybernetický útok nestátních aktérů z titulu nezbytnosti či sebeobrany. Bude rovněž oprávněn uplatnit protiopatření vůči jinému státu pro nesplnění povinnost náležité péče spočívající v ponechání útoku nestátních aktérů působících z jeho území bez postihu.[628]

S narušením principu suverenity souvisí i problematika kybernetické špionáže (*cyberespionage*), jíž se věnuje pravidlo č. 32. Kybernetickou špionáž Tallinn Manual 2.0 definuje jako *„jakýkoli čin uskutečněný potají či pod falešnou záminkou, využívající kybernetické prostředky ke shromažďování informací nebo pokusu o něj."*[629] Zahrnuje zejména sledování, zachycení nebo vyzrazení elektronicky přenášených či uložených komunikací, dat a informací.[630] Vždy půjde především o narušení důvěrnosti informací. Pravidlo č. 32 stanoví, že státem prováděná

---

[626] Tamtéž, bod 2.5.

[627] Nepanuje však shoda na tom, zda může jednání organizované ozbrojené skupiny porušit suverenitu státu. Tallinn Manual 2.0., Rule 4 - Violation of sovereignty, bod 2.

[628] Tamtéž, bod 4.

[629] Tallinn Manual 2.0., Rule 32 - Peacetime cyber espionage, bod 2. Překlad autorka.

[630] Tamtéž.

kybernetická špionáž sice nepředstavuje v dobách míru sama o sobě porušení mezinárodního práva, avšak způsob, jakým je prováděna, jej porušit může. Ani mezinárodní obyčej špionáž jako takovou nezakazuje; to však neplatí, poruší-li suverenitu jiného státu nebo zákaz nevměšování se. Objevuje se však i názor, podle něhož je kyberšpionáž porušením základního principu mezinárodního práva - nevměšování se do vnitřních záležitostí státu, a proto je nutno považovat ji za odporující mezinárodnímu právu.[631]

Překvapivě není shody na tom, zda kybernetická špionáž prováděná orgány státu A za fyzické přítomnosti na území státu B naruší jeho suverenitu. Suverenita státu B ovšem jistě narušena bude, je-li kybernetická špionáž proti tomuto státu namířena.[632] Objevuje se i menšinový názor, podle něhož extenzivně prováděná nekonsensuální kybernetická špionáž státu za fyzické přítomnosti jeho orgánů na území sledovaného státu neporuší suverenitu sledovaného státu.[633] Názor se jeví zmatečný, neboť váže soulad s principem suverenity na rozsah prováděné kybernetické špionáže (čím větší rozsah, tím spíše bude v souladu) a nezohledňuje důvody, pro které může být špionáž prováděna v tak extenzivním rozsahu. Shoda však panuje na tom, že pouhý odposlech bezdrátových signálů, je-li prováděn mimo území sledovaného státu, se nedotkne jeho suverenity, neboť se neprojeví v jeho kybernetické infrastruktuře.[634] Uvedený názor však nezohledňuje skutečnost, že dojde k narušení důvěrnosti informací a dat právě v kybernetické infrastruktuře cílového státu.

Důvěrnost, integritu a dostupnost informací a dat chrání rovněž ustanovení diplomatického a konzulárního práva, o němž pojednává 7. část Tallinn Manual 2.0. Stěžejním principem je nedotknutelnost prostor, v nichž se nachází kybernetická infrastruktura.[635] Majetek v prostorách diplomatické mise nesmí být podroben prohlídce, ani být zabaven či zajištěn orgány přijímajícího státu bez souhlasu státu vysílajícího misi. Rovněž archivy, dokumenty a úřední korespondence diplomatické mise či konzulárního úřadu v elektronické podobě jsou nedotknutelné; nepodléhají tak zajištění, soudnímu rozhodnutí ani jiné formě státního zásahu, včetně kybernetické špionáže.[636] S

---

[631] BUCHAN, Russell. Cyber Espionage and International Law. In: TSAGOURIAS, Nicholas, BUCHAN, Russell. *Research Handbook on International Law and Cyberspace*. Edward Elgar, 2015, str. 168 - 189.

[632] Ledaže by měl stát pro kybernetickou špionáž určitý právem přiznaný důvod. Tallinn Manual 2.0., Rule 4 - Violation of sovereignty, bod 7.

[633] Tamtéž, bod 8. Pro případ chybného překladu do českého jazyka autorka textu konzultovala znění bodu 8 s vyučujícím anglického jazyka, avšak se shodným výsledkem.

[634] Tamtéž, bod 9.

[635] Pravidlo č. 39 Tallinn Manual 2.0 uvádí, že je kybernetická infrastruktura v prostorách diplomatické mise či konzulárního úřadu chráněna nedotknutelností této mise, resp. konzulárního úřadu.

[636] Tallinn Manual 2.0., Rule 41, bod 1.

tím souvisí i požadavek, aby přijímající stát učinil všechna vhodná opatření k ochraně kybernetické infrastruktury v prostorách diplomatické mise vysílajícího státu před jejím poškozením či vniknutím do uvedených prostor.[637] Netřeba však zajištění bezmezné ochrany. Přijatá opatření mají být vhodná, tj. přiměřená vůči konkrétním známým hrozbám a možnostem přijímajícího státu.[638] K důvěrnosti, ale i celistvosti a dostupnosti informací a dat se váže požadavek zajistit a chránit svobodnou kybernetickou komunikaci diplomatické mise či konzulárního úřadu pro všechny úřední účely. Přijímající stát tak nesmí např. zasahovat do e-mailové komunikace mezi konzulátem a státními orgány vysílajícího státu týkající se konzulárních záležitostí ani omezit dostupnost webové stránky diplomatické mise či internetového připojení mise.[639]

Vhodnějším a pro praxi srozumitelnějším vodítkem posuzování souladu kybernetických operací s principem suverenity se jeví přístup založený na zohlednění míry narušení územní celistvosti státu či rozsahu, v němž jsou zasaženy pravomoci státu. K porušení principu suverenity totiž dochází zejména při zasažení dat či služeb nezbytných pro výkon státní správy. Typickým případem je uvedena modifikace či potlačení dat potřebných pro fungování sociálních služeb, provádění voleb, sběr daní, či zajištění bezpečnosti státu. Není přitom rozhodné, zda jde o přímý nebo přenesený výkon státní správy. Rozhodující je, zasáhne-li útok do výkonu správních činností.[640] Pouhý útok na správní úřad (instituci), který by se však neprojevil v jeho správní činnosti (např. při výplatě sociálních dávek), by tak měl patrně být posouzen pouze jako případ počítačové trestné činnosti, ne však ve smyslu porušení principu suverenity, tj. jako akt v rozporu s mezinárodním právem.

Kybernetické činy nestátních aktérů (typicky jednotlivců, hackerských uskupení, obchodních společností atp.) upravuje mezinárodní právo pouze v omezeném rozsahu.[641] Tyto činy, nejsou-li přičitatelné státům, nemohou narušit ani suverenitu dotčeného státu, porušit princip nevměšování se, a nejsou ani nedovoleným použitím síly. Napadený stát se proto nemůže v reakci uchýlit k protiopatřením; možnost jednat v nutné obraně či z nezbytnosti jsou mu však

---

[637] Tallinn Manual 2.0, Rule 40.

[638] Tamtéž, bod 2.

[639] Tallinn Manual 2.0, Rule 42, body 1 - 2. Pravidlo č. 43 však stanoví související omezení: Prostory diplomatické mise či konzulárního úřadu nesmí být využity ke kybernetickým činnostem, jež jsou neslučitelné s diplomatickými či konzulárními úkoly. Diplomaté ani úředníci se rovněž nesmí podílet na kybernetických aktivitách zasahujících do vnitřních záležitostí přijímajícího státu nebo které porušují právní řád tohoto státu.

[640] Podrobněji Tallinn Manual 2.0., Rule 4 - Violation of sovereignty, body 10 - 17.

[641] Tallinn Manual 2.0, Rule 33 - Non-State actors.

zachovány.[642] Možné reakce na kybernetické útoky nestátních aktérů však bývají běžně upraveny ve vnitrostátních právních řádech, nejčastěji v rámci správního či trestního práva s ohledem na deliktní povahu útoků. Pokud se nestátní aktéři zapojí kybernetickými útoky do ozbrojeného či válečného konfliktu, podléhají jejich činy právu ozbrojeného konfliktu; vyloučena není ani odpovědnost podle mezinárodního práva trestního.[643]

Narušení bezpečnosti informací a dat se dotýkají i ustanovení o odpovědnosti států za protiprávní (kybernetické) činy z hlediska mezinárodního práva dle 4. části Tallinn Manual 2.0. Pojednáno bude o tom níže v kapitole 2.4. této práce.

Zmínit lze rovněž ustanovení v 11. části Tallinn Manual 2.0 o ochraně mezinárodních telekomunikačních infrastruktur. Zřídí-li stát kybernetickou infrastrukturu s cílem zajistit rychlou a nepřerušovanou mezinárodní telekomunikaci, pak ji musí i udržovat a chránit. S ohledem na pravomoc vykonávat kontrolu nad kybernetickou infrastrukturou nacházející se na státním území (projev principu suverenity státu) je však stát oprávněn pozastavit služby mezinárodní kybernetické komunikace (Internet) na svém území, či zcela zastavit přenos soukromé kybernetické komunikace, jestliže je tato v rozporu s vnitrostátním právním řádem, veřejným pořádkem, morálkou nebo představuje-li nebezpečí pro bezpečnost státu.[644] Příkladem pozastavení služeb mezinárodní kybernetické komunikace (dalo by se říci služeb informační společnosti), bylo rozhodnutí egyptské vlády zablokovat Internet a mobilní telefonické spojení po několik dní roku 2011 v souvislosti s občanskými nepokoji (protestující využívali komunikační platformy typu Twitter, Facebook aj.). Ačkoli Egypt nesplnil požadavek oznámit blokaci ostatním státům předem, pozastavení služeb bylo v souladu s mezinárodním právem.[645] Uvedené pravidlo se zdá spíše méně významným doplňkem principu suverenity, když zdůvodnění blokace mezinárodního internetového spojení je zcela na úvaze daného státu.

[642] Tamtéž, body 2 - 3.

[643] Tamtéž, bod 6 - 7.

[644] Tallinn Manual 2.0 Rule 62.

[645] Tamtéž, bod 4.

2.3.5.4. Směrnice EU o bezpečnosti sítí a informačních systémů[646]

Směrnice NIS přispívá k bezpečnosti informací a dat zejména stanovením požadavků organizačního charakteru, jež mají zajistit v členských státech EU řádné fungování bezpečnostních týmů typu CSIRT, čímž posílí bezpečnost kybernetického prostředí EU.

Úkolem týmů CSIRT má být předně monitorování incidentů na vnitrostátní úrovni, vydávání včasných varování a upozornění, informování o rizicích a incidentech dotčeným osobám, jakož i reakce na bezpečnostní incidenty a jejich analýza.[647] Bezpečnost informačních a komunikačních sítí a systémů má být zajištěna v klíčových hospodářských odvětvích. Směrnice NIS ukládá členským státům zřídit bezpečnostní týmy CSIRT, které budou pokrývat odvětví energetiky (elektřina, ropa, zemní plyn), dopravy (letecká, železniční, vodní a silniční doprava), bankovnictví i infrastrukturu finančních trhů. Jejich působení se má vztahovat i na klíčová odvětví zajišťující lidské zdraví - sektory zdravotnictví (pokryta mají být všechna zdravotnická zařízení bez ohledu na to, zda je zřizovatelem soukromá osoba) a dodávek a rozvodů pitné vody určené k lidské spotřebě. Zabezpečeno má být též odvětví digitální infrastruktury a služby on-line tržiště, internetového vyhledávání a cloud computingu.[648] Za účelem vzájemné rychlé a účinné spolupráce došlo k zřízení sítě vnitrostátních CSIRT,[649] která má zejména usnadnit výměnu informací či k žádosti zástupce týmu CSIRT určit koordinovanou reakci na kybernetický bezpečnostní incident.[650]

Směrnice NIS rovněž stanovila členským státům požadavek zajistit u provozovatelů základních služeb[651] přijetí opatření k předcházení incidentům ovlivňujícím bezpečnost sítí a informačních systémů a neprodlené hlášení nastalých incidentů se závažným dopadem na kontinuitu základních služeb.[652] Obdobný požadavek platí i ve vztahu k poskytovatelům digitálních

---

[646] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (v práci též jako „směrnice NIS").

[647] Podrobněji srov. úkoly a požadavky na bezpečnostní týmy typu CSIRT uvedené v Příloze I, bod 2, písm. a) směrnice NIS.

[648] Srov. čl. 9 odst. 1 ve spojení s Přílohami II a III směrnice NIS.

[649] Srov. čl. 12 směrnice NIS.

[650] Srov. jednotlivé úkoly sítě CSIRT ve smyslu čl. 12, odst. 3 směrnice NIS.

[651] Podle čl. 4 odst. 4 směrnice NIS je provozovatelem základní služby veřejný nebo soukromý subjekt, jehož druh je uveden v příloze II a který splňuje kumulativní kritéria stanovená v čl. 5 odst. 2: poskytuje službu, která je základní z hlediska zachování kritických společenských nebo ekonomických činností, poskytování dotyčné služby je závislé na sítích a informačních systémech, a incident by vedl k významnému narušení poskytování této služby.

[652] Srov. čl. 14 odst. 2, 3 směrnice NIS. Podle odst. 5 téhož ustanovení informuje na základě informací od provozovatele základních služeb příslušný orgán nebo tým CSIRT i další dotčený členský stát, má-li incident významný dopad na kontinuitu základních služeb i v tomto státě.

služeb.[653] Ostatní subjekty mohou hlásit incidenty se závažným dopadem na kontinuitu služeb, které poskytují, dobrovolně.[654]

V budoucnu má dojít k rozšíření okruhu povinných subjektů novou směrnicí EU o bezpečnosti sítí a informačních systémů. Získala si pracovní název směrnice NIS2. Přijetí konečného znění směrnice NIS2 se předpokládá na konci roku 2022, přičemž členské státy by měly provést změny v legislativě v průběhu roku 2024. Kromě rozšíření regulovaných odvětví (např. o odpadové hospodářství) i regulovaných služeb (např. nově regulované služby cloud computingu) a změn v identifikaci povinných osob (hledisko minimálního počtu zaměstnanců či minimálního ročního obratu či bilanční sumy roční rozvahy), má směrnice NIS2 rozlišovat mezi povinnými subjekty: subjekty v režimu „essential" budou mít uloženy přísnější povinnosti než ty spadající do režimu „important".[655]

2.3.5.5. Zákon o kybernetické bezpečnosti a vyhláška o kybernetické bezpečnosti

ZKB zvyšuje kybernetickou bezpečnost tím, že vybraným orgánům a osobám ukládá povinnost zavést a provádět nezbytná bezpečnostní opatření pro zajištění kybernetické bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury, informačního systému základní služby, významného informačního systému a sítí elektronických komunikací a informačních systémů využívaných v souvislosti se zajišťováním digitálních služeb.[656] Bezpečnostní požadavky musí být zohledněny i při výběru dodavatelů informačních a komunikačních systémů. Tato restrikce výběru je sice omezením hospodářské soutěže, děje se však v souladu se zákonem, respektive ZKB výslovně uvádí, že dané omezení je odůvodněnou překážkou hospodářské soutěže.[657]

Bezpečnostními opatřeními jsou organizační a technická opatření stanovená v § 5 odst. 2 a 3 ZKB. Ustanovením § 6 písm. a), ve spojení s § 28 odst. 2 písm. a) ZKB zákonodárce zmocnil příslušný správní orgán (původně jím byl Národní bezpečnostní úřad, nyní je to NÚKIB) ke specifikaci obsahu a rozsahu bezpečnostních opatření, s ohledem na zajištění jejich dostatečné flexibility vzhledem k budoucímu technologickému vývoji. Důvodová zpráva k tomu uvádí, že

---

[653] Srov. čl. 16 odst. 1 až 3 směrnice NIS.

[654] Přitom se výslovně stanoví, že na základě dobrovolného ohlášení nesmí být oznamujícímu subjektu uložena žádná povinnost, která by mu nebyla uložena, kdyby toto ohlášení neučinil. Srov. čl. 20 směrnice NIS.

[655] NÚKIB. *NÚKIB představuje evropskou směrnici NIS2*. Op. cit.

[656] Srov. § 4 odst. 1 až 3 ZKB.

[657] Srov. § 4 odst. 4 ZKB.

podobu bezpečnostních opatření nebylo možné ponechat z důvodu právní jistoty na povinných orgánech a osobách.[658]

Vyhláška o kybernetické bezpečnosti stanoví konkrétní opatření, která mají přispět k zajištění důvěrnosti, celistvosti a dostupnosti informací a služeb. Zajištěním dostupnosti se věnuje např. § 15 této vyhlášky, který specifikuje povinnosti v rámci řízení kontinuity činností. Charakterem jde o organizační opatření, jejichž cílem je bránit přerušení činnosti povinné osoby a umožnit rychlou reakci na nastalou krizi, jež by ochránila organizaci před závažnými následky lidských chyb či katastrof. Jde o vytvoření určitého systému managerského řízení krizových stavů.[659] Podrobněji konkrétní kroky v rámci prevence a reakce na krizové události rozebírají Smejkal, Sokol a Kodl.[660] K zajištění důvěrnosti i celistvosti informací přispívají technická opatření, jako např. kryptografie a aktivní blokace nežádoucí komunikace,[661] či povinnosti v rámci správy a ověřování identit.[662] Vyhláška uvádí i zařízení a jejich prvky, u nichž je nutné použít nástroj nepřetržité ochrany před malware,[663] či povinnosti při zajišťování dostupnosti informací.[664]

Významnou povinností, kterou ukládá ZKB, je nutnost hlásit kybernetické bezpečnostní incidenty bezodkladně po jejich zjištění a vyhodnocení události jako kybernetického bezpečnostního incidentu.[665] Smyslem je umožnit vládnímu i národnímu CERT, jimž jsou incidenty hlášeny, reagovat na nastalou bezpečnostní situaci a koordinovat ochranu kritické informační infrastruktury, významných informačních systémů a významných sítí. NÚKIB (resp. původně NBÚ) byl zákonem zmocněn[666] i k definování konkrétních parametrů kybernetických bezpečnostních incidentů a způsobu jejich nahlašování. Vyhláška o kybernetické bezpečnosti proto uvádí podmínky: kybernetické bezpečnostní incidenty mají být hodnoceny nejen podle důležitosti

---

[658] Důvodová zpráva k ZKB. Op. cit., § 6.

[659] SMEJKAL, Vladimír, SOKOL, Tomáš, KODL, Jindřich. Op. cit., str. 148.

[660] Tamtéž, str. 149 - 160.

[661] Srov. § 18 písm. c), d), § 26 vyhlášky o kybernetické bezpečnosti.

[662] Srov. § 19 vyhlášky o kybernetické bezpečnosti.

[663] Srov. § 21 odst. 1 písm. a) vyhlášky o kybernetické bezpečnosti.

[664] Srov. § 27 vyhlášky o kybernetické bezpečnosti. Podrobněji SMEJKAL, Vladimír, SOKOL, Tomáš, KODL, Jindřich. Op. cit., str. 190 an.

[665] Povinnost se týká orgánů a osob zajišťujících významnou síť, jakož i správců a provozovatelů informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury, významného informačního systému a informačního systému základní služby. Srov. § 8 odst. 1 ve spojení s § 3 písm. b) až f) ZKB. Povinnost hlásit kybernetický bezpečnostní incident s významným dopadem na poskytování jeho služeb má i poskytovatel digitální služby, jestliže disponuje informacemi pro posouzení významu tohoto dopadu. Srov. § 8 odst. 2 ZKB.

[666] § 28 odst. 2 písm. b) ZKB.

chráněných informací a služeb co do složek důvěrnosti, celistvosti (integrity) a dostupnosti. Jednotlivé kategorie incidentů (I - III.) zohledňují počet dotčených uživatelů, rozsah vzniklé či předpokládané škody, dopady na služby poskytované jinými informačními a komunikačními systémy, jakož i délku trvání incidentů či zeměpisný rozsah dotčené oblasti.[667] Samotná triáda CIA slouží též ke kategorizaci kybernetických bezpečnostních incidentů.[668]

Plnění zákonných povinností u vybraných orgánů a osob, jakož i dodržování prováděcích právních předpisů v oblasti kybernetické bezpečnosti, sledují zaměstnanci NÚKIB v rámci výkonu kontroly.[669]

ZKB dále upravuje opatření, která provádí NÚKIB k ochraně informačních systémů nebo služeb a sítí elektronických komunikací před hrozbami v oblasti kybernetické bezpečnosti, jakož i ta, jimiž řeší existující kybernetické bezpečnostní incidenty. Jde o varování, reaktivní opatření a ochranná opatření.[670] Podrobněji jsou opatření rozebrána v 3. části této práce.

ZKB rovněž upravuje tzv. stav kybernetického nebezpečí, který definuje jako „*stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost služeb elektronických komunikací anebo bezpečnost a integrita sítí elektronických komunikací, a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací.*"[671] Důvodová zpráva poukazuje na nutnost řešit natolik masivní *„ohrožení nebo narušení kybernetické bezpečnosti, že v jeho důsledku mohou být ohroženy nebo dokonce poškozeny fundamentální národní zájmy."*[672] Pokud nebudou stačit běžné mechanismy upravené v ZKB, může ředitel NÚKIB vyhlásit stav kybernetického nebezpečí na maximální dobu 7 dní, kdy je NÚKIB oprávněn vydat rozhodnutí nebo opatření obecné povahy ve smyslu § 13 ZKB, která budou určena i dalším orgánům a osobám.[673] Při vyhlášení stavu kybernetického nebezpečí je tudíž třeba respektovat princip subsidiarity - nelze jej vyhlásit, lze-li nebezpečí odvrátit jinak, tedy typicky opatřeními na ochranu informačních systémů nebo služeb a sítí elektronických komunikací. Z hlediska činnosti NÚKIB upravené v ZKB lze vyhlášení stavu

---

667 Srov. § 31 odst. 1 vyhlášky o kybernetické bezpečnosti.

668 § 31 odst. 3 vyhlášky o kybernetické bezpečnosti.

669 Kontrolu, nápravná opatření a přestupky v oblasti kybernetické bezpečnosti upravuje Hlava V ZKB.

670 § 11 odst. 2 ZKB.

671 § 21 odst. 1 ZKB.

672 Důvodová zpráva k ZKB. Op. cit. § 21.

673 § 21 odst. 4 a 5 ZKB.

kybernetického nebezpečí chápat jako prostředek *ultima ratio*. Dále již přichází na řadu vyhlášení nouzového stavu vládou podle ústavního zákona o bezpečnosti ČR.[674]

Jak uvádí Důvodová zpráva k ZKB, stav kybernetického nebezpečí se nemá dotknout uživatelů informačních systémů, sítí a služeb elektronických komunikací - jeho vyhlášením dojde jen k rozšíření okruhu orgánů a osob, které budou povinny provádět reaktivní opatření vydaná NÚKIB; stav kybernetického nebezpečí proto také není upraven v zákoně č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „krizový zákon"), neboť práv a povinností občanů ČR se nedotýká.[675]

Je nicméně otázkou, zda mezi stavem kybernetického nebezpečí a nouzovým stavem nestojí ještě stav nebezpečí ve smyslu § 3 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (dále jen „krizový zákon"). Podle něj se stav nebezpečí může vyhlásit jako bezodkladné opatření, *„jsou-li ohroženy životy, zdraví, majetek, životní prostředí, pokud nedosahuje intenzita ohrožení značného rozsahu, a není možné odvrátit ohrožení běžnou činností správních úřadů, orgánů krajů a obcí, složek integrovaného záchranného systému nebo subjektů kritické infrastruktury."* Lze si představit, že v důsledku kybernetického bezpečnostního incidentu, který postihne např. velkou krajskou nemocnici či jadernou elektrárnu, budou ohroženy životy, zdraví a majetek, intenzita ohrožení však nebude vyhodnocena co do značného rozsahu tak, aby odůvodnila nouzový stav ve smyslu čl. 5 ústavního zákona o bezpečnosti ČR, současně však činnost NÚKIB ve stavu kybernetického nebezpečí nepostačí k odvrácení ohrožení. V takovém případě by bylo jistě na místě vyhlásit stav nebezpečí podle krizového zákona.

2.3.5.6. Standardy a normy

Otázky důvěrnosti, integrity a dostupnosti informací v organizacích řeší i standardy a normy. Zmínit lze např. mezinárodní standard ISO 27001, který specifikuje nejlepší praxi pro zavádění systému řízení bezpečnosti informací, či mezinárodní standard ISO 27002 stanovící soubor postupů pro opatření bezpečnosti informací a kodex chování.[676]

---

[674] Podle § 21 odst. 6 ZKB *„[n]ení-li možné odvrátit ohrožení bezpečnosti informací v informačních systémech nebo bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v rámci stavu kybernetického nebezpečí, ředitel Úřadu neprodleně požádá vládu o vyhlášení nouzového stavu. Rozhodnutí a opatření obecné povahy vydaná Úřadem podle § 13 před vyhlášením nouzového stavu zůstávají v platnosti, pokud tato opatření nejsou v rozporu s krizovými opatřeními vyhlášenými vládou."*

[675] Důvodová zpráva k ZKB. Op. cit., § 21.

[676] Podrobněji SMEJKAL, Vladimír, SOKOL, Tomáš, KODL, Jindřich. Op. cit., str. 282 - 283.

Standardy a normy lze v česky psaných dokumentech považovat za synonyma.[677] Technickými požadavky, technickými normami a státním zkušebnictvím se zabývá zákon č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o technických požadavcích"). Soustavu českých technických norem tvoří původní české technické normy, jakož i evropské a mezinárodní normy přejaté překladem, přejaté v původním jazyce, anebo přejaté schválením k přímému používání.[678] Slovy zákona jde o *„dokument schválený Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví (dále jen „Úřad") pro opakované nebo stálé použití vytvořený podle tohoto zákona a označený písmenným označením ČSN, jehož vydání bylo oznámeno ve Věstníku Úřadu."*[679]

České technické normy nejsou obecně závazné.[680] Zákon ovšem může stanovit povinnost řídit se určitou technickou normou. Pokud by pak z důvodu jejího porušení, tj. porušení zákonné povinnosti, vznikla škoda, a zároveň by byly dovozeny i další podmínky stanovené v § 2910 občanského zákoníku, bylo by takové porušení technické normy důvodem ke vzniku povinnosti škůdce nahradit vzniklou škodu. Vedle soukromoprávní odpovědnosti nelze vyloučit ani vznik trestní odpovědnost či odpovědnosti za spáchání přestupku, bude-li naplněna skutková podstata, jejímž znakem by bylo porušení české technické normy.[681]

K závaznosti českých technických norem se vyjádřil i Nejvyšší správní soud v rozsudku ze dne 22. 12. 2004, č. j. 4 As 31/2003-111, publikovaným pod č. 549/2005 Sb. NSS, v němž ve vztahu k činnosti správního orgánu soud zdůraznil, že postup v rozporu s českou technickou normou vypracovanou podle zákona o technických požadavcích lze označit za nezákonný pouze tehdy, pokud by pro daný případ byla závaznost technické normy stanovena právním předpisem. Závazný charakter přitom mohou mít české technické normy i v soukromoprávních vztazích.[682]

---

[677] Tamtéž, str. 237.

[678] § 4 odst. 2 zákona o technických požadavcích.

[679] § 4 odst. 1 zákona o technických požadavcích.

[680] Tamtéž.

[681] Jde o tzv. blanketní dispozici, jež odkazuje obecně na normu nebo více norem téhož druhu, často na prováděcí právní předpisy či předpisy určitého právního odvětví. Srov. JELÍNEK, Jiří, DANKOVÁ, Katarína, TLAPÁK NAVRÁTILOVÁ, Jana, PELC, Vladimír, ŘÍHA, Jiří, STEJSKAL, Vojtěch. Op. cit., str. 47.

[682] K závaznosti české technické normy ve vztahu k řádnému provedení díla srov. např. rozsudek Nejvyššího soudu ze dne 29. 4. 2020, sp. zn. 23 Cdo 3071/2019.

2.4. Kybernetické operace a mezinárodní odpovědnost státu

2.4.1. Nestátní aktéři jako původci kybernetických operací

Kyberprostor vnímá řada států jako pátou doménu možného válečného konfliktu, neboť rozeznávají nebezpečné vlastnosti nástrojů, jimiž lze v kyberprostoru zaútočit.[683] I v kyberprostoru jsou však státy povinny respektovat mezinárodní právní řád, a to jak během ozbrojeného konfliktu, tak v době míru. Následující text vychází především z mého překladu pravidel uvedených v druhé verzi Tallinnského manuálu, který v práci označuji ve zkratce jako Tallinn Manual 2.0 (viz shora).[684] Text se ozbrojenému konfliktu nevěnuje - v tomto ohledu lze odkázat zejména na první z Tallinnských manuálů,[685] na čtvrtou část Tallinn Manual 2.0[686] i na odbornou literaturu.[687]

V kyberprostoru nepůsobí jen státy. Původci i oběťmi kybernetických útoků mohou být vedle států i soukromé subjekty, jejichž působení mohou státy na svém území z různých důvodů tolerovat. Může jít o pachatele trestných činů, o teroristy, o obchodní společnosti praktikující kyberšpionáž s cílem získat konkurenční výhody, anebo o jednotlivce bez shora nastíněné zvláštní motivace. Ačkoli mezinárodní právo nepřiznává nestátním aktérům výsostné postavení, jaké mají státy, kyberprostor stírá rozdíly mezi státem a jednotlivci. V oblasti kybernetické bezpečnosti může dokonce řada nestátních aktérů přesahovat kapacity mnoha států.[688] Úloha nestátních aktérů v kyberprostoru bude patrně i nadále významná, a to jednak z důvodu jejich angažovanosti v kybernetické kriminalitě a kyberútocích, jednak díky konceptu Internetu věcí a hodnotě dat, kterou je řada států i nestátních aktérů odhodlána bránit i využívat.[689]

---

[683] ZIOLKOWSKI, Katharina. Op. cit., str. 5.

[684] SCHMITT, Michael. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* [online]. 2. vydání. Cambridge: Cambridge University Press, 2017. Dostupné: https://www.cambridge.org/core/books/abs/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/law-of-international-responsibility/99E333F8578ADCC567A92BECF932E4C3 [Cit. 2022-11-04].

[685] SCHMITT, Michael N. *Tallinn manual on the international law applicable to cyber warfare: prepared by the international group of experts at the invitation of the NATO cooperative cyber defence centre of excellence*. Cambridge: Cambridge University Press, 2013.

[686] Tallinn Manual 2.0, Part IV. The law of cyber armed conflict.

[687] Např. WOLTAG, Johann-Christoph. Computer Network Operations During an International Armed Conflict. In: *Cyber Warfare: Military Cross-Border Computer Network Operations under International Law.* Intersentia, 2014, str. 197-258. Nebo SOLIS, Gary D. *The Law of Armed Conflict: International Humanitarian Law in War.* 3. vydání. Cambridge: Cambridge University Press, 2021, str. 532-561.

[688] BANNELIER, Karine, CHRISTAKIS, Theodore. Cyberattaques - Prévention-Réactions : Rôles des Etats et des acteurs privés [online]. *Les Cahiers de la Revue Défense Nationale*, Paris, 2017, str. 10. Dostupné: https://ssrn.com/abstract=2957795 [Cit. 2022-11-14].

[689] Tamtéž, str. 11.

Právní normy upravující kybernetické operace nestátních aktérů jsou v kompetenci jednotlivých států. Jednání nestátních aktérů bude vždy předmětem výkonu jurisdikce některého ze států.[690] Vznikají mezinárodní úmluvy s cílem potírat nebezpečné kybernetické útoky a trestnou činnost, jež ovlivňuje území více států. Příkladem je již několikrát zmiňovaná Úmluva o počítačové kriminalitě.

Státy mají z hlediska mezinárodního práva povinnost neumožnit zneužití svého území k páchání protiprávních činů vůči ostatním státům.[691] Zmíněná povinnost se vztahuje i na kybernetickou infrastrukturu a počítačová zařízení nacházející se na státním území. Stát je povinen dbát náležité opatrnosti (náležité péče),[692] jež spočívá právě v tom, že *„vědomě nedovolí zneužití svého státního území či území a kybernetické infrastruktury nacházející se pod státní kontrolou, k provedení kybernetických operací, jež by ovlivnily práva jiných států a měly by pro ně vážné nepříznivé důsledky"*.[693] Způsob, jakým zabrání škodlivým kybernetickým operacím, je na volbě konkrétního státu.[694] Princip náležité péče má zásadní vliv na situace, kdy jsou původcem kybernetických útoků nestátní aktéři a jejich činy není možné přičíst některému státu.

2.4.1.1. Princip náležité péče (*due diligence*)

Princip náležité péče či náležité opatrnosti, vyjádřený v pravidle č. 6 Tallinn Manual 2.0, bývá rovněž chápán jako požadavek bdělosti či prevence. Požaduje se, aby *„stát přijal veškerá opatření, která jsou za daných okolností proveditelná, s cílem ukončit kybernetickou operaci (útok), jenž ovlivňuje práva jiných států a má pro ně závažné nepříznivé důsledky"*.[695]

Pokud si je stát vědom, že jeho území či infrastruktury pod jeho kontrolou jsou zneužívány k páchání kybernetických útoků proti jiným státům, musí dotčené státy neprodleně informovat. Rovněž je povinen zahájit vyšetřování s cílem zjistit původce útoků a postihnout je za ně.[696]

Součástí principu náležité péče však není povinnost podniknout konkrétní preventivní kroky k zajištění, aby nedošlo k využití státního území ke kybernetickým útokům namířeným na jiné státy

---

[690] Tallinn Manual 2.0, Rule 33 - Non-State actors.

[691] BANNELIER, Karine, CHRISTAKIS, Theodore. Op. cit., str. 12.

[692] Tallinn Manual 2.0 uvádí pojem *due diligence*, tj. doslova náležitá bdělost, opatrnost. Překlad autorka.

[693] Tallinn Manual 2.0, Rule 6 - Due diligence (general principle). Překlad autorka.

[694] Tallinn Manual 2.0, Rule 7 - Compliance with the due diligence principle, bod 6.

[695] Tallinn Manual 2.0, Rule 7 - Compliance with the due diligence principle. Překlad autorka.

[696] BANNELIER, Karine, CHRISTAKIS, Theodore. Op. cit., str. 29. Dále srov. též rozsudek Mezinárodního soudního dvora ze dne 9. 4. 1949, *Corfu Channel Case* (United Kingdom of Great Britain and Northern Ireland v. Albania). Dostupný: http://www.icj-cij.org/en/case/1/judgments [Cit. 2022-11-02].

- do této míry není princip náležité péče alespoň dosud mezinárodním společenstvím vnímán.[697] Rovněž nejsou státy oprávněny použít princip náležité péče jako záminku k uplatnění nástrojů hromadného sledování a narušování základních práv a svobod, zejména práva na soukromí. Státy jsou oprávněny používat technologie jen v mezích toho, co umožňuje mezinárodní právo, a především s respektem k ochraně základních lidských práv a svobod.[698]

Tallinn Manual 2.0 uvádí příklad, kdy se princip náležité péče uplatní. Bude jím situace, v níž uskupení hackerů pocházející ze státu A zaútočí na stát B a způsobí mu tím škodu (materiální ujmu), přičemž k útoku využije kybernetickou infrastrukturu nacházející se na území státu C. Musí se ovšem současně jednat o kybernetický čin v rozporu s mezinárodním právem. Ve vztahu ke kyberšpionáži se proto princip náležité opatrnosti neuplatní, neboť kyberšpionáž sama o sobě není zakázána mezinárodním právem (srov. Pravidlo 32 Tallinn Manual 2.0), ledaže by mezinárodní smlouva stanovila jinak. Jestliže orgány státu C budou mít povědomí o kybernetickém útoku, jsou na základě principu opatrnosti povinny proti útoku zakročit. Konkrétní opatření, kterými by stát C měl zamezit kybernetickému útoku, nebudou bezbřehá; v dané situaci lze požadovat pouze proveditelná (dosažitelná) opatření. Obdobný požadavek bude platit i v případě anektovaného území, či u vládní kybernetické infrastruktury nacházející se mimo území státu. Rovněž v případě státu, jehož územím data pouze procházejí (např. skrze optický kabel), se princip náležité opatrnosti uplatní, avšak pouze za předpokladu, že si transitní stát bude vědom škodlivého přenosu dat skrze vlastní infrastrukturu. Povědomí o škodlivém přenosu nicméně bude spíše výjimečným, neboť většina datového provozu prochází soukromou infrastrukturou poskytovatelů internetového připojení.[699]

Povědomí o kybernetickém útoku lze dovodit ze skutečnosti, že státní orgány, zpravodajské služby apod., zaznamenají kybernetický útok vedený ze státního území nebo obdrží důvěryhodnou informaci o takovém útoku. Povědomí lze rovněž dovodit za situace, kdy stát sice neví, že z jeho území je prováděn kybernetický útok vůči jinému státu, avšak na základě objektivních skutečností o takovém útoku měl a mohl vědět; to platí zejména tehdy, je-li k útoku zneužita státní infrastruktura, anebo je-li útočeno skrze veřejně známé zranitelnosti či malware.[700]

---

[697] Tallinn Manual 2.0, Rule 6 - Due diligence (general principle), bod 5.

[698] BANNELIER, Karine, CHRISTAKIS, Theodore. Op. cit., str. 23.

[699] Tallinn Manual 2.0, Rule 6 - Due diligence (general principle), body 8 - 10 a 14.

[700] Tamtéž, body 37 - 40.

Ačkoli mezinárodní právo dopadá na kybernetické operace nestátních aktérů jen v omezené míře,[701] za určitých podmínek lze považovat činy nestátních aktérů za činy konkrétního státu, které založí jeho mezinárodněprávní odpovědnost. Tato situace nastane, pokud fyzické či právnické osoby budou jednat na základě příkazů či pokynů konkrétního státu nebo pod jeho kontrolou. Rovněž přihlásí-li se stát k danému činu, tj. prohlásí-li jej za vlastní, založí tím svoji mezinárodněprávní odpovědnost.[702] Více o mechanismu přičitatelnosti pojednává následující podkapitola.

Nelze-li kybernetický útok nestátních aktérů považovat za čin konkrétního státu, nebude čin představovat ani intervenci nebo nedovolené použití síly, neboť těch se může dopustit jedině stát. Obvykle takový čin nenaruší ani suverenitu státu, proti němuž je namířen.[703] Dotčený stát se tudíž nemůže uchýlit k protiopatřením ve smyslu mezinárodního práva. Může však postupovat proti útočníkovi v souladu s vnitrostátním právem a zakročit na obranu hodnot, jež chrání jeho právní řád. Za určitých podmínek může napadený stát jednat rovněž na základě práva na sebeobranu[704] a krajní nouze.[705]

Mezinárodní právo však předpokládá reakci na kybernetický útok nestátních aktérů, který nelze přičíst některému státu, pokud stát nedostojí povinnosti náležité péče a nezabrání závažným nepříznivým důsledkům na území jiného státu, které způsobí kybernetický útok nestátních aktérů provedený z jeho území. Zmíněnou reakcí jsou protiopatření (*countermeasures*). Za situace, v níž lze kybernetický útok přičíst některému státu, se princip náležité péče a protiopatření při jeho porušení neuplatní.

Z hlediska mezinárodního práva však nelze přistoupit k protiopatřením v reakci na jakýkoli kybernetický útok. Možné to bude pouze ve vztahu k útoku, který způsobí škodu v určité významné míře. Hranice výše škody, na kterou stát zareaguje protiopatřením z důvodu, že jiný stát zanedbal náležitou opatrnost, tj. kdy dojde k uplatnění principu náležité opatrnosti, ovšem není jednoznačná. Obdobně jako je tomu v mezinárodním právu životního prostředí by mělo jít o závažné nepříznivé důsledky, tj. o škodu podstatného rozsahu, nikoli toliko o nepříjemnosti, drobná narušení, či škodu

---

[701] Tallinn Manual 2.0, Rule 33 - Non-State actors.

[702] BANNELIER, Karine, CHRISTAKIS, Theodore. Op. cit., str. 16.

[703] Byť na tom nepanuje mezi odborníky úplná shoda. Srov. Tallinn Manual 2.0, Rule 33 - Non-State actors, bod 2.

[704] V případě, kdy kybernetický útok dospěje do úrovně ozbrojeného útoku. Srov. Tallinn Manual 2.0, Rule 71, pojednávající o sebeobraně proti ozbrojenému útoku.

[705] Tallinn Manual 2.0, Rule 26 - Necessity. Překlad autorka.

zanedbatelného rozsahu.[706] Nemělo by se tak jednat například o případ pouhého zveřejnění nepříznivé informace vůči státu A bloggerem státu B z území tohoto státu B. Takový čin by totiž nevedl k závažným nepříznivým důsledkům pro stát A ani by neporušil žádný (mezinárodní) závazek státu B. Skutečnost, že došlo k porušení mezinárodně uznaného závazku státu je totiž další podmínkou pro uplatnění principu náležité opatrnosti: kybernetický útok nestátních aktérů musí být v rozporu s mezinárodním závazkem státu, z jehož území byl útok proveden. Opačný případ by však nastal u blokování vládních webových stránek klíčových pro výkon veřejných subjektivních práv, jako např. volebního práva.[707]

Na základě principu náležité péče lze užít protiopatření rovněž v případě kybernetického útoku na soukromou infrastrukturu (skutečnost, zda je útok veden na státní nebo soukromá zařízení a sítě totiž není rozhodující). Pokud v rámci obchodního konkurenčního boje provede obchodní společnost ve státě A ničivý kybernetický útok vůči svému konkurentovi ve státě B, pak stát A poruší princip náležité péče, jestliže o útoku ví, a přesto nezvolí dostupná opatření, jak tomuto útoku zabránit, přičemž útok způsobí obchodní společnosti ve státě B závažnou škodu.[708] Na rozdíl od účastenství na kybernetickém útoku jiného státu ve formě pomoci, jež předpokládá jednání státních orgánů ve formě konání, dojde k porušení principu náležité péče při opomenutí státních orgánů konat.[709]

2.4.2. Státní aktéři jako původci kybernetických operací

Není tajemstvím, že se řada států uchyluje k prosazování svých politických cílů kybernetickými prostředky. Jak uvádí Akoto, *„nelze se spoléhat na veřejné popírání či mlčení států, neboť poté bychom museli uzavřít, že dosud nedošlo k žádnému kybernetickému útoku státu"*.[710] Mezi zvláštní rysy kybernetických operací totiž patří utajený způsob provádění a popření, že by mělo jít o součást zahraniční politiky státu; naopak, řada států využívá k provedení kybernetických

---

[706] Tallinn Manual 2.0, Rule 6 - Due diligence (general principle), body 25 a 26. Velmi problematické jsou případy, kdy je škoda způsobena botnety umístěnými na území více států. Podrobněji srov. tamtéž, body 29 - 31.

[707] Tamtéž, bod 22 - 27.

[708] Tamtéž, bod 36.

[709] Tamtéž, bod 43. Dále též Tallinn Manual 2.0, Rule 7 - Compliance with the due diligence principle, bod 2.

[710] AKOTO, Evelyne. Les cyberattaques étatiques constituent - elles des actes d'agression en vertu du droit international public?: Première Partie [online]. *Ottawa Law Review*, Vol. 46, č. 1, 2015, str. 20. Dostupné: https://ssrn.com/abstract=2685249 [Cit. 2022-11-14]. Překlad autorka.

útoků namířených proti jiným státům soukromých osob, vlivem čehož je dovození mezinárodní odpovědnosti zvláště obtížné.[711]

Za kybernetický útok, jehož původcem je stát, však lze označit jakýkoli kybernetický útok sponzorovaný nebo zahájený přímo státem A či jeho jménem na jeho popud, anebo provedený díky jeho záměrnému opomenutí konat, z území tohoto státu, proti kybernetické infrastruktuře či počítačovému prostředí, jež jsou umístěny na území státu B.[712] Vhodné se zdá doplnit, že útok státu A může být namířen i proti kybernetické infrastruktuře pod kontrolou státu B, nejen proti té nacházející se na jeho území. Odpovědným státem bude stát, který porušuje závazek vůči jinému státu; stát, vůči němuž závazek existuje a není splněn, je poškozeným státem.[713]

Pravidlo č. 14 Tallinnského manuálu uvádí, že *„[s]tát nese mezinárodní odpovědnost za kybernetický čin, který mu je přičten a který je porušením mezinárodněprávního závazku."*[714] Citovaná úprava vychází z návrhu článků Komise OSN pro mezinárodní právo k tématu odpovědnosti států za protiprávní čin.[715] Zmíněný dokument o odpovědnosti států za mezinárodně protiprávní chování se stal předlohou řady ustanovení druhé verze Tallinnského manuálu. Návrh článků Komise OSN pro mezinárodní právo k tématu odpovědnosti států za protiprávní chování byl po dlouhých letech vyjednávání a cizelování přijat v roce 2001. Valné shromáždění OSN zahrnulo text jako přílohu své Rezoluce č. 56/83. Ač se nejedná o závazný právní dokument, mezinárodní soudy a tribunály odkazují od té doby v řadě rozhodnutí na jeho znění.[716] Návrh článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování tudíž nabývá na důležitosti, čím častěji na něj v rámci své rozhodovací činnosti odkazují mezinárodní soudy a tribunály. Detailnější rozbor hmotněprávních norem mezinárodního práva upravujících odpovědnost

---

[711] Tamtéž.

[712] Tamtéž, str. 10.

[713] Tallinn Manual 2.0, Section 1: Internationally Wrongful Acts By State, bod 3.

[714] Tallinn Manual 2.0, Rule 14 - Internationally wrongful cyber acts. Překlad autorka.

[715] ILC. Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, 2001, UN Doc. A/56/10.

[716] CRAWFORD, James. *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries.* Cambridge: Cambridge University Press, 2003, str. 48.

států za protiprávní činy[717] přesahuje cíle této práce, lze proto odkázat na dostupnou literaturu.[718] Postačí uvést, že z obecného hlediska čin, který povede ke vzniku mezinárodní odpovědnosti státu, musí kumulativně splnit následující podmínky: bude spáchán konáním nebo opomenutím za předpokladu, že takovým jednáním bude porušena povinnost uložená státu mezinárodním právem, a současně bude možné takový čin přičíst státu na základě norem mezinárodního práva.[719] Válečným konfliktům se následující text nevěnuje. V případě neexistence ozbrojeného konfliktu mezi dvěma státy se jakýkoli kybernetický útok mezi nimi považuje za čin uskutečněný v době míru a nepůjde o akt kybernetické války.[720]

Ačkoli Charta OSN, která vznikla s cílem vyvarovat se válečným hrůzám známým z první a druhé světové války,[721] se na první pohled nezdá jako dostačující dokument pro řešení konfliktů odehrávajících se v kyberprostoru, obsahuje klíčové pravidlo: zákaz použití síly. Podle čl. 2 odst. 4 Charty OSN *„[v]šichni členové se vystříhají ve svých mezinárodních stycích hrozby silou nebo použití síly jak proti územní celistvosti nebo politické nezávislosti kteréhokoli státu, tak jakýmkoli jiným způsobem neslučitelným s cíli Organizace spojených národů."*[722] Zákaz použití síly představuje primární normu mezinárodního práva. Uplatní se i v situaci, v níž neexistuje zvláštní smluvní ujednání o kybernetických operacích.

Každý mezinárodně protiprávní čin státu má za následek vznik odpovědnostního vztahu mezi poškozeným státem a státem, který porušil mezinárodní závazek.[723] Reparační povinnost státu v případě porušení mezinárodního závazku je principem mezinárodního práva.[724] Mezinárodní

---

[717] V práci používám spíše pojem čin nežli chování, který mezinárodní právo veřejné používá častěji, narozdíl od trestního práva hmotného, kde se hovoří o (protiprávních) činech. Domnívám se, že chování je širšího významu než čin.

[718] Srov. např. ČEPELKA, Čestmír, JÍLEK Dalibor, ŠTURMA, Pavel. *Mezinárodní odpovědnost*. Brno: Masarykova univerzita, 2003. ČEPELKA, Čestmír, ŠTURMA, Pavel, BÍLKOVÁ, Veronika. *Kodifikace a rozvoj mezinárodního práva: kodifikace mezinárodního práva, právo mezinárodních smluv, právo mezinárodní odpovědnosti*. Praha: Eva Rozkotová - IFEC, 2008, str. 130 a násl. ŠTURMA, Pavel. Mezinárodní odpovědnost za škodlivé následky činností nezakázaných mezinárodním právem. *Mezinárodní odpovědnost*. 1. vyd. Brno : Masarykova univerzita, 2003. KOLB, Robert. *The international law of state responsibility: an introduction*. Cheltenham, UK: Edward Elgar Publishing, 2017. CRAWFORD, James. *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries.* Cambridge: Cambridge University Press, 2003.

[719] Čl. 2 Návrhu článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování.

[720] AKOTO, Evelyne. Op. cit., str. 9.

[721] Vyhláška ministra zahraničních věcí č. 30/1947 Sb., ze dne 16. ledna 1947 o chartě Spojených národů a statutu Mezinárodního soudního dvora, sjednaných dne 26. června 1945 na konferenci Spojených národů o mezinárodní organisaci, konané v San Francisku (dále jen „Charta OSN").

[722] Čl. 2 odst. 4 Charty OSN.

[723] Čl. 1 Návrhu článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování.

[724] Srov. např. rozsudek Mezinárodního soudního dvora ze dne 26. 7. 1927, *Factory at Chorzów* (Německo v. Polské republice), PCIJ SeriesA No. 9, 21.

odpovědnost zahrnuje podle okolností případu obsahově různé nové právní vztahy, jež mohou zahrnovat požadavek na zdržení se protiprávní činnosti a zákaz jejího opakování, povinnost k náhradě vzniklé újmy, možnost provedení protiopatření i uložení sankce.[725] Prostředky nápravy, které má poškozený stát k dispozici, upravují právní normy o mezinárodní odpovědnosti států. Tallinn Manual 2.0 zdůrazňuje, že stejně tomu bude i v případě kritérií přičitatelnosti protiprávního činu konkrétnímu státu v kyberprostoru.[726]

Druh reakce poškozeného státu na kybernetický útok namířený vůči jeho státním zájmům, jakož i intenzita takové reakce, bývá často výsledkem rychlého posouzení v důsledku nedostatku času a informací. Obecně však platí, že čím bude kybernetický útok závažnějším porušením mezinárodní normy, tím více by se měl reagující stát opírat o konkrétní důkazy, které by měl být schopen v případě potřeby poskytnout (i veřejně). Intenzita svépomocných reakcí státu, mezi něž se řadí retorze, protiopatření, krajní nouze a sebeobrana, narůstá úměrně se závažností porušení mezinárodního práva.[727] Zároveň platí, že dotčený stát by měl jednat „rozumně", tj. *„takovým způsobem, jak by jednaly za stejných nebo obdobných okolností rozumné státy"*.[728]

Zásadní otázkou je pak rozlišení činů jednotlivců (soukromých osob) od státních činů, neboť z hlediska mezinárodního práva se chování soukromých osob nacházejících se na státním území, případně majících státní občanství, státu nepřičítá. Uvedené pravidlo je problematické v případě kybernetických útoků, neboť je mohou snadno uskutečnit soukromé osoby.

2.4.3. Přičitatelnost (atribuce)

2.4.3.1. Přičitatelnost kybernetických operací státních orgánů

Klíčovou podmínkou pro vznik mezinárodní odpovědnosti státu je přičitatelnost (atribuce) mezinárodně protiprávního činu (chování) státu. Základní pravidlo zní: *„Kybernetické operace prováděné státními orgány či osobami nebo subjekty zmocněnými vnitrostátním právem k výkonu státní moci, lze přičíst tomuto státu."*[729]

Česká právnická literatura rozumí státními orgány *„orgány, které stát zřizuje právě k plnění funkcí státu a vybavuje je za tím účelem pravomocí a působností rozhodovat o subjektivních*

[725] Srov. Část druhou a Část třetí, Kapitolu druhou Návrhu článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování.

[726] Tallinn Manual 2.0, Section 1: Internationally Wrongful Acts By State, bod 4.

[727] Tamtéž, bod 11 a 13.

[728] Tamtéž, bod 12. Překlad autorka.

[729] Tallinn Manual 2.0, Rule 15 - Attribution of cyber operations by State organs. Překlad autorka.

právech a právních povinnostech jemu bezprostředně nepodřízených právních subjektů."[730] Jedná se o orgány moci zákonodárné, výkonné a soudní. Jakékoli aktivity v kyberprostoru prováděné například vládou ČR jako vrcholným orgánem moci výkonné, ale i ministerstvy, zpravodajskými službami, či prezidentem republiky, poruší-li tyto aktivity mezinárodněprávní závazek státu, dají vzniknout mezinárodní odpovědnosti ČR.

Pojem státních orgánů je zde nutno vykládat široce: za státní orgán se považují všechny osoby a subjekty, které mají status státního orgánu podle vnitrostátního právního řádu daného státu, a to bez ohledu na svoji funkci či postavení v rámci hierarchického uspořádání.[731] Nevyžaduje se, aby vnitrostátní právo označovalo daný subjekt výslovně za státní orgán. Stát se nemůže zříci odpovědnosti za čin subjektu, který jednal jako státní orgán, tím, že by mu podle vnitrostátního práva takový status odepřel.[732] Stěžejní má být faktická závislost subjektu na státu, jehož je pouhým instrumentem.

Stát odpovídá i za činy státních orgánů, které představují překročení svěřených pravomocí k výkonu státní moci.[733] Bude-li např. příslušník vojenského zpravodajství provádět nezákonné kybernetické operace v rozporu s příkazy nadřízených, bude stát odpovídat za jakékoli porušení mezinárodních závazků, jichž se tento příslušník dopustí. Opačná situace však nastane v případě výlučně soukromých aktivit, např. při zneužití přístupu ke státní kybernetické infrastruktuře a spáchání trestného činu. Takové chování jednotlivce nebude státu přičteno.[734]

Stát odpovídá rovněž za přenesený výkon státní moci v případě nepřímých vykonavatelů státní správy, pokud jednají v rámci svěřené pravomoci.[735] Stát přitom zavazuje i jednání *ultra vires*.[736] Tallinn Manual 2.0 například uvádí exces v podobě aktivní kybernetické obrany ve formě zpětného hackingu (*hacking back*) ze strany soukromé společnosti zmocněné k pasivní kybernetické obraně státu.[737] Stát by měl patrně odpovídat rovněž za činnost soukromých osob, pokud k ní došlo na základě uzavřené a platné veřejnoprávní smlouvy v rámci zákonem předpokládané působnosti a

---

[730] VOJTEK, Petr. § 3 [Subjekty, za jejichž činnost stát odpovídá]. In: VOJTEK, Petr, BIČÁK, Vít. *Odpovědnost za škodu při výkonu veřejné moci.* 4. vydání. Praha: C. H. Beck, 2017, str. 35.

[731] Čl. 4 odst. 2 Návrhu článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování.

[732] Bod 11 komentáře k čl. 4 Návrhu článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování.

[733] Čl. 7 Návrhu článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování.

[734] Tallinn Manual 2.0, Rule 15 - Attribution of cyber operations by State organs, body 6 - 7.

[735] Čl. 5 Návrhu článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování.

[736] Čl. 7 Návrhu článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování.

[737] Tallinn Manual 2.0, Rule 15 - Attribution of cyber operations by State organs, bod 12.

pravomoci.[738] Výjimečně bude stát odpovídat i za činnost soukromých osob nezmocněných k výkonu dané pravomoci, pokud se samotný stát nachází v takové situaci, která mu znemožňuje výkon pravomoci, ačkoli by byl takový výkon pravomoci nutností, např. v případě vnitřního ozbrojeného konfliktu.[739]

Územní hledisko je pro problematiku přičitatelnosti jednání státu nepříliš významné. Jak je patrné z výkladu o kybernetické trestné činnosti, existuje mnoho způsobů, jak poškozený stát zmást a provést kybernetický útok bez vazby na území útočícího státu. Příkladem může být padělání identity a IP adres (*spoofing*), zneužití botnetu k provedení útoku, ale také provedení kybernetického útoku pomocí soukromé kybernetické infrastruktury z různých státních území.[740]

V případě, kdy stát jedná prostřednictvím státního orgánu jiného státu, jenž mu byl dán k dispozici, považuje se výkon pravomoci tohoto orgánu za jednání přijímajícího státu.[741] To za podmínek, že dotčený orgán jedná pod výhradním vedením a kontrolou přijímajícího státu, nikoli státu vysílajícího (byť vysílající stát může i financovat dále jeho činnost), a dále že je daná činnost prováděna výlučně k účelům a jménem přijímajícího státu. Pokud by však např. stát A vyslal státu B svůj CERT tým za účelem potlačení kybernetického útoku, jehož cílem by byly oba státy, zůstane odpovědným za činnost svého CERT týmu stát A. Přijímající stát však odpovídá i za exces cizího státního orgánu, pokud takový orgán kontroluje.[742]

Stát reagující na kybernetický útok jiného státu musí mít k dispozici důkazní prostředky, jimiž hodlá prokázat přičitatelnost kybernetického útoku jinému státu. Prokázání přičitatelnosti kybernetických operací konkrétnímu státu bývá spojeno s řadou obtíží, neboť zahrnuje tři roviny dokazování. Nejprve je třeba prokázat umístění počítačových zařízení či serverů, které byly původcem kybernetické operace, poté je třeba ztotožnit osobu, která tato zařízení ovládala, a konečně je třeba prokázat, že jednání takové osoby lze přičíst konkrétnímu státu.[743] Důkazní prostředky přitom nemusejí být předloženy pouze mezinárodním soudům a tribunálům; často je vlády předkládají různým politickým orgánům i široké veřejnosti za účelem získání širší politické

---

[738] Srov. Tallinn Manual 2.0, Rule 15 - Attribution of cyber operations by State organs, bod 10, který zmiňuje smluvní přenesení pravomoci provádět digitální forenzní analýzu v rámci činnosti orgánů činných v trestním řízení na soukromou osobu.

[739] Podrobněji tamtéž, bod 17.

[740] Tallinn Manual 2.0, Rule 15 - Attribution of cyber operations by State organs, body 14 - 15. Popsán je zde útok na jihokorejská média a bankovní sektor v roce 2013, který byl připsán Severní Koree, byť byl proveden pomocí botnetů skrze kybernetické infrastruktury na území řady států.

[741] Tallinn Manual 2.0, Rule 16 - Attribution of cyber operations by organs of other States.

[742] Tamtéž, body 1 - 5.

[743] ROSCINI, Marco. Op. cit., str. 239 - 240.

podpory pro svůj následný postup.[744] Podrobněji lze k problematice dokazování kybernetických operací odkázat například na článek Marca Rosciniho.[745]

2.4.3.2. Přičitatelnost kybernetických operací nestátních aktérů

Jednání soukromých subjektů v zásadě nelze považovat za jednání státu. Mezinárodní právo stanoví specifické podmínky, za kterých však lze jednání jednotlivců (soukromých osob) přičíst konkrétnímu státu a dovodit jeho mezinárodní odpovědnost. Tallinn Manual 2.0 zmiňuje následující podmínky: *„Kybernetické operace prováděné nestátními aktéry lze přičíst státu, pokud jsou prováděny podle jeho pokynů či pod jeho vedením nebo kontrolou, anebo jestliže je stát uzná za své."*[746] Pro kyberprostor se tak přebírá úprava čl. 8 Návrhu článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování, který se vztahuje na chování jednotlivců i skupin.[747] Úprava dopadá na samostatně jednající hackery, na organizované aktivistické skupiny či hnutí typu Anonymous, na obchodní korporace, i na organizované skupiny páchající trestnou činnost či teroristická uskupení; přítomnost hierarchického uspořádání ani stupeň organizovanosti skupiny není rozhodující.[748]

Stát odpovídá za činy nestátních aktérů, existuje-li mezi státem a jednajícím soukromým subjektem faktický vztah, který se demonstruje udílením pokynů, řízením činnosti nebo výkonem kontroly.[749] Nestátní aktér jednající na základě pokynů státu např. může fungovat jako „pomocná síla" v případě nedostatečné kapacity státních orgánů zvládnout masivní kybernetický útok.[750] Dopustí-li se přitom nestátní aktér mezinárodně protiprávního činu, bude odpovědným stát.

Má-li být jednání nestátních aktérů přičitatelné státu proto, že je prováděno pod kontrolou státu, musí ovšem jít o efektivní kontrolu. Stát musí v takovém případě nařizovat provedení kybernetických operací a řídit jejich průběh i jejich ukončení, přičemž musí jít o nedílnou součást

---

[744] Příkladem je předložení důkazních prostředků Radě bezpečnosti OSN Reaganovou administrativou k ospravedlnění ozbrojeného zákroku v Tripoli v Lybii roku 1986 jakožto opatření v sebeobraně. ROSCINI, Marco. Op. cit., str. 241.

[745] ROSCINI, Marco. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations [online]. *Texas International Law Journal*, 2015, č. 50. Dostupné: https://ssrn.com/abstract=2611753 [Cit. 2022-11-02].

[746] Tallinn Manual 2.0., Rule 17 - Attribution of cyber operations by non-State actors. Překlad autorka.

[747] Čl. 8 Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování zní: *„Jednání osoby či skupiny osob bude považováno za akt státu ve smyslu mezinárodního práva, jestliže tato osoba či skupina osob ve skutečnosti jedná podle pokynů tohoto státu, či pod jeho vedením nebo kontrolou."* Překlad autorka.

[748] Tallinn Manual 2.0, Rule 17 - Attribution of cyber operations by non-State actors, bod 2.

[749] Tamtéž, bod 3.

[750] Srov. příklady tamtéž, bod 4.

státem plánovaných aktivit.[751] Nejedná se o pouhou spolupráci státu a soukromých subjektů ani o případy poskytnutí vybavení či financování aktivit ze strany státu. Takové podpůrčí aktivity státu by však mohly být považovány za nedovolenou intervenci.[752]

Narozdíl od pravidel upravujících přičitatelnost u státních orgánů v zásadě stát neodpovídá za exces v jednání soukromých osob. Tallinn Manual 2.0 příkladem uvádí tři roviny excesu: 1. Dá-li stát A pokyn k destruktivním kybernetickým útokům vůči majetku státu B, odpovídá za jednání nestátního aktéra, který se snažil takový cíl splnit instalací zvláště škodlivého malware. 2. Pokud by se malware nepředpokládaně rozšířil do systémů státu C a způsobil zde škodu, bude jednání soukromé osoby rovněž přičitatelné státu A, neboť škoda vznikla na základě jednání soukromé osoby, k němuž dal stát A pokyn, byť součástí jeho pokynu nebylo způsobit škodu státu C. 3. Zaměří-li se soukromá osoba v rozporu s pokynem státu A na použití malware vůči státu C, půjde o exces a její jednání nebude státu A přičitatelné. Kybernetické operace soukromé osoby jsou excesem, který nelze státu příčíst, jestliže nesouvisejí s účelem operace kontrolované státem, ledaže by je stát uznal a přijal za své.[753]

Uznání a přijetí kybernetického útoku nestátního aktéra za vlastní musí být ze strany státu výslovné, aby mu bylo možné daný útok přičíst. Uznání mlčky, respektive tichý souhlas či schvalování by takové následky nevzbudilo. O výslovné uznání a přijetí kybernetického útoku za vlastní by mohlo jít v případě, kdy by stát cíleně podnikl konkrétní kroky k ochraně útočníků před protiopatřeními či jinou reakcí ze strany poškozeného státu tak, aby mohl útok pokračovat.[754]

Jestliže shora nastíněné podmínky k tomu, aby bylo jednání jednotlivce přičteno konkrétnímu státu, naplněny nejsou, může stát popřít svoji odpovědnost. Problém přičitatelnosti však mohou státy zneužívat s cílem získat politickou či vojenskou výhodu. Tím se stává problém přičitatelnosti součástí konceptu *lawfare*, kdy je právo zneužito k získání vojensky hodnotného cíle, který by jinak byl získán s pomocí tradičních vojenských prostředků. Zejména v hybridních konfliktech, mezi něž se řadí i využití kybernetických operací, jde o čím dál častěji využívanou taktiku.[755]

---

[751] Rozsudek Mezinárodního soudního dvora ze dne 27. 6. 1986, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America),* odst. 115. Dostupný: https://www.icj-cij.org/en/case/70 [Cit. 2022-11-14], jakož i Tallinn Manual 2.0, Rule 17 - Attribution of cyber operations by non-State actors, body 6 - 7.

[752] Podrobněji Tallinn Manual 2.0, Rule 17 - Attribution of cyber operations by non-State actors, body 8 - 9.

[753] Tamtéž, body 12 - 13 a 15.

[754] Tamtéž, bod 16.

[755] BRUNER, Tomáš, FAIX, Martin. Problém přičitatelnosti jako nástroj lawfare [online]. *Obrana a strategie*. Brno: University of Defence, 2018, 2018(1), str. 79-95. Dostupné: https://www-ceeol-com.ezproxy.is.cuni.cz/search/journal-detail?id=139 [Cit. 2022-11-14].

Lze doplnit, že s pojmem přičitatelnosti, resp. atribuce, se setkáme i na vnitrostátní úrovni. Národní strategie kybernetické bezpečnosti jej vysvětluje jako *„[p]roces přičitatelnosti škodlivých aktivit v kyberprostoru určitému zdroji k aktivitám konkrétního státu nebo aktivitám nezávislým na státních strukturách. Provádí se na technické, netechnické a všezdrojové úrovni. Na politické úrovni poté probíhá schválení atribuce a rozhodnutí o jejím využití."*[756] Podle Akčního plánu je úkolem NÚKIB, MZV, PČR, ÚV ČR a zpravodajských služeb *„[v]ytvořit, implementovat a v relevantních případech aktivovat efektivní národní rámec plnohodnotné atribuce závažných kybernetických útoků."*[757]

2.4.4. Okolnosti vylučující protiprávnost kybernetických operací

2.4.4.1. Přehled okolností vylučujících protiprávnost

Mezinárodní právo zohledňuje určité okolnosti, za kterých nelze považovat chování státu za protiprávní. Pravidlo č. 19 Tallinn Manual 2.0 vychází z Kapitoly V. Návrhu článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování. Protiprávnost aktu zahrnujícího kybernetické operace se tak vylučuje v případech: a) souhlasu (*consent*), b) sebeobrany (*self-defence*), c) protiopatření (*countermeasures*), d) krajní nouze (*necessity*), e) vyšší moci (*force majeure*), a f) tísně (*distress*).[758]

Přítomnost okolnosti vylučující protiprávnost znamená, že jednající stát neporušil mezinárodní závazek, resp. že daný čin nelze hodnotit za rozporný s mezinárodním právem.[759] Tyto okolnosti však nemohou vyloučit protiprávnost, pokud dotčený čin porušil imperativní normu (např. lidskoprávní normy).[760] Vedle šesti citovaných okolností vylučujících protiprávnost existují další instituty, jež mohou být aplikovány vedle nich jako *lex specialis*. Jde o schválení určitého aktu Radou bezpečnosti OSN či o koncept krajní nouze v rámci ozbrojeného konfliktu ve vztahu k mezinárodnímu humanitárnímu právu.[761]

---

[756] NÚKIB. *Národní strategie kybernetické bezpečnosti České republiky na období let 2021 - 2025.* Op. cit., str. 13 - 14.

[757] NÚKIB. *Akční plán k Národní strategii kybernetické bezpečnosti ČR na období let 2021 až 2025.* Op. cit., str. 7.

[758] Tallinn Manual 2.0, Rule 19 - Circumstances precluding wrongfulness of cyber operations. Překlad autorka.

[759] Tamtéž, str. 20.

[760] Čl. 26 Návrhu článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování.

[761] Podrobněji viz CRAWFORD, James. Opak, cit., str. 54 an.

Situace případného odškodnění u okolností vylučujících protiprávnost však není jednoznačná, neboť nelze vyloučit, že u některých z řečených okolností bude požadavek odškodnění poškozeného státu na místě.[762]

Souhlasí-li stát s kybernetickou operací jiného státu, nemůže později s úspěchem tvrdit, že tato operace, byla-li provedena v mezích uděleného souhlasu, byla v rozporu s mezinárodním závazkem. Souhlas musí být udělen předem a svobodně, tj. bez jakéhokoli nátlaku či výhrůžky, a to k tomu oprávněným orgánem státu.[763] Ačkoli lze doporučit výslovné udělení souhlasu, v některých případech postačí i souhlas implicitní.[764]

Je-li kybernetický útok (operace) součástí sebeobrany státu proti ozbrojenému útoku, nepůjde z hlediska mezinárodního práva o protiprávní čin. Sebeobrana rovněž vylučuje porušení suverenity státu, který prve zaútočil. I jednání v sebeobraně však musí dostát závazku státu chránit základní lidská práva a neútočit na civilní cíle.[765] Sebeobrana v reakci na porušení zákazu použití ozbrojené síly navíc později vylučuje požadavek odškodnění po státu, který se uchýlil k sebeobraně.[766]

O protiopatření a krajní nouzi pojednají následující dvě podkapitoly.

V případě vyšší moci není odškodnění vyloučeno.[767] Tato okolnost zahrnuje výskyt nepředvídatelné události či nepřekonatelné síly, které jsou mimo kontrolu státu a za daných okolností tomuto státu fakticky znemožňují, aby dostál mezinárodnímu závazku.[768] Pouhé ztížení splnění závazku či jeho plnění s vyššími náklady však nelze kvalifikovat jako vyšší moc, stejně jako situace, v níž nelze závazek splnit kvůli chování státu, který jej měl splnit.[769] Tallinn Manual 2.0 uvádí jako příklad vyšší moci zničení počítačového serveru při tornádu, vlivem čehož nelze server využít v souladu s uzavřenou mezinárodní smlouvou.[770]

---

[762] Podrobněji ČEPELKA, Čestmír. Náhrada škody způsobené chováním státu za okolností vylučujících protiprávnost tohoto chování. In: ČEPELKA, Čestmír, JÍLEK Dalibor, ŠTURMA, Pavel. *Mezinárodní odpovědnost*. Brno: Masarykova univerzita, 2003, str. 9 - 110.

[763] Tallinn Manual 2.0, Rule 19 – Circumstances precluding wrongfulness of cyber operations, body 2 - 8.

[764] Tamtéž, bod 7.

[765] Tamtéž, body 11 - 12.

[766] ČEPELKA, Čestmír. Op. cit., str. 21 an.

[767] Tamtéž, str. 63 an.

[768] Čl. 23 Návrhu článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování.

[769] Tamtéž. Tallinn Manual 2.0., Rule 19 – Circumstances precluding wrongfulness of cyber operations, body 15 - 16.

[770] Tallinn Manual 2.0, Rule 19 - Circumstances precluding wrongfulness of cyber operations, bod 15.

Tíseň jako okolnost vylučující protiprávnost se vztahuje na život ohrožující případy. Uplatní se v situaci, v níž jednotlivec, jehož jednání je přičitatelné státu, nemá jiný rozumný způsob, jak zachránit život svůj nebo životy jiných osob svěřených mu do péče.[771] Je však vyloučeno, aby stát, který se dovolává tísně, přispěl k této situaci. Jednání v tísni rovněž nesmí vést ke srovnatelné nebo větší újmě než jaká by nastala, pokud by jednající stát jinak dostál svému závazku.[772]

Za žádných okolností však nelze vyloučit protiprávnost činu v případě porušení imperativní normy, která je přijímána a uznávána mezinárodním společenstvím a od níž se nelze jakkoli odchýlit. Kybernetické operace porušující zákaz agrese, genocidy či mučení proto budou za všech okolností protiprávní.[773]

2.4.4.2. Vybrané okolnosti vylučující protiprávnost: Protiopatření

Podle pravidla č. 20 Tallinn Manual 2.0 je *„stát oprávněn přistoupit k protiopatřením, ať již kybernetického či jiného rázu, v reakci na porušení mezinárodního závazku jiným státem."*[774] Ačkoli jsou protiopatření zařazena mezi okolnostmi vylučujícími protiprávnost, a to jak v Tallinn Manual 2.0, tak i v Návrhu článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování, jde v podstatě o výkon práva přinutit odpovědný stát k respektování mezinárodněprávních závazků. Z tohoto důvodu nepřichází v úvahu povinnost k odčinění škody, jež by případně vznikla donucovanému státu v souvislosti s uplatněnými protiopatřeními.[775]

Protiopatřením se rozumí konání či opomenutí poškozeného státu v reakci na mezinárodně protiprávní čin, které je namířeno proti státu odpovědnému za porušení mezinárodního závazku;[776] samo protiopatření by rovněž bylo porušením mezinárodního závazku vůči odpovědnému státu, nebýt protiprávního činu, na který se protiopatřením reaguje. Mezinárodní právo tudíž protiopatření připouští jako po právu.[777]

---

[771] Čl. 24 odst. 1 Návrhu článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování.

[772] Tallinn Manual 2.0, Rule 19 – Circumstances precluding wrongfulness of cyber operations, bod 20.

[773] Srov. Vyhlášku ministra zahraničních věcí ze dne 4. září 1987 č. 15/1988 Sb., o Vídeňské úmluvě o smluvním právu, čl. 53. Viz Tallinn Manual 2.0, Rule 19 – Circumstances precluding wrongfulness of cyber operations, bod 22.

[774] Tallinn Manual 2.0, Rule 20 - Countermeasures (general principle). Překlad autorka.

[775] ČEPELKA, Čestmír. Op. cit., str. 51.

[776] Srov. Tallinn Manual 2.0, Rule 24 - States entitled to take countermeasures.

[777] Rozsudek Mezinárodního soudního dvora ze dne 27. 6. 1986, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*. Op. cit., odst. 249, či rozsudek téhož soudu ze dne 25. 9. 1997, *Gabčíkovo-Nagymaros Project (Hungary v. Slovakia),* odst. 82–83. Dostupný: https://www.icj-cij.org/en/decisions/judgment/1997/1997/desc [Cit. 2022-11-15]. A dále i Tallinn Manual 2.0, Rule 20 - Countermeasures (general principle), bod 1.

Prvotně bylo protiopatření vnímáno jako cesta k novaci porušeného závazku, jejímž smyslem bylo vyloučit možnost volného uchýlení se k donucení represáliemi nebo válkou.[778] Protiopatření by tak mělo sloužit k vyhnutí se válečnému konfliktu. I z toho důvodu je nelze směšovat s odvetnými opatřeními v boji, k nimž dochází během ozbrojeného konfliktu. Nejde ani o postupy proti nepříteli během ozbrojeného konfliktu, které souvisejí s tímto konfliktem.[779] Protiopatření nelze zaměňovat ani s retorzemi, které samy o sobě nejsou porušením mezinárodního závazku.[780]

Cílem protiopatření je přimět odpovědný stát k opětovnému plnění dotčeného mezinárodního závazku.[781] Reagují na trvající porušení či neplnění mezinárodní právní povinnosti státem, jakož i na opakující se jednotlivé útoky. Např. v případě trvajících DDoS útoků na vládní počítačové systémy a sítě bude dotčený stát kdykoli oprávněn přistoupit k protiopatřením vůči odpovědnému státu. Jestliže však odpovědný stát nebude nadále porušovat mezinárodní závazek a nebude ani hrozit opakováním protiprávní činnosti, a bude zjednána náprava či poskytnuta záruka, nebude možné se již k protiopatřením uchýlit.[782] Protiopatření dále nebudou přípustná, bude-li porušení mezinárodního závazku již předmětem řízení před soudem či tribunálem.[783]

Protiopatření mají být prostředkem k obnovení řádných právních vztahů mezi státy, nemají být nástrojem zastrašení či pomsty. Neměly by ani vést k dalším porušením mezinárodních závazků vůči třetím stranám.[784] Stát, jenž porušil mezinárodní závazek, musí strpět od poškozeného státu protiopatření, jestliže neníní odčinit újmu, kterou způsobil. Tato újma je přitom některými vnímána jako újma *erga omnes*, tj. vůči všem státům vytvářejícím mezinárodní společenství.[785] Pojmovým znakem protiopatření ovšem je, že k nim je oprávněn přistoupit právě poškozený stát.

Pokud se stát dotčený porušením mezinárodního závazku rozhodne přistoupit k protiopatřením, měl by o tom informovat odpovědný stát. Zmíněný požadavek patrně nebude

---

[778] Podrobněji k historickému vývoji pojmu protiopatření srov. ČEPELKA, Čestmír. Op. cit., str. 23 - 26.

[779] K protiopatřením se však lze uchýlit v reakci na jednání strany, jež je součástí mezinárodního ozbrojeného konfliktu, avšak v reakci na porušení jiných norem než je právo ozbrojeného konfliktu. Tallinn Manual 2.0, Rule 20 - Countermeasures (general principle), bod 3.

[780] Tamtéž, bod 4.

[781] Tallinn Manual 2.0, Rule 21 - Purpose of countermeasures.

[782] Tamtéž, body 6 - 7, a čl. 49 odst. 1 Návrhu článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování.

[783] Čl. 52 odst. 3 Návrhu článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování. Podrobněji srov. Tallinn Manual 2.0., Pravidlo č. 21, body 14 - 18.

[784] Srov. Tallinn Manual 2.0, Rule 25 - Effect of countermeasures on third parties.

[785] ČEPELKA, Čestmír. Op. cit., str. 27.

možné vždy plnit u kybernetických útoků, na něž je zpravidla nutno zareagovat rychle. Pro tyto případy je dotčený stát oprávněn přistoupit k urgentním protiopatřením bez notifikace, na což pamatuje i návrh článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování.[786] V každém případě stát, který hodlá přistoupit k protiopatřením, musí mít k dispozici důkazní prostředky, jimiž prokáže existenci kybernetického útoku porušujícího mezinárodní závazek státu a jeho přičitatelnost konkrétnímu státu, a pokud útok nebude možné státu přičíst, pak musí prokázat, že daný stát nedostál povinnosti náležité péče spočívající v tom, že kybernetickému útoku nezamezil.[787]

Při volbě konkrétní reakce by měl stát vzít v úvahu riziko eskalace konfliktu.[788] V nejlepším případě by měly být následky protiopatření dočasné, resp. odstranitelné. Bránění v přístupu ke klíčovým datům (informacím) na základě omezení jejich dostupnosti či omezení služby by dostálo této podmínce, zatímco vymazání či zničení dat nikoli. Nepanuje však shoda na tom, zda by dotčený stát měl z možných kybernetických protiopatření zvolit to s nejsnáze odstranitelnými negativními dopady, anebo zda postačí jen faktická možnost odstranění nepříznivých dopadů.[789] V každém případě však protiopatření nesmí vést k porušení základních lidských práv ani imperativních norem a musí respektovat nedotknutelnost diplomatických a konzulární misí.[790]

Klíčovým hlediskem uplatnění protiopatření (ať již kybernetického rázu či nikoli) je proporcionalita. Protiopatření musí být úměrné nejen vůči újmě, kterou utrpěl dotčený stát a na níž protiopatření reagují, nýbrž i vůči závažnosti mezinárodně protiprávního činu a dotčeným právům.[791] Újma však nemusí znamenat, že došlo ke vzniku škody, natož škody určitého rozsahu. Postačí, že byl porušen mezinárodní závazek (srov. shora).

Z hlediska požadavku proporcionality může být obtížné předem hodnotit dopady protiopatření, které je kybernetického rázu. Před tím, než stát přistoupí ke konkrétnímu protiopatření, proto Tallinn Manual 2.0 doporučuje pečlivé posouzení (např. skrze zmapování cílového systému, kontroly klíčových informací).[792] Dopady konkrétního protiopatření je třeba

---

[786] Čl. 52 odst. 2 Návrhu článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování.

[787] ROSCINI, Marco. Op. cit., str. 239.

[788] Tallinn Manual 2.0., Rule 21 - Purpose of countermeasures, body 1 - 2.

[789] Tamtéž, bod 9.

[790] Srov. Tallinn Manual 2.0, Rule 22 - Limitations on countermeasures.

[791] Tallinn Manual 2.0, Rule 23 - Proportionality of countermeasures, a čl. 51 Návrhu článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování.

[792] Tallinn Manual 2.0, Rule 23 - Proportionality of countermeasures, bod 6.

hodnotit souhrnně; přistoupí-li jednající stát k více kybernetickým operacím, mohly by samostatně představovat jen zanedbatelné riziko, avšak ve svém souhrnu by byly kybernetickým útokem s citelným dopadem pro fungování klíčových služeb státu.

Protiopatření mají především obnovit stav, v němž státy plní mezinárodní závazky. Zvolený druh protiopatření však nemusí nutně souviset s dotčeným závazkem, jehož plnění se stát domáhá. Zásadní totiž je, zda zvolené protiopatření povede odpovědný stát k dodržování mezinárodního závazku. Proto je možné, aby se reagovalo na porušení mezinárodních smluv z nejrůznějších oblastí právní úpravy právě kybernetickým protiopatřením, jakož i naopak: lze zvolit klasické protiopatření z oblasti mezinárodních obchodních vztahů, které bude reagovat na kybernetický útok porušující státní suverenitu.[793]

Jelikož důvodem uchýlení se k protiopatřením je docílit obnovy vzájemných řádných vztahů mezi státy, není možné zvolit protiopatření proti nestátním aktérům. Výjimkou by byl případ, kdy by byly činy nestátních aktérů přičitatelné konkrétnímu státu. Lze se nicméně setkat s odlišným názorem, podle něhož lze protiopatření užít i proti nestátním aktérům, pokud by porušili mezinárodní závazek (typicky zákaz použití síly a nenarušení státní suverenity) vůči státu. Zastánci tohoto přístupu zdůrazňují, že je výhodný zejména tam, kde nelze kybernetický útok přičíst žádnému státu. Tak by tomu bylo i v případě teroristických skupin, proti nimž by stát, na jehož území operují, sice zasáhl v souladu s principem náležité péče všemi dostupnými prostředky, avšak marně a kybernetický útok by nadále trval.[794] Zmíněný postoj lze považovat za praktický. Pomíjí však možnosti států reagovat na kybernetický útok na základě dalších okolností vylučujících protiprávnost, a sice krajní nouze nebo sebeobrany. I z těchto důvodů není většinově akceptován.[795] Na druhou stranu však krajní nouze i sebeobrana vyžadují, aby kybernetický útok dosáhl určité síly, respektive aby již vážně a bezprostředně ohrozil klíčové státní zájmy. U protiopatření na rozdíl od toho není hledisko ohrožení podstatné. Postačí totiž, že stát porušil mezinárodní závazek, byť by takový závazek neměl sám o sobě ničivý dopad na poškozený stát.

2.4.4.3. Vybrané okolnosti vylučující protiprávnost: Krajní nouze

Podle Tallinn Manual 2.0 *„může stát jednat ve stavu krajní nouze, reaguje-li na činy představující nanejvýše závažné a bezprostřední ohrožení podstatných zájmů státu, ať jde o činy*

[793] Obdobně tamtéž, bod 10.

[794] Tallinn Manual 2.0., Rule 21 - Purpose of countermeasures, body 5 a 7 - 9.

[795] Podrobněji tamtéž, bod 10.

kybernetického rázu či nikoli, pokud se jedná o jediný možný prostředek ochrany takových zájmů."[796]

Předlohou úpravy je čl. 25 Návrhu článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování. Citovat lze proto shrnutí podmínek krajní nouze podané Čepelkou: *„Musí jít (i) o podstatný zájem, tedy širší než je zájem existenční, avšak vždy podstatný. Musí jít (ii) o případ ohrožení, a to nanejvýše závažné a bezprostřední, jež stát přiměje chovat se v rozporu s mezinárodním závazkem k tíži státu jiného, protože právě to je jedinou možností, jak odvrátit řečené ohrožení, tedy není jiný způsob - byť mnohem nákladnější, avšak v souladu s jeho mezinárodními závazky - jak toto ohrožení odvrátit. Musí jít (iii) o situaci, ke které stát, dovolávající se stavu krajní nouze, sám nepřispěl, a to buď z nedbalosti nebo záměrně. A konečně, (iv) obětovaný zájem státu poškozeného musí být menší, než zájem ochráněný opatřeními v krajní nouzi."*[797]

Klíčovou podmínkou pro dovolání se krajní nouze je skutečnost, že podstatný (zásadní, *essential*) zájem státu se ocitl v ohrožení. Jaký zájem to je, Tallinn Manual 2.0 nekonkretizuje a ani mezinárodní právo všeobecně přijímanou definici nezná; bude proto třeba neurčitý pojem vykládat ve vztahu k okolnostem.[798] Výjimečně bude dokonce možné, aby bylo v rámci krajní nouze zasáhnuto na ochranu podstatných zájmů mezinárodního společenství jako celku. Každý stát se totiž může dovolat odpovědnosti jiného státu, jenž kybernetickými operacemi porušuje závazky *erga omnes*, tj. vůči mezinárodnímu společenství jako celku.[799] Tallinn Manual 2.0 příkladem uvádí situaci, v níž by nestátní aktéři skrze Internet s úspěchem podnítili genocidu ve státě. Byly-li by splněny ostatní podmínky pro jednání v krajní nouzi, byl by jakýkoli stát oprávněn zasáhnout kybernetickými prostředky proti takovému podněcování genocidy.[800] Uvedený příklad je mimořádně zajímavý s ohledem na silné pole působnosti on-line sdělovacích prostředků a existenci nejrůznějších elektronických komunikačních sítí.[801]

Požadavek nanejvýše závažného a bezprostředního ohrožení znemožňuje, aby stát provedl kybernetickou operaci s odkazem na krajní nouzi v jiných případech než u zcela fundamentálního

---

[796] Tallinn Manual 2.0, Rule 26 - Necessity. Překlad autorka.

[797] ČEPELKA, Čestmír. Op. cit., str. 75.

[798] Tallinn Manual 2.0, Rule 26 - Necessity, bod 2.

[799] Tallinn Manual 2.0, Rule 30 - Breach of obligations owed to the international community as a whole.

[800] Tallinn Manual 2.0, Rule 26 - Necessity, bod 3.

[801] Lze připomenout, že během genocidy ve Rwandě podněcovala místní média populaci Hutu ke genocidě, čímž podstatně přispěla k násilí vůči Tutsiům. Srov. KAYUMBA, David, *State Sovereignty Versus Individual Rights in the Case of the 1994 Genocide in Rwanda* [online]. Entebbe, 2006. Diplomová práce. Nkumba University, School of Social Sciences. Vedoucí práce Dr. Michael Mawa, bod 2.6.3. Dostupné: https://ssrn.com/abstract=1831542 [Cit. 2022-11-15].

ohrožení státních zájmů. Na základě Tallinn Manual 2.0 by bylo možné považovat za ohrožení fundamentálních zájmů státu kybernetický útok na státní kritickou infrastrukturu s významnými negativními dopady na bezpečnost, ekonomiku, veřejný zdravotní sektor nebo životní prostředí ve státě. Příkladem je uveden kybernetický útok, který by oslabil státní bankovní systém, způsobil dramatickou ztrátu důvěry v jeho akciový trh, zamezil veškerému leteckému či železničnímu provozu ve státě, znemožnil vyplácení dávek ze systému sociálního zabezpečení či důchodového pojištění nebo odstavil rozsáhlou elektrickou síť nebo integrovaný systém protivzdušné obrany, atp.[802] Pokud by se jednalo o situaci, v níž stát zatím neutrpěl žádnou újmu, musí pro uplatnění krajní nouze nebezpečí chráněnému zájmu stále trvat. Není však rozhodné, projeví-li se újma až za určitý čas.[803]

Skutečnost, že čin v krajní nouzi zasáhne do práv třetích států, není pro její uplatnění rozhodující. Výjimkou by ovšem byly kybernetické operace, jež by vážně poškodily základní zájmy třetích států: takové operace jsou zakázány, bez ohledu na rozsah újmy, kterou poškozený stát utrpěl.[804] Zmíněná omezující podmínka aplikace krajní nouze závisí opět na výkladu neurčité kategorie základních zájmů státu. S ohledem na shora uvedené příklady, které zmiňuje Tallinn Manual 2.0, se lze domnívat, že zapovězené budou opět kybernetické operace s vážnými negativními dopady do klíčové infrastruktury třetích států v oblasti státní bezpečnosti, ekonomiky, zdravotnictví, či životního prostředí. Uvedené negativní dopady projevující se ve sféře třetích států by měl stát jednající v krajní nouzi zohlednit ještě před započetím kybernetické operace. Zapovězeny by měly být též kybernetické operace představující násilnou akci či použití síly, neboť k nim lze přistoupit jen v rámci sebeobrany či se souhlasem Rady bezpečnosti OSN.[805]

Co se týče podmínky výlučnosti kybernetické operace v krajní nouzi, tj. neexistence jiné možnosti záchrany ohroženého základního zájmu státu, než právě provedení konkrétní kybernetické operace, nejsou z hlediska posuzování alternativ náklady ani ztížená možnost jiného způsobu řešení situace rozhodující. Jestliže je například možné přesměrovat datovou komunikaci z napadené

---

[802] Tallinn Manual 2.0, Rule 26 - Necessity, bod 5.

[803] Tamtéž, body 14 - 16 a rozsudek Mezinárodního soudního dvora ze dne 25. 9. 1997, *Gabčíkovo-Nagymaros Project (Hungary v. Slovakia)*. Op. cit., odst. 54.

[804] Tallinn Manual 2.0, Rule 26 - Necessity, body 6 a 8 a čl. 25 odst. 1 písm. b) Návrhu článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování.

[805] Srov. však i opačný názor uvedený v Tallinn Manual 2.0, Rule 26 - Necessity, bod 18.

infrastruktury jinam, byť s vyššími náklady, není možné s odkazem na krajní nouzi zvolit cestu zpětného hackingu (tzv. *hack back*), jímž bude narušena suverenita jiných států.[806]

Krajní nouze jako okolnost vylučující protiprávnost v oblasti vztahů mezi suverénními státy však budí kontroverze. Jak poukazuje Čepelka, problematická je situace, kdy se stát *„sám cítí být ve stavu krajní nouze, tj. pokládá sám sebe za závažně a bezprostředně ohroženého na svém podstatném zájmu a nemá podle vlastního posouzení absolutně žádný výběr prostředků, jak ochránit tento zájem, než právě k újmě jiného státu. Ten je však takto vzniklou situací zcela nevinen."*[807] Autor následně pokládá otázku, zda bude i v tomto případě dané chování zcela zbaveno protiprávnosti, resp. zda bude zbaveno jen odpovědnostního následku v podobě povinnosti nahradit vzniklou škodu? Podotýká, že krajní nouze je obvykle vnímána spíše jako nástroj politický, než právní.[808] I přes zmíněné kontroverze však lze krajní nouzi, s ohledem na obyčejový charakter i přijetí mezinárodními soudy, považovat za institut vztahující se také na kybernetické prostředí.[809]

Příčinou jednání v krajní nouzi může být vedle chování států i přírodní katastrofa či události nezávislé na vůli států. To umožňuje uplatnit institut krajní nouze i na kybernetické útoky a ohrožující kybernetické operace jednotlivců, teroristů, aktivistů a nejrůznějších skupin i neznámých útočníků, neboť jejich aktivity není nutné prve přičíst některému státu. Jednání v krajní nouzi proto může být jedinou přípustnou reakcí státu na kybernetický útok nestátního aktéra, který by nedosáhl hranice ozbrojeného útoku.[810]

2.4.5. *Hack-back*, aktivní kyberobrana

Termín *hack-back*, který by mohl být přeložen do českého jazyka poněkud neobratně jako „zpětný hacking",[811] naznačuje, že odpověď na kybernetický útok může využívat podobných technik jako útok samotný.[812] Zpětným hackingem se zabýval již roku 1999 Renee Albersheim, který popsal jeho cíl jako snahu nejen zmenšit škodu, ale i odradit útočníka poškozením jeho

---

[806] Tamtéž, bod 17. Ve vztahu k možné spolupráci s dalšími státy či mezinárodními organizacemi nepanuje shoda na tom, zda lze takovou spolupráci vzít v potaz jako alternativu jednání v krajní nouzi. Tamtéž, body 21 - 22.

[807] ČEPELKA, Čestmír. Op. cit., str. 72.

[808] Podrobněji tamtéž, str. 72 - 84.

[809] Tallinn Manual 2.0, Rule 26 - Necessity, bod 1.

[810] Tamtéž, body 9 - 11.

[811] Takovému překladu pojmu *hack-back* odpovídá i další anglický termín označující *hack-back*, jímž je *reverse hacking*.

[812] Některé techniky je přitom obtížné jednoznačně zařadit jako obranné nebo jako útočné. Podrobněji KOLOUCH, Jan. Op. cit., str. 181 a násl. nebo BANNELIER, Karine, CHRISTAKIS, Theodore. Op. cit., str. 62.

systému od dalších útoků.[813] Zpětný hacking se řídí pravidlem, podle něhož je nejlepší obranou útok. Lze se tak setkat i s eufemismem „aktivní kybernetická obrana", který se vyhýbá pejorativním konotacím, jež se pojí s hackingem.[814] Podstatou zpětného hackingu je, že se poškozený subjekt, který se stal obětí hackingu (či spíše crackingu), uchýlí k hackingu vůči původci prvotního útoku. S určitou nadsázkou tak lze říci, že se z oběti stává rovněž útočník.

Zpětný hacking není vhodné vnímat jako kategorii přípustných kybernetických operací, natož jako další okolnost vylučující protiprávnost v kyberprostoru. Zpětný hacking totiž může být součástí jednání státu v rámci sebeobrany, součástí protiopatření, či za stavu krajní nouze nebo tísně. Reaguje-li tudíž stát na kybernetický útok pomocí zpětného hackingu, musí jím zvolená kybernetická operace vždy respektovat daná ustanovení mezinárodního práva. Bude-li například stát zpětným hackingem odpovídat na porušení mezinárodního závazku jiným státem ve snaze donutit odpovědný stát k plnění závazku, musí respektovat limity institutu protiopatření rozebrané výše.

Nedostatečné kapacity některých států reagovat na kybernetické hrozby a ochránit fyzické i právnické osoby před kybernetickými útoky vedly k využívání zpětného hackingu i v řadách nestátních aktérů. Specializované právnické a fyzické osoby podnikající v oblasti kybernetické bezpečnosti tak nabízí nejen zabezpečení informačních a komunikačních systémů a sítí, tj. služby v rámci pasivní kybernetické obrany, nýbrž i metody atribuce útoků a služby aktivní kybernetické obrany, mezi které patří právě zpětný hacking.[815]

Podle některých umožňuje zpětný hacking vyhnout se zdlouhavým soudním či mimosoudním řízením, problematickému určení pravomoci, nedostatečně technicky vzdělaným soudcům či rozhodcům během sporného řízení, a představuje adekvátní a rychlou odpověď na útok v kyberprostoru, kde obvykle tradiční nápravné mechanismy selhávají.[816]

Častý hlavní argument podporující zpětný hacking popisuje veřejnou moc ve státě jako pomalou, neochotnou jednat v kyberprostoru a poskytnout v něm dostatečné záruky obětem kybernetických útoků. Podle tohoto argumentu státní moc není schopna dostatečně ochránit fyzické a právnické osoby před kybernetickými útoky, čímž je odůvodněn odklon od monopolu státního donucení a převzetí kybernetické (sebe)obrany do vlastních rukou. Lin poukazuje na nedostatečné

---

[813] ALBERSHEIM, Renee. The Legal Implications of Corporate Reverse Hacking. *Preventive Law Reporter*, vol. 18, 1999.

[814] Podrobněji BANNELIER, Karine, CHRISTAKIS, Theodore. Op. cit., str. 62.

[815] BANNELIER, Karine, CHRISTAKIS, Theodore. Op. cit., str. 59.

[816] MESSERSCHMIDT, Jan, E. Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm. *Columbia Journal of Transnational Law,* Vol. 52, No 1, 2013, str. 293.

působení práva v kyberprostoru, což připomíná primitivní stát. Hack-back podle něj pouze vyplňuje mezery tam, kam právo nedosáhne, a proto jej nepovažuje ani za narušení společenského řádu.[817] S tímto argumentem, jež připomíná osidlování Divokého západu po (znovu)objevení Severní Ameriky, nelze souhlasit z obdobných důvodů, pro které nelze rezignovat na působení práva v kyberprostoru.[818] Argument se zabývá nedostatky společenské smlouvy, spíše však jde o problém sebeobrany tam, kde ochrana ze strany státní moci přichází pozdě. Z hlediska přípustnosti zpětného hackingu by bylo možné se spíše ztotožnit s jiným argumentem založeným na právu každého bránit sebe a svůj majetek.[819]

Další argumenty podporující obecné zavedení možnosti zpětného hackingu hovoří zejména o rychlé a efektivní reakci na kybernetické útoky, která neponechává iniciativu pouze na útočnících, nýbrž využívá dostupnou technickou odbornost a sílu. Zpětný hacking také může umožnit zjištění klíčových informací o existenci dalších obětí útočníka a o útoku jako takovém nebo zabránit změnám zdrojových kódů, a tyto následně předat policejním orgánům.[820]

Zpětný hacking by měl mít rovněž významný odstrašující účinek pro potenciální útočníky do budoucna. Jestliže potenciální útočníci budou vědět, že se daná obchodní společnost uchyluje k protiútokům, které působí útočníkům vážné škody, útoku vůči ní se zdrží. Uvedený argument by měl být poplatný pro veřejnou i soukromou sféru, ponecháme-li stranou hledisko enumerativnosti veřejnoprávních pretencí a limity uplatňování státní moci. Poněkud úsměvná je však představa, podle níž by se např. Česká správa sociálního zabezpečení, narozdíl od jiných správních orgánů, běžně uchylovala k protiútokům, a tudíž by mezi hackery byla známa jako nebezpečný státní orgán, na jehož informační systémy se nevyplatí útočit. Odstrašující účinek zpětného hackingu však využívá například kybernetická strategie USA, které se potýkají s vysokým množstvím kybernetických útoků ze strany státem sponzorovaných hackerů ze zemí jako Rusko, Čína, Írán a Severní Korea. Americká legislativa dovoluje státním orgánům, nikoli však soukromé sféře, aby se uchýlila k aktivní kybernetické obraně. Současně se objevují názory, podle nichž by shodnou možnost obrany v USA měla mít k dispozici i soukromá sféra.[821]

---

[817] LIN, Patrick. *Ethics of Hacking Back: Six Arguments from Armed Conflict to Zombies* [online]. 26. 9. 2016, str. 9. Dostupné: http://ethics.calpoly.edu/hackingback.pdf [Cit. 2022-11-16].

[818] Srov. shora subkapitolu 1.4. Působení práva v kyberprostoru.

[819] LIN, Patrick. Op. cit., str. 10 - 12.

[820] Tamtéž, str. 13. Nebo BANNELIER, Karine, CHRISTAKIS, Theodore. Op. cit., str. 64.

[821] BAKER, Benjamin. *Considering the Potential Detterence Value of Legislation Allowing Hacking Back [online]*. May 22, 2018, str. 3 - 4. Dostupné: https://ssrn.com/abstract=3319530 [Cit. 2022-11-16].

Zpětný hacking zároveň umožňuje obchodním společnostem řešit slabiny v zabezpečení uvnitř společnosti a nezveřejňovat zranitelnosti svých systémů v kybernetickém zabezpečení. Uvedená strategie zaručuje lepší reputaci obchodních společností, jelikož nezveřejňování kybernetických útoků a incidentů na společnost nenaruší pověst obchodní společnosti u jejích klientů. Zvláště nepříznivé důsledky pro reputaci mají kybernetické útoky u bank, burz, společností podnikajících v oblasti kybernetické bezpečnosti a IT služeb, apod.[822]

Objevuje se rovněž argument, že zpětný hacking umožňuje obejít problémy jurisdikce bez nutnosti mezinárodní justiční spolupráce, respektive že řeší obtíže související s uplatněním státní moci mimo státní území.[823] S tímto argumentem však nelze souhlasit, jelikož samotný zpětný hacking nedostatky pravomoci vně státního území a problémy s narušením suverenity jiného státu neřeší, nýbrž je pouze nezohledňuje. Zpětný hacking, který stát provádí bez splnění podmínek sebeobrany, protiopatření, krajní nouze či tísně, bude porušením mezinárodního práva, přičemž taková kybernetická operace pravděpodobně vždy naruší i suverenitu jiného státu.

Mezi riziky uchylování se ke zpětnému hackingu patří hrozba eskalace konfliktu, který byl zpočátku zanedbatelný, jakož i hrozba destabilizace mezinárodního společenství.[824] Jestliže se nestátní aktéři na území různých států uchýlí opakovaně ke kybernetickým útokům vůči sobě navzájem, může konflikt získat politicky mezinárodní rozměr a narušit vzájemné vztahy obou států. Tím spíše, pokud budou mít oba státy tendenci nahlížet na zpětný hacking jako na kybernetickou operaci v krajní nouzi, následkem čehož budou považovat zásah do práv druhého státu za zcela oprávněný. S destabilizací mezinárodního společenství souvisí i některá další rizika, která zmiňují Bannelier a Christakis. Patří mezi ně ohrožení autority státu a jeho zahraniční politiky, jakož i ohrožení postihu trestné činnosti ze strany státních orgánů.[825]

Zejména posledně zmíněný argument ohrožení stíhání trestné činnosti lze považovat za zásadní pro vládu práva. Zpětný hacking totiž může znemožnit řádné vyšetření kybernetického útoku tím, že zničí klíčové důkazy, jež by mohly vést k odsouzení prvotního útočníka. Zpětný hacking rovněž může být nástrojem k zastření původního motivu útoku za pouhé jednání v aktivní kybernetické (sebe)obraně.

Nelze opomenout ani riziko chybné atribuce útoku a způsobení škod nevinným subjektům, ať již státním nebo soukromým. Nežádoucím dopadem by mohlo být i prohloubení nerovností mezi

---

[822] BANNELIER, Karine, CHRISTAKIS, Theodore. Op. cit., str. 65.

[823] Tamtéž, str. 66.

[824] Tamtéž, str. 67.

[825] Podrobněji k uvedeným argumentům srov. tamtéž, str. 68.

velkými obchodními společnostmi typu Google, které si mohou díky silnému technologickému kapitálu dovolit efektivní zpětný hacking, a středními a menšími obchodníky na trhu, kteří potřebnou technickou (i personální) kapacitu k provedení zpětného hackingu postrádají. Jak upozorňují Bannelier a Christakis, zmíněná nerovnost by mohla vést až k uplatňování elitářské kybernetické obrany, která představuje ve skutečnosti nekalé konkurenční praktiky.[826]

Se shora nastíněnými argumenty varujícími před neomezeným uplatňováním zpětného hackingu souhlasím a považuji je za převažující. Mezinárodní právní řád se vztahuje i na kyberprostor a jakákoli kybernetická operace, má-li být v souladu s ním, jej musí respektovat. Jestliže se stát či nestátní aktér uchýlí ke zpětnému hackingu, měl by být schopen obhájit před mezinárodním společenstvím, že jednal po právu.

2.4.6. Odpovědnost státu za mezinárodně protiprávní čin v kyberprostoru

„Je-li na základě shora uvedených pravidel dovozena mezinárodní odpovědnost státu za mezinárodně protiprávní chování v kyberprostoru, musí stát upustit od protiprávního chování a, je-li to vhodné, poskytnout ujištění a záruky, že se již nebude opakovat".[827] Poškozený stát se může vůči odpovědnému státu domáhat odčinění vzniklé újmy. Odpovědný stát je povinen zcela odčinit (*make full reparation*) újmy způsobené poškozenému státu mezinárodně protiprávním činem spáchaným kybernetickými prostředky.[828] Toto odčinění může nabývat podoby uvedení do původního stavu (*restitution*), odškodnění (*compensation*) i zadostiučinění (*satisfaction*).[829]

Úprava opět vychází z Návrhu článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování.[830] Poskytnutí ujištění a záruk není formulováno jako právní povinnost, avšak mělo by být nabídnuto tehdy, pokud se poškozený stát rozumně nemůže cítit ochráněný pouhým ukončením protiprávního chování. Jejich cílem je obnovení důvěry mezi oběma stranami konfliktu. Ujištění (*assurances*) odkazují na veřejná slovní prohlášení či sdělení, zatímco záruky (*guarantees*) neopakování míří na přijetí konkrétních opatření k zabránění opakování protiprávního chování. Kupříkladu porušil-li odpovědný stát povinnost náležité péče, pouhá slovní ujištění by nemusela být považována za dostačující; bude třeba přijmout konkrétní technické i legislativní

---

[826] Argument autoři nazývají jako riziko elitářské či pokrytecké kybernetické obrany. Srov. BANNELIER, Karine, CHRISTAKIS, Theodore. Op. cit., str. 70.

[827] Tallinn Manual 2.0, Rule 27 - Cessation, assurances, and guarantees. Překlad autorka.

[828] Tallinn Manual 2.0, Rule 28 - Reparation (general principle). Překlad autorka.

[829] Tallinn Manual 2.0, Rule 29 - Forms of reparation. Překlad autorka.

[830] Konkrétně z článků 30–31, 34–37, 42, 48 odst. 1.

změny, jež by odstranily zjištěné zranitelnosti kybernetické infrastruktury a zamezily jejímu zneužití do budoucna.[831]

Smyslem povinnosti odčinit způsobené újmy je v co nejvyšší míře odstranit následky protiprávního činu a obnovit situaci, jež by panovala, kdyby k protiprávnímu činu nebylo bývalo došlo.[832] Újma pokrývá jakoukoli materiální (hmotnou) újmu (tj. škodu) i imateriální (nehmotnou) újmu způsobenou mezinárodně protiprávní kybernetickou operací. Způsobený zásah do informačních služeb či ztráta dat obvykle povedou ke vzniku materiální újmy, která může postihnout nejen státní orgány a instituce, nýbrž i soukromou sféru ve státě (občané, obchodní korporace apod.). I takovou újmu je totiž nutno považovat za újmu způsobenou poškozenému státu, jejíhož odčinění se může po odpovědném státu domáhat. Ve vztahu ke státním orgánům uvádí Tallinn Manual 2.0 jako nehmotnou újmu např. ztrátu prestiže či narušení důvěry ve vládní instituce způsobené např. pozměněním informací uvedených na vládních webových stránkách.[833] Dalším příkladem nehmotné újmy by mohla být destabilizace politického prostředí a ztráta důvěry ve státní instituce vlivem manipulace probíhajících voleb skrze kybernetické operace, či znemožnění konání voleb v řádném termínu. Zajištění bezpečnosti, ale i autenticity hlasujících voličů a odevzdaných hlasů ve volbách jsou jedny z mnoha problematických aspektů, jež trápí řadu států při pokusech o plošné zavádění elektronických volebních systémů.[834]

Zásadní podmínkou pro odčinění je skutečnost, že újma musí být přímým následkem kybernetického protiprávního činu. Nepředvídatelné či příliš vzdálené následky nelze přičítat odpovědnému státu. To působí problémy zvláště v kyberprostoru, kde se snadno a rychle může šířit nejrůznější malware, přičemž mapování všech negativních dopadů je zpravidla obtížné. Poškozený stát by se měl rovněž pokusit o mírnění rozsahu újmy. Ačkoli mezinárodní právo neukládá žádnou takovou povinnost, rezignace na mírnění škod tam, kde to bylo snadno proveditelné (např. odpojením napadených systémů ze sítě), může ovlivnit rozsah poskytnutého odčinění, stejně jako nedbalostní či úmyslné jednání, kterým by poškozený stát přispěl ke škodě.[835]

---

[831] Tallinn Manual 2.0, Rule 27 - Cessation, assurances, and guarantees, body 4 - 6.

[832] Rozsudek Stálého dvora mezinárodní spravedlnosti v Haagu ze dne 26. 7. 1927, *Factory at Chorzów (Germany v. Poland)*, odst. 47. Dostupný: https://jusmundi.com/en/document/decision/en-factory-at-chorzow-jurisdiction-judgment-tuesday-26th-july-1927 [Cit. 2022-11-16].

[833] Tallinn Manual 2.0, Rule 28 - Reparation (general principle), body 2 - 3.

[834] Podrobněji k problémům a možnému řešení díky využití blockchainové technologie srov. SABHARWAL, Alakshendra, SAIFULLAH, Mohammad, GROVER, Priyanka, BATRA, Neha. Comparative Study of Blockchain Techniques in Electronic Voting System [online]. *Proceedings of the International Conference on Innovative Computing & Communication (ICICC) 202*1, July 11, 2021. Dostupné: https://ssrn.com/abstract=3884390 [Cit. 2022-11-16].

[835] Tamtéž, str. 6 - 9.

Konkrétní podoba odčinění vzniklé újmy závisí na okolnostech, jež mohou vést i k uplatnění více podob odčinění současně (vedle sebe).[836] Primární postavení zaujímá uvedení v předešlý stav. To však nelze automaticky směšovat s pouhým ukončením kybernetického útoku. Je-li k nepřátelské kybernetické operaci namířené vůči jinému státu zneužit škodlivý program, který již provedl v cílových počítačových systémech určité změny, nepostačí pouhé ukončení operace, nýbrž bude nutné zajistit poškozenému státu takové informace o programu, které umožní odstranění jeho následků (např. obnovení potlačených dat, odstranění sledovacích programů, apod.).[837] Jestliže nebude možné škodlivé následky odstranit, například z důvodu fyzického zničení sítě či počítačových systémů, anebo z důvodu výpadku služby v konkrétní čas, kdy bylo její poskytování z hlediska poškozeného státu zásadní, nebude uvedení v předešlý stav fakticky možné. V takovém případě bude na místě odškodnění, lze-li škodu vyjádřit v penězích, a zadostiučinění.[838]

Poskytnutí finančních náhrad v rámci odškodnění se vztahuje nejen na státní orgány, ale i na právnické a fyzické osoby nacházející se v jurisdikci poškozeného státu. Tallinn Manual 2.0 uvádí příkladem nejen nahrazení ušlého zisku z reklamy, která by byla zveřejněna na webové stránce, nebýt DDoS útoku, jež ji vyřadil z provozu, ale i kompenzaci trvale snížené hodnoty národních společností vlivem kybernetického útoku, když dovozuje paralelu s právem životního prostředí a přiznáním náhrad za ztracenou hodnotu a nutnou sanaci v místě.[839] Ačkoli může být inspirace mezinárodním právem z oblasti ochrany životního prostředí podnětná, nedomnívám se, že srovnání je zde vhodné. Zhoršení životního prostředí nelze přirovnávat ke zhoršené pověsti či postavení obchodních společností. Zatímco na příznivém životním prostředí je dán veřejný zájem, který stát má chránit, u pověsti obchodních společností jde předně o ochranu soukromých zájmů. Příznivé a zdravé životní prostředí je veřejný statek, z něhož benefitují všichni jednotlivci ve státě, včetně budoucích generací. I kdyby se nejednalo o běžnou soukromou obchodní společnost, nýbrž o veřejný podnik, okruh beneficientů bývá u veřejného podniku stejně mnohem užší. Těžko představitelný je i způsob, jak objektivně vyjádřit ztracenou důvěru v takový podnik v penězích.

Zadostiučinění pak zahrnuje uznání, že byl spáchán mezinárodně protiprávní čin a vyjádření lítosti nad ním, omluvu, jakož i jiné vhodné způsoby jednání státu.[840] V případě, že došlo ke spáchání protiprávního činu překročením pravomoci úředníka, jehož jednání bylo přičteno státu, lze

---

[836] Čl. 34 Návrhu článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování.

[837] Tallinn Manual 2.0, Rule 29 - Forms of reparation, body 2 - 3.

[838] Tamtéž, bod 5.

[839] Tamtéž, bod 7.

[840] Čl. 37 odst. 2 Návrhu článků Komise OSN pro mezinárodní právo o odpovědnosti států za protiprávní chování.

nahlížet na následné vyšetřování a potrestání jeho pochybení rovněž jako na určitou formu zadostiučinění.[841] Zadostiučinění bude na místě zejména tehdy, vedl-li kybernetický útok ke vzniku nehmotné újmy, anebo nejeví-li se uvedení do původního stavu ani odškodnění jako dostačující.[842]

[841] Tallinn Manual 2.0, Rule 29 - Forms of reparation, bod 10.

[842] Tamtéž, bod 9.

3. Zákon o kybernetické bezpečnosti

3.1. Nová právní úprava kybernetické bezpečnosti

3.1.1. Okolnosti a důvody přijetí nové právní úpravy[843]

Roku 2014, kdy v České republice došlo k přijetí zákona o kybernetické bezpečnosti, byly pojmy kybernetika[844] a kybernetická bezpečnost pro značnou část veřejnosti neznámé. Nová právní úprava reagovala na vzrůstající výskyt incidentů v kybernetickém prostředí, jež měly zásadní dopad na soukromou i veřejnou sféru a otevřela cestu pro uplatňování státní moci v kyberprostoru v souladu s ústavněprávními požadavky.

Závislost lidské společnosti na informačních a komunikačních technologiích narůstající během posledních desetiletí se týká soukromého i veřejného sektoru. O společenských změnách, jež se pojí s digitální revolucí, i o hodnotách informační společnosti pojednala první část práce. S ohledem na narůstající využívání ICT veřejnou správou při poskytování řady základních služeb v oblasti dopravy, sociálního zabezpečení, zdravotnictví, přenosu energií, evidence obyvatel, a dalších, jakož i vzhledem k souvisejícímu nárůstu kriminálních příležitostí,[845] bylo zapotřebí zabezpečit před kybernetickými útoky i kritickou infrastrukturu státu.[846]

Před přijetím ZKB vycházel soukromý sektor v oblasti zabezpečení informací většinou z různých bezpečnostních doporučení či standardů.[847] Z pohledu státní moci však neexistoval žádný zákon, na jehož základě by byl stát oprávněn v případě ohrožení kybernetické bezpečnosti uložit související povinnosti.[848] Z hlediska ústavního principu vázanosti státní moci zákonem a požadavku ukládání povinností soukromoprávním subjektům pouze zákonem[849] bylo nutné upravit problematiku kybernetické bezpečnosti právní úpravou na zákonné úrovni.

---

[843] Text je součástí práce autorky odevzdané v rámci XI. ročníku Studentské vědecké odborné činnosti na Právnické fakultě Univerzity Karlovy. RADEMACHEROVÁ, Kristina. *Principy a východiska kybernetické bezpečnosti de lege lata*. Op. cit., str. 6 - 7, 11 - 13.

[844] Podrobněji viz shora kapitola 1.2 Hodnoty informační společnosti. Kybernetika je nauka o řízení organismů a strojů, která podnítila rozvoj informatiky a jejíž zrod je spjat s r. 1948, kdy Norbert Wiener vydal dílo „Cybernetics, or Control and Communication in the Animal and Machine", tj. „Kybernetika, čili řízení a komunikace u živočichů a ve stroji". KNAPP, Viktor a kol. *Právo a informace.* Op. cit., str. 14 a násl.

[845] Srov. např. GRABOSKY, Peter. Op. cit., str. 243–249. WALL, David. Op. cit., str. 44–48.

[846] Za zvláště zranitelné jsou považovány řídící systémy v energetice a dopravě, jakož i informační systémy veřejné správy. Srov. Důvodovou zprávu k ZKB. Op. cit., str. 2.

[847] Viz standardy ISO/IEC 20000 a ISO/IEC 27000.

[848] Důvodová zpráva k ZKB. Op. cit., str. 4.

[849] Srov. čl. 2 odst. 3, odst. 4 Ústavy ČR a čl. 2 odst. 2, odst. 3 Listiny základních práv a svobod.

Problematikou uplatňování práva v kyberprostoru, zejména ochranou základních lidských práv a svobod na Internetu, jakož i ochranou před nežádoucími jevy, mezi něž patří kybernetická trestná činnost, terorismus, kybernetické bezpečnostní incidenty a útoky, se dlouhodobě zabývala řada mezinárodních organizací. Impulzem k přijetí nové právní úpravy se staly závazky ČR vůči EU i NATO.

Na půdě NATO bylo téma kybernetické obrany poprvé projednáváno na Pražském summitu roku 2002. Většího významu získaly kybernetická bezpečnost i kybernetická obrana[850] teprve po kybernetických útocích na estonskou infrastrukturu v roce 2007 a po rusko-gruzínském válečném konfliktu v roce 2008, jehož součástí byl kybernetický útok.[851] Nyní cílí NATO na posílení výměny informací a vzájemnou pomoc při prevenci, odražení a reparaci kybernetických útoků.

V rámci EU byl kladen důraz především na ochranu soukromí a osobních údajů.[852] Do popředí zájmu se však v posledních letech dostává právě téma posílení bezpečnosti kyberprostoru členských států, a to především vyšším zabezpečením informačních infrastruktur a prevencí počítačové trestné činnosti.[853] Počátkem roku 2013 Evropská komise předložila v rámci *Strategie kybernetické bezpečnosti: otevřený, bezpečný a chráněný kyberprostor*, návrh směrnice NIS, na jejímž základě měly členské státy zejména přijmout národní strategii pro bezpečnost sítí a informací, určit odpovědný orgán a zřídit CERT, skupinu odpovědnou řídit reakce na kybernetické hrozby.[854] ČR zčásti reagovala novou právní úpravou kybernetické bezpečnosti na politiku EU. V den přijetí směrnice NIS, tj. 6. 7. 2016, ovšem byla ČR jedním z prvních členských států, který již měl vlastní komplexní úpravu národní kybernetické bezpečnosti.[855]

Další mezinárodní organizace se stěžejním významem v evropské geografické oblasti, Rada Evropy, dlouhodobě apelovala především na zajištění svobody projevu a informační svobody v

---

[850] K vysvětlení obou pojmů srov. shora kapitolu 2.1. Kybernetická bezpečnost a kybernetická obrana jako úloha státu.

[851] K vývoji kybernetické obrany srov. NATO. *Cyber defence*. Op. cit., dále NATO. *NATO Summit Guide, Warsaw 2016*. Op. cit., str. 128. K estonskému incidentu srov. PAVLIKOVÁ, Miroslava. Op. cit.

[852] Srov. směrnici Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích).

[853] Srov. směrnici Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu (Text s významem pro EHP); nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu; směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii; nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center.

[854] Důvodová zpráva k ZKB. Op. cit., str. 2.

[855] POLČÁK, Radim. Kybernetická bezpečnost jako aktuální fenomén českého práva. Op. cit., str. 95.

prostředí veřejné počítačové sítě,[856] jakož i na prevenci kybernetické kriminality, skrze níž se Rada Evropy dotýká tématu bezpečnosti kybernetického prostředí. Na půdě Rady Evropy byla přijata Úmluva o počítačové kriminalitě, dosud jediná mezinárodní smlouva široce zaměřená na postih počítačové (kybernetické) kriminality v celosvětovém měřítku.[857]

V ochraně svobody projevu, soukromí a informačního sebeurčení na straně jedné, a v zajištění kybernetické bezpečnosti na straně druhé, lze vidět základní, a do určité míry konkurující východiska regulace kyberprostoru. Česká právní úprava se snaží o jejich skloubení. Posílení pravomocí státních orgánů by mělo zajistit vyšší úroveň kybernetické bezpečnosti, aniž by právní úpravou byl dotčen obsah přenášené komunikace.[858] Do jaké míry bude soulad požadavků svobody a bezpečnosti možný, ukáže vývoj regulace a využití pravomocí státních orgánů při zajišťování bezpečnějšího kyberprostoru.

3.1.2. Východiska právní úpravy, vztah ke směrnici NIS[859] [860]

Základním smyslem nové právní úpravy kybernetické bezpečnosti v ČR byla prevence vzniku kybernetických bezpečnostních incidentů pomocí systému bezpečnostních opatření. Svým způsobem se právní úprava podobá virtuální protipožární ochraně, kde požárem je ohrožení existence a funkčnosti informační infrastruktury. Lze se však setkat i s názorem, podle něhož nemá legislativní řešení kybernetické bezpečnosti v platném právu srovnatelné obdoby, a to ani v bezpečnostně-technických oborech.[861]

Polčák chápe jedinečnost právní úpravy v akcesoritě hodnocení bezpečnosti, v orientaci na proces, v nekonfliktním spojení veřejného a soukromého zájmu i v působení definičních autorit.

---

[856] COUNCIL OF EUROPE. *Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet* [online]. Dostupné: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2f8 [Cit. 2022-11-18]. COUNCIL OF EUROPE. *Declaration of the Committee of Ministers on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers* [online]. Dostupné: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805cb844 [Cit. 2022-11-18].

[857] Srov. shora kapitolu 2.3.5.1. Úmluva o počítačové kriminalitě. K pojmům počítačová a kybernetická kriminalita srov. poznámku pod čarou č. 42.

[858] Podrobněji srov. rozbor principů práva kybernetické bezpečnosti shora, zejména kapitolu 1.3.3.1. Technologická neutralita.

[859] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

[860] Text je součástí práce autorky odevzdané v rámci XI. ročníku Studentské vědecké odborné činnosti na Právnické fakultě Univerzity Karlovy. RADEMACHEROVÁ, Kristina. *Principy a východiska kybernetické bezpečnosti de lege lata*. Op. cit., str. 13 - 15.

[861] FREDLAND, John S. Op. cit., str. 26.

Hodnocení bezpečnosti počítačových systémů a sítí podle něj získává akcesorickou povahu tím, že k němu dochází teprve v návaznosti na účel konkrétního systému či sítě. Právní úpravu kybernetické bezpečnosti považuje orientovanou na proces vzhledem k zajišťování ochrany informačních procesů.[862]

Souhlasit lze s jedinečností právní úpravy z hlediska akcesorické povahy hodnocení bezpečnosti (tentýž model počítačového systému může být využíván k domácím aktivitám i ke komunikaci s evidenčním informačním systémem obsahujícím citlivá data), jakož i s fenoménem definičních autorit, který je typický pro celou oblast ICT.[863] Problematická je však jedinečnost právní úpravy spočívající v její orientaci na proces. Objektem právní úpravy není vždy konkrétní předmět. Může jím být i sám proces, resp. cokoli, co za objekt regulace určí právní norma. Výlučně procesně orientovanou právní úpravu lze nalézt i v jiných oblastech, kde dochází k regulaci určitých lidských aktivit či automatizovaných procesů. Příkladem může být zajištění důvěrnosti elektronických transakcí a z tohoto pohledu výlučně procesně orientovaný zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů.

Smyslem české právní úpravy je ochrana veřejného zájmu na nepřetržitém fungování služeb informační společnosti, jakož i ochrana práva člověka na informační sebeurčení. Mezi základní principy právní úpravy kybernetické bezpečnosti uvádí Důvodová zpráva k ZKB technologickou neutralitu, ochranu informačního sebeurčení člověka, ochranu nedistributivních práv, minimalizaci státního donucení, autonomii vůle regulovaných subjektů a princip bdělosti ve vztahu k ostatním státům i k mezinárodnímu společenství.[864] O principech právní úpravy kybernetické bezpečnosti bylo již pojednáno shora.[865]

Na úrovni EU si právní úprava klade za cíl posílit bezpečný kyberprostor zejména skrze vzájemnou spolupráci a výměnu klíčových informací. Základním předpisem je směrnice NIS,[866] jež vedla i k podstatné novelizaci ZKB,[867] a která vychází z premisy, podle níž vysoká společná úroveň

---

862 POLČÁK, Radim, HARAŠTA, Jakub, STUPKA, Václav. *Právní problémy kybernetické bezpečnosti*. Op. cit., str. 12–14.

863 Definiční autority určují uživatelům skrze technologické řešení faktické možnosti chování, čímž vytváří technickou normu, tj. kód. Podrobněji LESSIG, Lawrence. Op. cit. Působení definičních autorit bylo rozebráno též shora v podkapitole 1.3.3.4. Minimalizace státního donucení.

864 Důvodová zpráva k ZKB. Op. cit., str. 47 - 48.

865 Viz kapitola 1.3. Principy a východiska kybernetické bezpečnosti.

866 Viz kapitola 2.3.5.4. Směrnice EU o bezpečnosti sítí a informačních systémů.

867 Změny zapracoval zákon č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony.

bezpečnosti sítí a informačních systémů může být dosažena spíše na unijní úrovni než u jednotlivých členských států. Tím odůvodňuje přijetí regulace v souladu se zásadou subsidiarity v čl. 5 Smlouvy o EU.[868] Užší mezinárodní spolupráce má být zaměřena na zdokonalení bezpečnostních norem a výměnu informací. Zprostředkovat ji má i podpora Agentury ENISA.[869]

V mezinárodní spolupráci a sdílení informací lze spatřit další princip právní úpravy kybernetické bezpečnosti na úrovni EU, který zákonodárce ve vztahu k ZKB výslovně neuvádí. Dalším východiskem, který zmiňují směrnice NIS i ZKB, byť jej důvodová zpráva výslovně nejmenuje, je též spolupráce mezi veřejným a soukromým sektorem.[870] Spolupráce je zcela nezbytná s ohledem na to, že většinu sítí a informačních systémů v EU provozují soukromé subjekty. Oba právní předpisy kladou důraz i na sdílení informací s veřejností.[871] Na rozdíl od ZKB je však smyslem směrnice NIS zajistit hladké fungování vnitřního trhu, ochranu spotřebitelů a podniků v členských státech, a usnadnit přeshraniční pohyb zboží, služeb i osob. Protože má směrnice NIS zajistit v členských státech minimální standard, vztahuje se pouze na provozovatele základních služeb a poskytovatele digitálních služeb, a z orgánů veřejné správy jí podléhají jen ty, které provozují základní službu.[872] Působnost ZKB je s ohledem na § 3 ZKB širší, neboť ukládá povinnosti i jiným orgánům a osobám. Zajištění ochrany toliko veřejných informačních systémů český zákonodárce zjevně nepovažoval za dostatečně efektivní.[873]

Lze uzavřít, že ZKB zapracovává požadavky směrnice NIS týkající se zabezpečení sítí a informačních systémů v EU a je také úzce provázán s ochranou elektronických komunikací v ZEK. Cílem právní úpravy je tedy bezpečný přenos i ochrana obsahu dat, potažmo informací v kyberprostoru. Informační bezpečnosti se má dosáhnout zajištěním důvěrnosti, integrity a dostupnosti informací a dat.[874]

---

[868] Srov. recitál 74 směrnice NIS.

[869] Srov. recitály 43 a 66 a čl. 1 odst. 2 písm. b), c), e), čl. 7 odst. 2, čl. 8, čl. 11 a čl. 14 odst. 5 směrnice NIS.

[870] Srov. recitál 35 směrnice NIS či § 8, § 9 a § 20 ZKB, ohledně hlášení kybernetických bezpečnostních incidentů, sdílení údajů z evidence i poskytování metodické podpory a pomoci i součinnosti ze strany NÚKIB.

[871] Srov. recitál 40 a čl. 14 odst. 6 směrnice NIS a § 12 ZKB, týkající se varování o hrozbách kybernetické bezpečnosti.

[872] Srov. např. recitály 1–6 a 44 směrnice NIS. Kritéria pro určení provozovatele základní služby stanoví čl. 5 odst. 2 směrnice NIS.

[873] Důvodová zpráva k ZKB. Op. cit., str. 22–23.

[874] § 2 písm. c) ZKB.

3.1.3. Vývoj právní úpravy

ZKB nabyl účinnosti 1. 1. 2015. Jeho cílem bylo stanovit podmínky spolupráce mezi soukromým sektorem a veřejnou správou za účelem vyšší efektivity řešení kybernetických bezpečnostních incidentů. Zákon rovněž nově zavedl povinnosti fyzickým a právnickým osobám s cílem zvýšit bezpečnost kybernetického prostředí, které určil jako *„digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací"*.[875] Věcná působnost zákona je vymezena oblastí kybernetické bezpečnosti,[876] s výjimkou informačních a komunikačních systémů nakládajících s utajenými informacemi.[877] Zákon vymezil i pravomoc ústředního orgánu státní správy[878] - Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) v souvislosti s právy a povinnostmi dalších veřejnoprávních i soukromoprávních subjektů participujících na zajišťování kybernetické bezpečnosti.

ZKB však není jediným právním předpisem, který upravuje kybernetickou bezpečnost. Další zákony se zaměřují na specifické oblasti a jejich ustanovení jsou zpravidla v poměru speciality k ustanovením ZKB. Jde o zákon č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů (dále „ZEK"), nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, spolu s prováděcím zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů, a zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále „zákon o ochraně utajovaných informací)".

Příkladem zvláštních ustanovení je ochrana informačních a komunikačních systémů nakládajících s utajovanými informacemi, v § 33a - 35a zákona o ochraně utajovaných informací. Zvláštní ustanovení pokrývají i zpracování utajovaných informací, jež jsou sice v elektronické podobě, ale mimo informační a komunikační systém, a kryptografickou ochranu.[879] Zvláštní ustanovení, jež souvisí s ochranou bezpečnosti utajovaných informací a bezpečnosti státu v

[875] § 2 písm. a) ZKB.

[876] K vymezení kybernetické bezpečnosti viz kapitola 2.1. Kybernetická bezpečnost a kybernetická obrana jako úloha státu.

[877] § 1 odst. 3 ZKB.

[878] Srov. § 2 bod 16 zákona České národní rady č. 2/1969 Sb. o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění pozdějších předpisů.

[879] Srov. § 36 - 45 zákona o ochraně utajovaných informací.

působnosti NÚKIB nalezneme i v krizovém zákoně.[880] Na ústavní úrovni se kybernetické bezpečnosti teoreticky dotýká i nadřazený právní předpis - ústavní zákon o bezpečnosti ČR. Uplatní se v případech splnění stanovených podmínek pro vyhlášení nouzového stavu, stavu ohrožení státu nebo válečného stavu.[881] ZKB pak obsahuje zvláštní ustanovení např. ve vztahu k zákonu č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů. Zakazuje poskytnutí informací, jejichž zpřístupnění by mohlo ohrozit kybernetickou bezpečnost nebo účinnost bezpečnostního opatření. Neposkytují se ani informace z evidence kybernetických bezpečnostních incidentů umožňující určit toho, kdo incident ohlásil.[882]

Ještě před transpozicí směrnice NIS tak existovala v ČR komplexní právní úprava kybernetické bezpečnosti. V roce 2017 došlo k rozsáhlé novelizaci ZKB, provedené zákonem č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), který transponoval do českého právního řádu směrnici NIS. Jejím vlivem se dostaly pod režim ZKB i dosud neregulované subjekty. ZKB tak stanovil povinnosti k zabezpečení informačních systémů a sítí elektronických komunikací stěžejních pro poskytování základních služeb a digitálních služeb.[883] Stanovením povinností na poli kybernetické bezpečnosti novela cílila k tomu, aby ČR dostála požadavkům principu náležité péče (*due diligence*)[884] a minimalizovala zneužívání počítačových systémů a sítí na státním území ke kybernetickým útokům vůči cizím státům, a tím i vznik povinnosti nahradit takto způsobenou škodu.[885]

Do současné doby byl ZKB novelizován celkem osmkrát. Novelizace souvisely zejména s nutným implementováním požadavků stanovených právními předpisy EU. Mezi novelizacemi dotčené oblasti patřily především ochrana osobních údajů a úprava předávání dat, provozních údajů

---

[880] Podle § 33 krizového zákona mohou orgány krizového řízení kontrolovat dodržování krizového zákona a prováděcích předpisů v zařízeních NÚKIB, pokud by při kontrole mohlo dojít k ohrožení utajovaných informací nebo bezpečnosti státu, jen se souhlasem ředitele.

[881] Srov. čl. 2 ústavního zákona o bezpečnosti ČR.

[882] § 10a ZKB.

[883] Vláda ČR. Důvodová zpráva k zákonu č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony, č. 205/2017 Dz, str. 2 - 3.

[884] K principu *due diligence* srov. zejména podkapitolu 2.4.1.1. Princip náležité péče (*due diligence*).

[885] Vláda ČR. Důvodová zpráva k zákonu č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony, č. 205/2017 Dz, str. 5.

a informací,[886] ochrana funkčnosti digitálních služeb v prostředí EU, elektronizace veřejné správy a zabezpečení služeb cloud computingu,[887] evropské certifikáty kybernetické bezpečnosti,[888] ale i složení zvláštního kontrolního orgánu Poslanecké sněmovny Parlamentu ČR.[889] Za nejvýznamnější a nejrozsáhlejší novelizaci ZKB lze považovat již zmíněnou transpozici směrnice NIS s cílem zvýšit bezpečnost sítí a informačních systémů napříč EU.[890]

NÚKIB vznikl k 1. 8. 2017 s účinností novely provádějící směrnici NIS.[891] Prvotně bylo orgánem státní správy na poli kybernetické bezpečnosti Národní centrum pro kybernetickou bezpečnost (dále „NCKB"). Jednalo se o specializované pracoviště NBÚ sídlící v Brně, jež vzniklo na základě usnesení vlády ČR ze dne 19. 10. 2011.[892] Úlohou NCKB byla od počátku koordinace spolupráce na národní i mezinárodní úrovni při předcházení kybernetickým útokům a řešení kybernetických incidentů i útoků. Technickou součástí byl už vládní CERT, který se zabýval bezpečnostními incidenty, podílel se na výměně informací se zahraničními týmy, věnoval se vzdělávání a analýze dat, ale též upozorňoval například na chybné zabezpečení.[893] NÚKIB je již, narozdíl od NCKB, samostatným ústředním správním úřadem, stejně jako NBÚ, s nímž sdílí působnost v oblasti ochrany utajovaných informací.[894] Odpovídají tomu i novelizacemi postupně rozšiřované pravomoci NÚKIB, jimiž má zajistit bezpečný kyberprostor v rámci ČR, a tím ostatně i v rámci EU. O vybraných pravomocích úřadu bude pojednáno níže.

---

[886] Zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů, jakož i zákon č. 104/2017 Sb., kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a některé další zákony.

[887] Zákon č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci, ale i zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů.

[888] Zákon č. 226/2022 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.

[889] Zákon č. 35/2018 Sb., o změně některých zákonů upravujících počet členů zvláštních kontrolních orgánů Poslanecké sněmovny.

[890] Zákon č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony.

[891] Srov. Část čtvrtou zákona č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb.

[892] VLÁDA. Usnesení č. 781 ze dne 19. října 2011 o ustavení NBÚ gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. Přílohou usnesení byl i Statut Rady pro kybernetickou bezpečnost.

[893] ŠMÍD, Jaroslav. Implementace ZKB [online]. *Egovernment*. Praha: info*com, 2015, č. 2, str. 8. Dostupné: https://www.egovernment.cz/soubor/2015-2/ [Cit. 2022-11-20].

[894] § 21a odst. 1 ZKB a § 2 zákona č. 2/1969 Sb. o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky.

3.2. Systém zajištění kybernetické bezpečnosti

ZKB je právním předpisem, který budou mnozí (nejen právníci) číst s obtížemi. Připomíná lékopis plný definic a cizích pojmů, který by čtenář dobrovolně nečetl, nebyl-li by k tomu při nemoci donucen ve snaze nalézt vhodný lék. ZKB obsahuje široké množství popisných norem, definic a požadavků, v nichž se lze snadno ztratit. Řada slovních spojení v zákoně působí nepříliš srozumitelně. Důvodem je z části nutné propojení právního předpisu se světem informační a výpočetní techniky, technicko-bezpečnostními pojmy a oblastí norem krizového řízení, zčásti snad i transpozice právních předpisů EU do českého právního řádu, která může vést (z důvodu překladu) k použití méně srozumitelných českých výrazů.

Kybernetickou bezpečnost se zákon snaží zajistit tím, že ukládá povinnosti těm orgánům a osobám, jež by mohly být z důvodu poskytovaných a zajišťovaných služeb informační společnosti, popřípadě vzhledem ke spravování kritických informačních infrastruktur, zvláště zranitelné vůči kybernetickým hrozbám, a jejichž napadení by zároveň mohlo ohrozit i další osoby a instituce ve státě. Okruh povinných osob stanoví ZKB taxativně.[895] Vzhledem k dosavadnímu rozšiřování povinných subjektů, jakož i s ohledem na nárůst počtu systémů ICT, lze očekávat, že tento okruh bude i do budoucna narůstat.[896] O významný nárůst povinných subjektů se zaslouží i očekávaná směrnice NIS2, jejímž vlivem se dostane pod režim ZKB v ČR více než 6000 subjektů, namísto dosavadních přibližně 400.[897] Z hlediska poskytování právních služeb se povinnostem nevyhnou kupříkladu ani advokátní kanceláře. O povinnostech advokáta na poli kybernetické bezpečnosti podrobněji hovoří např. Brauner, který upozorňuje: *„Bylo by omylem se domnívat, že informační bezpečnost se týká pouze povinných subjektů uvedených v zákoně o kybernetické bezpečnosti a několika málo velkých advokátních kanceláří. Povinnosti na úseku informační bezpečnosti má totiž každý advokát, který zpracovává klientská data."*[898]

Stát tedy prostřednictvím zákona zajišťuje prevenci před narušením bezpečnosti informací v informačních systémech, bezpečnosti služeb a bezpečnosti a integrity sítí elektronických komunikací. Děje se tak pomocí relativně široké škály institutů v zákoně označených jako opatření. Mimo tato opatření NÚKIB přispívá ke zlepšení kybernetické bezpečnosti neformální vzdělávací

---

[895] Srov. zejména § 3 a § 3a ZKB.

[896] Počet systémů spadajících pod ZKB se bude zvyšovat i v následujících letech. NÚKIB. *Koncepce rozvoje Národního úřadu pro kybernetickou a informační bezpečnost* [online]. 2020, str. 10. Dostupné: https://www.nukib.cz/download/publikace/strategie_akcni_plany/Koncepce_rozvoje_NUKIB.pdf [Cit. 2022-11-21].

[897] NÚKIB. *NÚKIB představuje evropskou směrnici NIS2*. Op. cit.

[898] BRAUNER, Jan. Dopady technologického vývoje na povinnosti advokáta na úseku kybernetické bezpečnosti. *Bulletin advokacie*, 2022, č. 6, str. 18 a násl.

činností a uveřejněnými doporučeními, metodikami, podpůrnými návody, analýzami a mnoha dalšími dokumenty, které jsou dostupné na webových stránkách zmíněného správního úřadu.[899] Naplňuje tím svoji úlohu na poli prevence, vzdělávání i monitoringu, která je mu svěřena zákonem.[900]

Činnost v zákoně nazvanou „opatření" lze vnímat buď v rámci obecné prevence (viz bezpečnostní opatření organizační a technická ve smyslu §§ 4 až 6 ZKB), anebo jako činnost v rámci konkrétní prevence, pokud si tato klade za cíl přispět k ochraně před kybernetickou hrozbou, která již nastala (viz varování podle § 12 ZKB a povinnost předat data podle § 15a ZKB). Dále existují opatření již reagující na konkrétní kybernetický bezpečnostní incident (viz reaktivní opatření a ochranné opatření podle § 13 až 14 ZKB). V rámci kontroly při zjištění nedostatků dále lze uložit nápravné opatření upravené v § 24 ZKB. Je tedy patrné, že se jedná o širokou škálu úkonů, které správní orgán vykonává ve snaze vyhnout se hrozbě v oblasti kybernetické bezpečnosti, ve snaze na ni reagovat, anebo zamezit jejímu opakování, pokud již pominula.

Opatření k zajištění kybernetické bezpečnosti představují různorodou správní činnost, která je z hlediska odborné literatury opomíjenou oblastí.[901] Přehled a základní charakteristiky opatření ukládaných na základě ZKB se objevují nejčastěji v reklamních dokumentech podnikajících fyzických a právnických osob, jež nabízejí klientům služby z oblasti kybernetické bezpečnosti, včetně dosažení souladu s požadavky ZKB, neboť zákon umožňuje správní postih v případě jejich

---

[899] Srov. např. NÚKIB. *Doporučení k používání protokolu TLP ke sdílení chráněných informací* [online]. 10. 8. 2022. Dostupné: https://www.nukib.cz/cs/infoservis/doporuceni/ [Cit. 2022-10-05]. Nebo NÚKIB. *Bezpečná práce na dálku - doporučení pro firmy i zaměstnance* [online]. 20. 5. 2020. Dostupné: https://www.nukib.cz/cs/infoservis/doporuceni/ [Cit. 2022-10-05].

[900] Podle § 22 písm. j) ZKB zajišťuje NÚKIB prevenci, vzdělávání a metodickou podporu v oblasti kybernetické bezpečnosti a ve vybraných oblastech ochrany utajovaných informací, podle písm. u) téhož ustanovení provádí analýzu a monitoring kybernetických hrozeb a rizik.

[901] Výjimkou je článek Jakuba Klodwiga o varování NÚKIB: KLODWIG, Jakub. *Varování NÚKIB v systematice zákona o kybernetické bezpečnosti a možnosti jeho zohlednění v zadávacím řízení* [online]. Revue pro právo a technologie, 2021, č. 23, str. 49-75. Reaktivních a ochranných opatřeních se dotýká článek Jakuba Vostoupala o posuzování shody: VOSTOUPAL, Jakub. *Certifikace kyberbezpečnostních technologií* [online]. Revue pro právo a technologie, 2019, č. 20, str. 147-268. Článek Radima Polčáka rozebírá zavedení právní úpravy kybernetické bezpečnosti v ČR: POLČÁK, Radim. *Kybernetická bezpečnost jako aktuální fenomén českého práva** [online]. Revue pro právo a technologie, 2015, č. 11, str. 95-149. Dostupné: https://journals.muni.cz/revue/article/view/2980 [Cit. 2022-09-21]. Z hlediska soudní praxe se problematiky bezpečnostních opatření okrajově dotýká i rozsudek Nejvyššího správního soudu ze dne 6. 3. 2019, č. j. 2 As 153/2018-31. Komentář k ZKB od Martina Maisnera a Barbory Vlachové z převážné míry vychází z důvodové zprávy k zákonu: MAISNER, Martin. VLACHOVÁ, Barbora. *Zákon o kybernetické bezpečnosti: Komentář*. Praha: Wolters Kluwer, 2015.

nesplnění.[902] Proto budou jednotlivá zákonem stanovená opatření níže rozebrána a pojednáno bude rovněž o dosud vydaných opatřeních ze strany NÚKIB. Ta se však nevztahují k informačním a komunikačním systémům nakládajícím s utajovanými informacemi, neboť tyto jsou vyloučeny z působnosti zákona[903] a podléhají utajení.[904]

3.2.1. Bezpečnostní opatření (§§ 4 a 5 ZKB)

ZKB poprvé užívá pojem opatření hned v úvodu Hlavy II: Systém zajištění kybernetické bezpečnosti. Bezpečnostním opatřením se tu rozumí *„souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru."*[905] Zákon ukládá soukromým osobám zahrnutým do soustavy kritické informační infrastruktury, významných informačních systémů či informačních systémů základní služby, povinnost zavést a provádět bezpečnostní opatření v nezbytném rozsahu a vést o nich také bezpečnostní dokumentaci; bezpečnostní požadavky musí tyto osoby rovněž zohlednit při výběru svých dodavatelů informačních a komunikačních systémů.[906]

Smyslem opatření je zajistit bezpečnost informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury, informačního systému základní služby a významného informačního systému. Vhodná a přiměřená bezpečnostní opatření jsou povinni zavést a provádět také poskytovatelé digitálních služeb. Vedle soukromých osob zákon ukládá povinnost zohlednit a zajistit dodržování bezpečnostních pravidel i orgánům veřejné moci, a to ve vztahu k uzavírání smluv o poskytování služeb cloud computingu.[907]

---

[902] Srov. např. DELOITTE. *Soulad se zákonem o kybernetické bezpečnosti* [online]. Dostupné: https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/technology/cz_soulad_se_zakonem_o_kyberneticke_bezpecnosti.pdf [Cit. 2022-11-21]. CYBERSECURITY. *Braňte se kybernetickým hrozbám. Systematicky a účinně: komplexní řešení kybernetické bezpečnosti pro vaši společnost* [online]. Dostupné: https://www.cybersecuritycompliance.cz/?gclid=CjwKCAjwyaWZBhBGEiwACslQo82pLjca7QhC7WRlN9J8pHsmvNgBJayp-GsY8hs2dTyUdWPcPBHiTRoCNR0QAvD_BwE [Cit. 2022-11-21]. ACRESIA. *Implementace ZKB* [online]. Dostupné: https://www.acresia.com/index.php/sluzby/68-implementace-zakona-o-kyberneticke-bezpecnosti [2022-11-21].

[903] § 1 odst. 3 ZKB.

[904] Jak uvádí důvodová zpráva: *„Pro specifické postavení zpravodajských služeb České republiky, kdy tyto služby spravují informační systémy velké důležitosti, avšak není z věcného hlediska (zájem zpravodajských služeb na utajení metod a forem práce) a současně z důvodu faktické nemožnosti v některých případech adekvátně dostát povinnostem návrhu zákona o kybernetické bezpečnosti, možné o těchto systémech sdělovat konkrétní údaje a tyto systémy tak dekonspirovat či je podrobovat možné kontrole ze strany NBU, byla stanovena výjimka pro tyto systémy."* Důvodová zpráva k ZKB. Obecná část. Op. cit., str. 44.

[905] § 4 odst. 1 ZKB.

[906] Srov. § 4 odst. 2 a 4 ZKB.

[907] Srov. § 4 odst. 5 - 7 ZKB.

Zmíněná povinnost se úzce dotýká zadávání veřejných zakázek a ZKB výslovně stanoví, že zohlednění bezpečnostních požadavků se nepovažuje za nezákonné omezení hospodářské soutěže či její neodůvodněnou překážku.[908] Povinnost zohlednit bezpečnostní požadavky lze hodnotit kladně, neboť usnadňuje vyřazení nedůvěryhodných dodavatelů informačních a komunikačních infrastruktur ze služeb státu.[909] V souvislosti s kybernetickými hrozbami při používání technických nebo programových prostředků společnosti Huawei a ZTE vydal také NÚKIB varování ve smyslu § 12 ZKB.[910]

V rámci prevence ZKB stanoví sadu pokynů a pravidel, jejichž dodržování vyžaduje. Za jejichž nedodržení, které kvalifikuje jako přestupek,[911] umožňuje uložit sankci ve formě pokuty v citelné výši. Horní hranice její výměry činí v případě nezavedení nebo neprovádění bezpečnostních opatření, anebo nevedení bezpečnostní dokumentace částku 5 000 000 Kč, přičemž zákon nezohledňuje, který z povinných subjektů se přestupku dopustí.[912] Maximální možná výše ukládané pokuty je tak značná, uvážíme-li, že ji zákon umožňuje uložit za přestupek, kde znakem skutkové podstaty není ani vznik škody. Zákonodárce se tak rozhodl zvolit možnost výrazného postihu již u porušení samotné prevence kybernetického nebezpečí. Lze proto očekávat, že právě absence škody bude častým argumentem přestupců s cílem dosáhnout u NÚKIB uložení nižší pokuty.

Bezpečnostní opatření by měla směřovat povinné subjekty k aktivnímu uplatňování bezpečnostní politiky, tedy pravidel, směrnic a zvyklostí, které určují způsoby, pomocí nichž jsou v systémech řízena, chráněna a distribuována aktiva, včetně citlivých informací.[913] Jak upozorňují Doucek, Konečný a Novák, *„těmito politikami vyjadřuje vedení organizace svoji vůli ve vztahu ke kybernetické bezpečnosti a bezpečnosti informací a dává najevo svoji podporu, která je pro účelné a účinné prosazování kybernetické bezpečnosti a bezpečnosti informací nezbytná. V praxi to znamená,*

---

[908] Srov. § 4 odst. 4 a 7 ZKB. Zadávání veřejných zakázek v oblasti ICT se věnují i doporučení a podpůrné materiály NÚKIB, např.: NÚKIB. *Vzorové hodnocení rizik pro veřejnou zakázku* [online]. 22. 8. 2022. NÚKIB. *Zohlednění varování ze dne 17. 12. 2018 v zadávacím řízení* [online]. 14.1.2022. či NÚKIB. *Zadávání veřejných zakázek v oblasti ICT a kybernetická bezpečnost v 1.3* [online]. 31. 7. 2020. Vše dostupné: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/ [Cit. 2022-11-21].

[909] Podrobněji k zohlednění rizik na straně zadavatelů viz SMEJKAL, Vladimír, SOKOL, Tomáš, KODL, Jindřich. Op. cit., str. 100 - 110.

[910] NÚKIB. *Varování NÚKIB před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation* [online]. 17. 12. 2018. Dostupné: https://www.nukib.cz/cs/uredni-deska/ [Cit. 2022-11-21].

[911] Srov. skutkové podstaty přestupků v § 25 odst. 3 písm. a) až c), odst. 5 písm. a) až c), odst. 6 písm. a) až c), odst. 7 písm. a) až c), odst. 8 písm. a) až c), odst. 9 písm. a), odst. 10 písm. b) ZKB.

[912] Srov. § 25 odst. 14 písm. a) ZKB.

[913] ISO 27001, citace dle DOUCEK, Petr, KONEČNÝ, Martin, NOVÁK, Luděk. Op. cit., str. 169.

že vedení je odpovědné nejen za schválení a vydání bezpečnostních politik ..., ale že vedení je také současně povinno se všemi platnými pravidly důsledně řídit."[914]

Zajištění souladu s bezpečnostními opatřeními je podstatou dosažení stavu *compliance*, tj. souladu s regulatorními požadavky normotvůrce; v opačném případě hrozí postih.[915] Jak upozorňuje Vostoupal, *compliance* je kontinuální stav, opatření je třeba plnit dlouhodobě, nestačí je jednorázově splnit. Nedostatečnou bude pouhá formální shoda *„prázdných pokynů, kterými se nikdo nebude řídit. Je nezbytné, aby společnost, na kterou dopadá regulatorní požadavek ..., skutečně přijala nezbytná opatření, která budou mít potenciál k naplnění kýženého pozitivního stavu."*[916]

Přehled bezpečnostních opatření, která zákon dělí na organizační a technická, je uveden v § 5 ZKB. Organizační opatření představují *„povinnost pořizovat plány a aplikovat řídící, organizační a kontrolní postupy"*, zatímco technická opatření se týkají vlastního *„zabezpečení informačních a komunikačních systémů, včetně detekce, vyhodnocování a řešení kybernetických bezpečnostních událostí a incidentů."*[917] Ačkoli ZKB stanoví výčet bezpečnostních opatření, podrobněji jejich obsah nespecifikuje. Lze pak souhlasit se Smejkalem, Sokolem a Kodlem, že uvedené výčty bezpečnostních opatření neposkytují zcela jasnou představu, jak mají být tato opatření realizována.[918] Jak dále upozorňuje Vostoupal, příliš obecně nastavené pravidlo představuje zvýšené podnikatelské riziko, jež s sebou nese hrozbu (nejen) správního postihu za jeho nesplnění, a také neúnosně zvyšuje vlastní míru uvážení. Poukazuje přitom na náklady *compliance* procedur, které mohou být pro malé a střední společnosti podstatně vyšší než samotné náklady spojené s povinností hradit škodu.[919] Z hlediska menších podnikatelů by poté nemuselo být finančně výhodné preventivně nastavená bezpečnostní opatření podle ZKB uplatňovat, což jistě nebylo vůlí zákonodárce a k celkově bezpečnějšímu kybernetickému prostředí to nepřispívá.

Co si pod výčtem bezpečnostních opatření mají povinné osoby představit, objasňuje až podzákonný právní předpis. Na základě § 6 ZKB byl správní orgán (původně NBÚ) zmocněn k přijetí prováděcího předpisu, kterým bude fakticky stanoven obsah a rozsah bezpečnostních opatření. Tímto předpisem se stala vyhláška o kybernetické bezpečnosti. Ačkoli v důvodové zprávě

---

[914] DOUCEK, Petr, KONEČNÝ, Martin, NOVÁK, Luděk. Op. cit., str. 170.

[915] Podrobněji k pojmu *compliance* viz VOSTOUPAL, Jakub. Op. cit., str. 155.

[916] VOSTOUPAL, Jakub. Op. cit., str. 156.

[917] Důvodová zpráva k ZKB, str. 74.

[918] SMEJKAL, Vladimír, SOKOL, Tomáš, KODL, Jindřich. Op. cit., str. 112.

[919] VOSTOUPAL, Jakub. Op. cit., str. 157. K podrobnějšímu rozboru *compliance* a klasického modelu odpovědnosti, jakož i nevýhod *compliance*, viz tamtéž, str. 156 - 159.

je argumentováno nutností zajistit, aby byla konkretizace bezpečnostních opatření *„dostatečně flexibilní ve vztahu k budoucímu vývoji techniky"*,[920] uvedený způsob vedl k tomu, že obsah ukládané povinnosti stanoví až podzákonný právní předpis.

Na první pohled by se mohlo zdát, že jde o porušení zásady zákonnosti uvedené v čl. 4 odst. 1 Listiny základních práv a svobod, podle něhož *„[p]ovinnosti mohou být ukládány toliko na základě zákona a v jeho mezích a jen při zachování základních práv a svobod."* Jde o obecnou podmínku pro výkon veřejné moci, která stanoví výhradu zákona pro její veškerý výkon, včetně stanovení povinností jednotlivcům (viz také čl. 2 odst. 3 a 4 Ústavy ČR). Výhradu zákona orgán veřejné moci poruší, pokud by uložil při aplikaci práva povinnost nad rozsah stanovený zákonem. Výhradu zákona však nelze chápat absolutně, neboť by to vedlo k absurdním důsledkům a popření smyslu podzákonné normotvorby.[921] Formulace „na základě zákona" nevylučuje, aby k upřesnění povinnosti došlo v rámci podzákonného právního předpisu. Zákon však musí vždy stanovit minimálně základ dané povinnosti.[922]

Vyhláška o kybernetické bezpečnosti, která je podzákonným právním předpisem ústředního orgánu státní správy, může ve smyslu čl. 79 odst. 3 Ústavy ČR konkretizovat povinnost upravenou v základních rysech zákonem, nesmí však přesáhnout meze zákona. Zákon současně nesmí umožnit podzákonnému právnímu předpisu příliš široký prostor pro úpravu, a tím otevřít cestu ke stanovení povinností mimo zákonné parametry.[923] Pokud by tedy vyhláška o kybernetické bezpečnosti stanovila obsah organizačního nebo technického bezpečnostního opatření, který by však neodpovídal rámci tohoto opatření ve smyslu výčtu v § 5 odst. 2 a 3 ZKB, byla by výhrada zákona porušena.

Jak tenká je hranice mezi konkretizací povinností ukládaných zákonem a porušením výhrady zákona ukázal v komentářové literatuře zmiňovaný spor týkající se povinnosti podrobit se očkování stanovenému ve vyhlášce Ministerstva zdravotnictví. Zatímco kasační Nejvyšší správní soud dal žalobcům za pravdu, když měl za to, že *„předmětná zákonná právní úprava vytváří veřejné správě zcela neomezený prostor pro úvahu, které druhy vakcinace zařadí mezi tzv. ‚pravidelné', na něž se*

---

[920] Důvodová zpráva k ZKB, str. 74.

[921] Srov. nález Ústavního soudu ze dne 16. 10. 2001, Pl. ÚS 5/01.

[922] HEJČ, David. Čl. 4 [Podmínky pro ukládání povinností a pro omezení základních práv a svobod]. In: HUSSEINI, F., BARTOŇ, M., KOKEŠ, M., KOPA, M. a kol. *Listina základních práv a svobod*. 1. vydání (1. aktualizace). Praha: C. H. Beck, 2021, marg. č. 6.).

[923] Tamtéž.

bude vztahovat zákonná povinnost ‚podrobit se očkování', a které nikoliv",[924] Ústavní soud dospěl k opačnému závěru, když dovodil, že meze zákonného zmocnění prováděcí vyhláška nepřekročila.[925]

Pokud tedy ZKB stanoví povinnost zavést a provádět v rámci organizačních bezpečnostních opatření bezpečnostní politiku,[926] konkretizuje ji vyhláška o kybernetické bezpečnosti jako *„soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv"*.[927] Primárním aktivem se přitom rozumí *„informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém"*.[928] Zmíněné vymezení lze jistě považovat v mezích zákona. Stejně tomu bude např. i u řízení rizik, což vyhláška poněkud neobratně konkretizuje jako *„činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik"*.[929] Zároveň vyhláška stanoví i podrobnější povinnosti v rámci řízení rizik, jako stanovení metodik, identifikaci relevantních hrozeb, pravidelné hodnocení rizik včetně zpracování zprávy, plány ke zvládání rizik, apod.[930] Zde však můžeme spatřit úskalí v tom, že zákon sice ukládá povinnost řídit rizika, avšak nestanoví zásadní věc, a sice co je nutné považovat za riziko. Podzákonnému právnímu předpisu tak ve smyslu shora uvedené judikatury otevírá možná až příliš široký prostor pro úvahu, co stanoví rizikem. Současná podoba vyhlášky o kybernetické bezpečnosti stanoví v mezích zákona rizika velmi obecně, a tak proti ní nelze nic namítat. Nemusí tomu tak ovšem být vždy.

Ve vztahu k aplikaci bezpečnostních opatření orgány veřejné moci se soudní praxe dotkla podmínek, za nichž může správní orgán aktivně blokovat nežádoucí komunikaci, tj. aplikovat technické opatření v rámci bezpečnosti komunikačních sítí.[931] Nejvyšší správní soud v rozsudku ze dne 6. 3. 2019, č. j. 2 As 153/2018-31, dospěl k závěru, že „*zablokování určité IP adresy prostřednictvím jejího zařazení na tzv. blacklist poskytovatelem služeb v oblasti kybernetické bezpečnosti za účelem ochrany elektronické podatelny správního orgánu (§ 4 zákona č. 181/2014*

---

[924] Rozsudek Nejvyššího správního soudu ze dne 21. 7. 2010, č. j. 3 Ads 42/2010-92.

[925] Nález Ústavního soudu ze dne 27. 1. 2015, sp. zn. Pl. ÚS 19/14.

[926] § 4 odst. 2, § 5 odst. 1 písm. a), odst. 2 písm. c) ZKB.

[927] § 2 písm. c) vyhlášky o kybernetické bezpečnosti.

[928] § 2 písm. g) vyhlášky o kybernetické bezpečnosti.

[929] § 2 písm. i) vyhlášky o kybernetické bezpečnosti.

[930] Srov. § 5 odst. 1 písm. a) - i) vyhlášky o kybernetické bezpečnosti.

[931] Srov. § 5 odst. 3 písm. b) ZKB, § 18 písm. d) vyhlášky o kybernetické bezpečnosti.

Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů) není nezákonným zásahem do práv podatele, ledaže správní orgán zablokoval IP adresu svévolně."[932]

Nejvyšší správní soud se případem zabýval na základě kasační stížnosti proti zamítnutí žaloby na ochranu před nezákonnými zásahy Městského úřadu Domažlice, které měly spočívat především v zařazení žalobce a vedení dotčené IP adresy na *black-listu* spamového filtru elektronické podatelny úřadu (žalobce označil více domnělých nezákonných zásahů, které zde však netřeba rozvádět). Podstatou případu byla skutečnost, že žalobce zaslal městskému úřadu elektronickou cestou odvolání proti správnímu rozhodnutí prostřednictvím IP adresy, kterou městský úřad vedl na seznamu blokovaných adres, pročež nebylo možné z této adresy zasílat relevantní podání. Správní rozhodnutí (pro žalobce nepříznivé) tudíž nabylo právní moci.

Kasační soud vyšel z ustálené judikatury, podle níž se datová zpráva považuje za doručenou teprve tehdy, je-li dostupná elektronické podatelně. U elektronických zpráv je tedy rozhodný nikoli okamžik jejich odeslání, ale doručení správnímu orgánu.[933] Soud zopakoval, že *„[p]o správním orgánu není možné požadovat, aby nechal svou elektronickou podatelnu nezabezpečenou proti jakýmkoliv možným e-mailovým útokům či zahlcení nevyžádanou poštou. Správní orgán je naopak povinen zabezpečit fungování své elektronické podatelny a z toho důvodu je zřejmé, že přistoupí k použití jistých bezpečnostních opatření – v současném případě např. využití služeb společnosti, která poskytuje bezpečnostní produkty v této oblasti, z nichž jedním je též blacklist potenciálně nebezpečných blokovaných adres."*[934] Výjimky by u elektronických zpráv bylo možné připustit jen u zjevně svévolného nastavení spamového filtru či *blacklistu* ze strany správního orgánu.[935]

Z citovaného rozsudku kasačního soudu vyplývá, že je odpovědností účastníka řízení, aby zvolil řádný zákonný procesní postup, jenž mu zaručí, že se správní orgán, a posléze i soud, dozví jeho stanovisko ve věci. V případě zprávy o neúspěšném doručení podání musí zajistit jeho řádné doručení jiným způsobem. Do určité míry soud posvětil i zařazení a vedení IP adres na *black-listu* jako způsobu ochrany podatelny správního orgánu. Těžko si lze rovněž představit, že by zařazení IP

---

[932] Rozsudek Nejvyššího správního soudu ze dne 6. 3. 2019, č. j. 2 As 153/2018-31.

[933] Viz rozsudky Nejvyššího správního soudu ze dne 11. 6. 2015, č. j. 7 Azs 113/2015 - 34, a ze dne 29. 11. 2017, č. j. 1 As 214/2017 – 32.

[934] Rozsudek Nejvyššího správního soudu ze dne 6. 3. 2019, č. j. 2 As 153/2018-31, bod 13. Zvýrazněno dle rozsudku.

[935] Tamtéž.

adresy na *black-list* představovalo nezákonný zásah, pokud měl účastník řízení současně možnost komunikovat se správním orgánem mnoha jinými způsoby, než právě z blokované IP adresy.[936]

3.2.2. Opatření v užším slova smyslu (§ 11 ZKB)

3.2.2.1. Varování (§ 12 ZKB)

Varování je prvním z opatření v užším slova smyslu, které ZKB upravuje v §§ 11 - 15. Zákon zmíněná opatření souhrnně definuje jako *„úkony, jichž je třeba k ochraně informačních systémů nebo služeb a sítí elektronických komunikací před hrozbou v oblasti kybernetické bezpečnosti nebo před kybernetickým bezpečnostním incidentem anebo k řešení již nastalého kybernetického bezpečnostního incidentu."*[937] Narozdíl od bezpečnostních opatření reagují opatření v užším slova smyslu již na konkrétní kybernetickou bezpečnostní hrozbu či přímo na bezpečnostní incident. Užití termínu „opatření" u preventivně míněných bezpečnostních opatření v §§ 4 a 5 ZKB, a poté opětovně zde, se proto může zdát mírně matoucí. Opatření vyjmenovaná v § 11 odst. 2 ZKB si tak u části akademické obce vysloužila přezdívku „protiopatření",[938] která dobře vystihuje jejich charakter a vymezuje je od bezpečnostních opatření popsaných shora.

Právní formou se varování řadí mezi tzv. jiné úkony podle části čtvrté správního řádu. Varování má podpůrnou formu, jejíž právní účinky lze považovat za méně zásadní než v případě ochranného a reaktivního opatření, která nabývají forem opatření obecné povahy, případně i rozhodnutí (jde-li o reaktivní opatření). Klodwig považuje varování za sdělení podle části čtvrté správního řádu.[939] Podle mého názoru však varování odpovídá spíše zbytkové kategorii jiných úkonů ve smyslu části čtvrté správního řádu, než výslovně sdělení. Varování podle ZKB je natolik specifickým institutem, že se obvyklým sdělením správního orgánu, jež mají veskrze informativní charakter, vymyká. Vzhledem k § 158 odst. 1 správního řádu se bude na varování, které je jiným úkonem, ovšem také vztahovat část čtvrtá správního řádu.

S ohledem na právní formu jiného úkonu podle části čtvrté správního řádu nelze varování napadnout samostatnou správní žalobou, ledaže by ve skutečnosti materiálně šlo o správní rozhodnutí. Individuální ochranou proto bude ochrana v režimu podkladových úkonů ve smyslu § 75 odst. 2 s. ř. s., bude-li ovšem varování současně závazným podkladem pro napadené

[936] V projednávané věci šlo o zjevné obstrukční jednání při zastupování pachatelů dopravních přestupků, jak kasační soud i poznamenal v závěru svého rozhodnutí. Viz rozsudek Nejvyššího správního soudu ze dne 6. 3. 2019, č. j. 2 As 153/2018-31, bod 17.

[937] § 11 odst. 1 ZKB.

[938] POLČÁK, Radim, HARAŠTA, Jakub, STUPKA, Václav. Op. cit., str. 30.

[939] KLODWIG, Jakub. Op. cit., str. 56.

rozhodnutí, a dále též ochrana v režimu zásahové žaloby podle § 82 a násl. s. ř. s.[940] Narozdíl od běžných podkladových úkonů, kterými jsou typicky stanoviska či odborná vyjádření správních orgánů, je však varování samostatným aktem vydávaným bez závislosti na správním řízení.

Smyslem varování je upozornit veřejnost oficiální cestou na hrozbu v oblasti kybernetické bezpečnosti, která vyžaduje bezprostřední reakci. Podmínkou pro vydání varování je proto konkrétní informace o existenci hrozby. ZKB v § 12 odst. 1 ukládá NÚKIB vydat varování tehdy, *„dozví-li se zejména z vlastní činnosti nebo z podnětu provozovatele národního CERT anebo od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí, o hrozbě v oblasti kybernetické bezpečnosti."* Dozví-li se NÚKIB o existenci této hrozby, musí o ní vydat varování (srov. *„vydá"*), zde není prostor pro úvahu. Při zjišťování existence hrozeb pro kybernetickou bezpečnost je klíčová spolupráce s dalšími orgány státní správy jak v tuzemsku, tak v zahraničí. Podnět však může NÚKIB obdržet odkudkoli (srov. „*zejména*"). Vhodné je rovněž uveřejnění informace o technickém řešení, má-li hrozba technickou povahu a takové řešení již má NÚKIB k dispozici.[941]

Orgány a osoby, jimž ZKB ukládá povinnosti, se musí varováním přímo zabývat. NÚKIB jim proto varování také sám oznámí.[942] Varování musí být rovněž uveřejněno, aby se s ním mohla seznámit širší veřejnost. Stane se tak přímo na internetových stránkách NÚKIB. Jak poukazuje Klodwig, *„[v]ýznam takového prokazatelného sdělení přitom vytváří očekávání společnosti, že regulovaný subjekt bude adekvátně reagovat. Informace totiž není pouhým dohadem, nebo spekulací v tisku, ale vážně míněnou adresnou zprávou, která může pocházet od tuzemských zpravodajských služeb, zahraničních spojenců či v různé míře vycházet z tajných informací."*[943]

Povinné subjekty[944] musejí na základě vydaného varování provést v rámci řízení rizik jejich analýzu, v níž zohlední kybernetickou hrozbu, která je předmětem varování, tím, že přijmou bezpečnostní opatření reagující na související rizika. Zmíněné povinnosti související s řízením rizik podrobněji rozebírá metodika, kterou vydal NÚKIB v souvislosti s prvním z vydaných varování.[945] Nejen v zájmu regulovaných subjektů bude adekvátní reakce na popsanou kybernetickou hrozbu.

---

[940] POTĚŠIL, Lukáš. § 154 [Zákonné vymezení tzv. jiných úkonů a úprava procesního postupu]. In: POTĚŠIL, Lukáš, HEJČ, David, RIGEL, Filip, MAREK, David. *Správní řád*. 2. vydání. Praha: C. H. Beck, 2020, s. 769, marg. č. 5.

[941] Důvodová zpráva k ZKB. Obecná část. Op. cit., str. 78.

[942] § 12 odst. 2 ZKB.

[943] KLODWIG, Jakub. Op. cit., str. 58.

[944] Jde o povinné orgány a osoby uvedené v § 3 písm. c) až f) a h) ZKB.

[945] NÚKIB. *Metodika k varování ze dne 17. prosince 2018* [online], str. 4. Dostupné: https://www.govcert.cz/download/kii-vis/2019_01_04_metodika_k_varov%C3%A1n%C3%AD_z_17-12-2018_v1.0.pdf [Cit. 2022-11-22].

Půjde totiž o způsob, jak se vyvarovat vzniku škody nejen na vlastním majetku, ale též ve vztahu ke smluvním partnerům, prokáže-li se, že škodě bylo možné zabránit.[946]

Varování může souviset i s výskytem konkrétního kybernetického bezpečnostního incidentu. Je-li tímto incidentem dotčena kritická informační infrastruktura, provozování základní služby nebo poskytování digitální služby, a vyžaduje-li to současně ochrana vnitřního pořádku a bezpečnosti, života a zdraví osob nebo ekonomiky státu, stanoví zákon oprávnění NÚKIB informovat o tomto incidentu také veřejnost. NÚKIB tak učiní po konzultaci s dotčeným orgánem či osobou, případně jim uloží veřejnost informovat.[947] Ve druhém případě bude podoba konkrétní informace na dotčeném subjektu.[948]

Zákon nestanoví povinnost informovat o incidentu veřejnost v každém případě, nýbrž dává správnímu úřadu v § 12 odst. 3 ZKB prostor pro úvahu, zda veřejnost vůbec informovat. NÚKIB má možnost, shledá-li zákonem stanovené důvody, veřejnost o incidentu informovat nebo neinformovat (resp. povinnost informovat uložit dotčeným orgánům či osobám). Veřejnost tím pádem bude informována až na základě správního uvážení. Taková správní úvaha však musí vždy respektovat meze a hlediska stanovená zákonem a být v souladu s pravidly logického úsudku.[949] Podle důvodové zprávy musí správní úřad vzít v úvahu při rozhodování o zveřejnění informací o kybernetickém bezpečnostním incidentu *„potřebu zachování rovnováhy mezi zájmem veřejnosti být informovanou o hrozbách a možným poškozením pověsti či obchodních zájmů provozovatelů základních služeb a poskytovatelů digitálních služeb, kteří incidenty ohlašují.”*[950] Jelikož půjde o situace, v níž může být dotčeno fungování pro stát klíčových služeb, bude vhodné před rozhodnutím o informování zajistit také stanoviska dalších dotčených správních orgánů.[951]

Jelikož zákon hovoří o konzultaci s incidentem dotčenými orgány a osobami, a zároveň nestanoví časovou podmínku pro samotné informování o incidentu, lze předpokládat, že míní poskytnout dotčeným orgánům a osobám prostor pro zvládnutí incidentu ještě před tím, než o něm bude informována veřejnost.

Je-li varování vydáno v souvislosti s konkrétní technologií či programovým vybavením, jako tomu bylo v případě varování ze dne 17. 12. 2018 ve vztahu k použití prostředků společnosti

---

[946] Na souvislosti se vznikem občanskoprávní odpovědnosti upozorňuje KLODWIG, Jakub. Op. cit., str. 58 - 59.

[947] § 12 odst. 3 ZKB.

[948] Důvodová zpráva k ZKB. Zvláštní část. Op. cit., bod 26.

[949] Srov. např. rozsudek Nejvyššího správního soudu ze dne 26. 8. 2004, č. j. 5 Azs 170/2004-72.

[950] Důvodová zpráva k ZKB. Op. cit. Zvláštní část, bod 26.

[951] Tamtéž.

Huawei a ZTE,[952] neznamená to automaticky zákaz jejich dalšího používání. Plošný zákaz určitých technologií by mohl uložit jen zákon. Rovněž NÚKIB zdůraznil, že institut varování představuje *„nutnost zvážit případné bezpečnostní riziko související s jejich užíváním. Dovolí-li to výsledky analýzy rizik, uvedené technické nebo programové prostředky je možné i nadále používat."*[953]

V souvislosti s citovaným varováním ohledně společností Huawei a ZTE vydal NÚKIB metodiku o institutu varování, určenou zejména pro povinné subjekty provádějící v rámci prevence bezpečnostní opatření. Metodika se věnuje i zajištění souladného postupu se zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů. Subjekty, které neprovádí bezpečnostní opatření ani široká veřejnost, varování nemusí jakkoli zohlednit. Smejkal a kol. však upozorňují, že se i přístupy jednotlivých povinných osob liší, a to *„od reakce spočívající v zákazu dodávek od těchto výrobců až po neakceptování varování s tím, že údajná analýza rizik žádná rizika neukázala."*[954] U širší veřejnosti lze však shledat, že varování ohledně společností Huawei a ZTE má dopad na její další počínání i ochotu dotčené technologie používat (zmíněné varování je stále v platnosti). Čínská společnost Huawei, která byla uváděna mezi největšími dodavateli mobilních sítí a další infrastruktury pro české operátory,[955] zaznamenala v souvislosti s varováním pokles tržeb a ztrátu klíčových zakázek.[956] Povinné subjekty totiž musely zohlednit varování v rámci analýzy a řízení rizik, jakož i při výběru dodavatelů a přípravě smluvních dokumentů, v souladu s § 4 odst. 4 ZKB. Jak upozornila metodika NÚKIB, *„[z]a dodavatele se v tomto případě považují nejen společnosti Huawei Technologies Co., Ltd., a ZTE Corporation, uvedené v samotném varování, ale i všechny další společnosti, které technické nebo programové prostředky zmiňovaných společností přeprodávají nebo které dodávají technické celky, jejichž součástí jsou prostředky zmiňovaných společností."*[957]

---

[952] NÚKIB. *Varování před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation* [online]. 17. 12. 2018. Dostupné: https://www.nukib.cz/cs/uredni-deska/ [Cit. 2022-11-21].

[953] NÚKIB. *Metodika k varování ze dne 17. prosince 2018* [online], str. 4. Dostupné: https://www.govcert.cz/download/kii-vis/2019_01_04_metodika_k_varov%C3%A1n%C3%AD_z_17-12-2018_v1.0.pdf [Cit. 2022-11-22].

[954] SMEJKAL, Vladimír, SOKOL, Tomáš, KODL, Jindřich. Op. cit., str. 101.

[955] CENTRUM KYBERNETICKÉ BEZPEČNOSTI. *Úřad pro kybernetickou bezpečnost varoval před výrobky firem Huawei a ZTE* [online]. 18. 12. 2022. Dostupné: https://centrumkyberbezpecnosti.cz/urad-pro-kybernetickou-bezpecnost-varoval-pred-vyrobky-firem-huawei-a-zte/ [Cit. 2022-11-22].

[956] SEDLÁK, Jan. *Huaewei v Česku kvůli sankcím a varování spadly tržby skoro o tři miliardy* [online]. Lupa.cz, 9.9.2022. Dostupné: https://www.lupa.cz/aktuality/huawei-v-cesku-kvuli-sankcim-a-varovani-spadly-trzby-skoro-o-tri-miliardy/?opinionsListing-extraParameters%5BadditionalAdvertPositions%5D%5B0%5D=rectangle-top&opinionsListing-extraParameters%5BadditionalAdvertPositions%5D%5B1%5D=opinions-list-behind-3rd-item&opinionsListing-order=insert&do=opinionsListing-reorder [Cit. 2022-11-22].

[957] NÚKIB. *Metodika k varování ze dne 17. prosince 2018* [online]. Op. cit., str. 12.

Ve vztahu k varování ohledně společností Huawei a ZTE se již objevila kritika rozporu obsahu varování a metodiky NÚKIB.[958] Metodika udává, že je třeba omezování rizikových technologií formulovat věcně, nikoli osobně s vyloučením konkrétních dodavatelů. Zmíněné opatření NÚKIB skutečně varuje před používáním prostředků konkrétních společností. Mezi primárními důvody však uvádí právní a politické prostředí Čínské lidové republiky (dále jen „ČLR"), jejímiž zákony jsou společnosti Huawei a ZTE povinny se řídit, organizační a personální propojení jmenovaných společností s ČLR, která vyžaduje podíl společností na zpravodajských aktivitách státu, a aktivní prosazování politických zájmů ČLR na území ČR, včetně zpravodajských aktivit vlivového a špionážního charakteru ze strany ČLR.[959]

Podstatou prvého varování NÚKIB tedy bylo propojení jmenovaných společností s ČLR a její právní a politické prostředí, nikoli konkrétní technologie. Pokud by mělo být varování zaměřeno obecně na rizikové technologie, muselo by vyloučit používání špionážního software jako takového. To se však děje skrytě a běžně v rozporu se zájmy dotčených stran, jinak by nešlo o špionáž. S opatřením NÚKIB, jež by varovalo obecně před používáním technologií špionážního charakteru, by nebylo možné nesouhlasit, nicméně efektivita takového varování by nebyla nijak valná.

V pořadí druhé z vydaných varování NÚKIB se týkalo hrozby kybernetických útoků na nemocnice a další významné cíle v ČR.[960] Na rozdíl od prvního varování jeho platnost již skončila.[961] NÚKIB v něm varoval před kybernetickou hrozbou, *„spočívající v realizaci rozsáhlé kampaně závažných kybernetických útoků na informační a komunikační systémy v České republice, zejména pak na systémy zdravotnických zařízení."* Ohrožena byla zejména dostupnost, důvěrnost a integrita informací u důležitých informačních a komunikačních systémů.[962] Nebezpečnost kybernetických útoků byla citelnější vzhledem k probíhající pandemii koronaviru, trvání nouzového stavu na území ČR, jakož i nutnosti zajistit fungování mnoha informačních a komunikačních systémů. NÚKIB ve varování doporučil provést konkrétní bezpečnostní úkony spočívající v informování a poučení uživatelů o malware, provedení technických opatření a offline záloh dat,

---

[958] SMEJKAL, Vladimír, SOKOL, Tomáš, KODL, Jindřich. Op. cit., str. 100.

[959] NÚKIB. *Varování před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation* [online] . Op. cit., odst. 4 a 5.

[960] NÚKIB. *Varování před hrozbou kybernetických útoků na nemocnice a jiné významné cíle ČR* [online]. 16. 4. 2020. Dostupné: https://www.nukib.cz/cs/uredni-deska/ [Cit. 2022-11-22].

[961] NÚKIB. *Ukončení účinnosti varování ze dne 16. dubna 2020* [online]. 20. 5. 2020. Dostupné: https://www.nukib.cz/cs/uredni-deska/ [Cit. 2022-11-22].

[962] NÚKIB. *Varování před hrozbou kybernetických útoků na nemocnice a jiné významné cíle ČR* [online]. Op. cit., výrok.

jakož i prověření konkrétních *hashů*[963] škodlivých souborů. Spojil tím svoji preventivní působnost ve smyslu § 22 písm. j) ZKB s institutem varování dle § 12 ZKB.

Zatímco podstatou prvního varování bylo omezení působení čínských společností v českém prostředí vzhledem k bezpečnostním rizikům pro stát, druhé varování plnilo klasickou funkci, neboť varovalo před kybernetickou hrozbou a poskytlo rady, jak jí čelit.

Další dvě varování NÚKIB souvisejí s ozbrojeným konfliktem mezi Ruskou federací a Ukrajinou. V únoru a březnu 2022 správní úřad varoval před kybernetickými útoky na strategické organizace v ČR[964] a před nedodržením smluvních závazků dodavateli ICT služeb a produktů s významným vztahem k Ruské federaci.[965] Obě varování obsahují doporučené postupy k zvládnutí kybernetických hrozeb i preventivní opatření k zabezpečení systémů v ČR. Varování z 25. 2. 2022 je určeno zejména strategickým institucím veřejné správy (významné informační systémy), prvkům kritické informační infrastruktury, informačním systémům základních služeb a médiím. Má vysoce technickou povahu, neboť informuje o jednotlivých technikách ke zmírnění možných kybernetických útoků (zejména DDoS) využívajících známé zranitelnosti systémů. Varování z 21. 3. 2022 souvisí se sankcemi vůči Ruské federaci. Oproti únorovému varování se vyznačuje převážně preventivním charakterem, když uvádí doporučené postupy v případě, že subjekty využívají ICT služby a produkty závislé na dodavatelích s významným vztahem k Ruské federaci. Významný vztah toto varování rovněž definuje.

Dosud poslední z vydaných varování NÚKIB se týká použití tzv. chytrých elektroměrů pocházejících ze zemí s nedůvěryhodným právním prostředím, tj. mimo státy EU, Evropského hospodářského prostoru, Organizace pro hospodářskou spolupráci a rozvoj, a Severoatlantické aliance.[966] Varování je určeno především provozovatelům distribuční soustavy elektřiny, kteří jsou na základě české i evropské legislativy povinni implementovat technologické inovace v oblasti měření elektřiny. Vzhledem k možným dopadům narušení bezpečnosti technologií umožňujících požadovanou úroveň přímého měření (ovlivnění měření a odeslání chybných dat do centrály, hromadné odpojení odběrných míst, narušení stability přenosové soustavy a *blackout*), NÚKIB

---

[963] Podle Výkladového slovníku kybernetické bezpečnosti jde o jednosměrnou matematickou transformaci vstupních dat (textu) do souboru (otisk, *hash*). Narušení bezpečnosti *hash* funkce je chápáno jako kolize. JIRÁSEK, Petr, NOVÁK, Luděk, POŽÁR, Josef. Op. cit., str. 50.

[964] NÚKIB. *Varování před hrozbou kybernetických útoků na strategické organizace v České republice* [online]. 25. 2. 2022. Dostupné: https://www.nukib.cz/cs/uredni-deska/ [Cit. 2022-11-22].

[965] NÚKIB. *Varování v souvislosti s ekonomickými sankcemi spojenými s Ruskou federací* [online]. 21. 3. 2022. Dostupné: https://www.nukib.cz/cs/uredni-deska/ [Cit. 2022-11-22].

[966] NÚKIB. *Varování před použitím chytrých elektroměrů ze zemí s nedůvěryhodným právním prostředím* [online]. 30. 5. 2022. Dostupné: https://www.nukib.cz/cs/uredni-deska/ [Cit. 2022-11-22].

varoval před možným ohrožením standardního fungování ČR a její energetické bezpečnosti. Varování proto upozorňuje na existenci hrozby ještě před nákupem technických a programových prostředků potenciálně ohrožujících kybernetickou bezpečnost, *„aby bylo energetickým společnostem, na které povinnost zavedení nové technologie dopadá, umožněno s identifikovanou hrozbou dále pracovat a zohlednit ji v procesu řízení rizik."*[967] Varování tudíž bude mít zásadní dopad pro zahájení zadávacích řízení podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů.

Z uvedených skutečností je zřejmé, že institut varování má značný potenciál ovlivnit politickou, ekonomickou i bezpečnostní situaci v ČR. NÚKIB skrze tento institut dosud varoval před dvěma konkrétními technologickými společnostmi, jakož i před neplněním smluvních závazků dodavatelů s významným vztahem k Ruské federaci, a v neposlední řadě ovlivnil zadávání veřejných zakázek. Informoval však také o doporučených postupech obrany před kybernetickými útoky.

Varování by se na první pohled mohlo jevit spíše jako doporučení. Nezohlednění obsahu varování ovšem může mít pro povinné subjekty negativní dopady. Orgány a osoby, které jsou povinny zavést bezpečnostní opatření, musí v rámci řízení rizik zohlednit varování vydané NÚKIB podle § 12 ZKB, a to při hodnocení rizik a v plánu zvládání rizik.[968] Orgány a osoby, které jsou povinny zavést bezpečnostní opatření, jsou rovněž povinny hodnotit kybernetickou hrozbu, před níž správní úřad varuje, a to na odpovídající úrovni podle jeho varování.[969] Pokud by povinné subjekty nereflektovaly varování, vystavují se nebezpečí uložení nápravného opatření v rámci výkonu kontroly ve smyslu § 23 odst. 1 a § 24 odst. 1 ZKB. Nesplnění některé z povinností uložených nápravným opatřením je přestupkem.[970]

3.2.2.2. Reaktivní opatření (§§ 13 a 15 ZKB)

Reaktivní opatření je, narozdíl od varování, institut, kterým již lze přímo zasáhnout do práv a povinností jiných osob. Uplatní se tehdy, je-li nutno řešit kybernetický bezpečnostní incident,

---

[967] Tamtéž, odst. 12.

[968] Srov. § 5 odst. 1 písm. h) bod 3 vyhlášky o kybernetické bezpečnosti.

[969] Využívá-li povinná osoba dle odst. 5 přílohy č. 2 vyhlášky o kybernetické bezpečnosti jinou metodu pro hodnocení rizik, musí hrozbu hodnotit v rámci této metody na srovnatelné úrovni jako v případě postupu podle § 5 odst. 1 písm. d) vyhlášky o kybernetické bezpečnosti.

[970] Srov. § 25 odst. 1 písm. d), odst. 2 písm. f), odst. 3 písm. l), odst. 4 písm. p), odst. 5 písm. j), odst. 6 písm. n), odst. 7 písm. j), odst. 8 písm. j), odst. 9 písm. f), odst. 10 písm. f) ZKB.

případně před tímto incidentem zabezpečit informační systémy nebo sítě a služby elektronických komunikací.

Reaktivní opatření umožňuje autoritativně nařídit zavedení bezpečnostních opatření u konkrétních orgánů nebo osob dotčených kybernetickým bezpečnostním incidentem. Ukládá-li NÚKIB konkrétnímu adresátovi provést reaktivní opatření, musí to být formou správního rozhodnutí. Bude-li třeba, aby reaktivní opatření provedl okruh orgánů nebo osob určený podle určitého kritéria, jakým bylo např. používání zranitelného software,[971] bude reaktivní opatření vydáno ve formě opatření obecné povahy.[972]

V případě, že bude uložena povinnost provést reaktivní opatření konkrétnímu subjektu, NÚKIB vydá rozhodnutí jako první úkon ve věci, a může tak učinit i v řízení na místě.[973] Zákon přitom nepřipouští, aby urychlenou reakci na kybernetický incident zmařil sebemenší problém s doručováním takového rozhodnutí jeho adresátovi. Nepodaří-li se rozhodnutí doručit do vlastních rukou adresáta do 3 dnů ode dne jeho vydání, doručí se mu jednoduše vyvěšením na úřední desce NÚKIB, a tímto okamžikem bude rozhodnutí i vykonatelné.[974] Případnému rozkladu zákon nepřiznává odkladný účinek.[975]

Zákonodárce si byl vědom nutnosti reagovat na kybernetický bezpečnostní incident urychleně a zabezpečit kyberprostor. Není přitom rozhodné, zda bude uložena povinnost konkrétnímu subjektu či blíže neurčenému okruhu orgánů a osob, tj. zda bude reaktivní opatření nabývat formy rozhodnutí nebo opatření obecné povahy. Právě s odkazem na nutnost ochrany kybernetického prostoru zákonodárce vyloučil u rozhodnutí odkladný účinek opravného prostředku,[976] a u opatření obecné povahy stanovil okamžik jeho účinnosti k okamžiku vyvěšení reaktivního opatření na úřední desce NÚKIB. Zároveň vyloučil, aby se před vydáním reaktivního opatření ve formě opatření obecné povahy vedlo námitkové a připomínkové řízení podle správního řádu. Připomínky vůči vydanému opatření obecné povahy umožnil teprve po jeho vydání, a to ve lhůtě 30 dnů ode dne vyvěšení opatření obecné povahy na úřední desce NÚKIB.[977]

---

[971] Na uvedený způsob vymezení povinných subjektů upozorňuje KLOWIG, Jakub. Op. cit., str. 55.

[972] § 13 odst. 3 ZKB.

[973] § 13 odst. 1 ZKB.

[974] § 13 odst. 1 ZKB.

[975] § 13 odst. 2 ZKB.

[976] Důvodová zpráva k ZKB. Obecná část. Op. cit., str. 79.

[977] § 15 odst. 2 ZKB.

Zákon stanoví povinnost provádět reaktivní opatření správcům a provozovatelům informačního či komunikačního systému kritické informační infrastruktury, jakož i významného informačního systému a informačního systému základní služby. Ostatní povinné subjekty (poskytovatelé služby elektronických komunikací a subjekty zajišťující síť elektronických komunikací nebo zajišťující významnou síť) jsou povinny provádět reaktivní opatření pouze za stavu kybernetického nebezpečí nebo za nouzového stavu vyhlášeného na žádost ředitele NÚKIB.[978] Orgány a osoby, které povinně provádějí bezpečnostní opatření, musí též zohlednit vydané reaktivní opatření v rámci tzv. řízení rizik podle § 5 odst. 1 písm. h) bod 3 vyhlášky o kybernetické bezpečnosti, a to při hodnocení rizik a v plánu zvládání rizik.

Aby bylo možné kontrolovat reakce na kybernetické bezpečnostní incidenty, ukládá § 13 odst. 4 ZKB vybraným povinným osobám zaslat správnímu úřadu oznámení o provedení reaktivního opatření a jeho výsledek. Výslovně se neuvádí, zda se oznamovací povinnost vztahuje pouze na reaktivní opatření vydané formou opatření obecné povahy, o jehož vydání jsou orgány a osoby uvedené v § 3 ZKB vyrozuměny,[979] anebo i na adresáty správních rozhodnutí. S ohledem na smysl reaktivního opatření a potřebu kontroly řešení incidentu se oznamovací povinnost bude vztahovat patrně i na adresáty správního rozhodnutí. Ostatně zákon stanoví, že kdo bez zbytečného odkladu neoznámí NÚKIB výsledek provedení reaktivního opatření podle § 13 odst. 4 ZKB, dopustí se přestupku.[980] Nesplnění povinnosti stanovené reaktivním opatřením je rovněž přestupkem, za nějž lze uložit pokutu až 1 000 000 Kč.[981]

Náprava vadných správních aktů v případě reaktivního opatření přichází v úvahu buď v řízení o rozkladu, jde-li o rozhodnutí, anebo v rámci připomínek k vydanému opatření obecné povahy. Jak bylo řečeno, vzhledem k nutnosti rychlé reakce na nastalý bezpečnostní incident může připomínkové řízení proběhnout až zpětně. NÚKIB nicméně může vydané opatření obecné povahy na základě uplatněných připomínek změnit nebo zrušit.[982]

Jelikož ZKB vyloučil použití ustanovení § 172 správního řádu, které upravuje blíže i připomínkové řízení, je úprava připomínek v zákoně poměrně kusá. ZKB v § 15 odst. 2 stanoví pouze lhůtu k podání připomínek a orgán příslušný k jejich vypořádání. Není ovšem jednoznačné

---

[978] Srov. § 11 odst. 3 písm. a), b) a § 21 odst. 6 ZKB.

[979] Srov. § 15 odst. 1 ZKB.

[980] Srov. § 25 odst. 1 písm. b), odst. 2 písm. d), odst. 3 písm. j), odst. 4 písm. m), odst. 5 písm. h), odst. 6 písm. k), odst. 7 písm. h), odst. 8 písm. h) ZKB.

[981] Srov. § 25 odst. 14, písm. b) ZKB.

[982] § 15 odst. 2 ZKB.

kdo všechno může připomínky k opatření obecné povahy uplatnit - zda pouze orgány a osoby uvedené v § 3 ZKB, které byly o vydaném reaktivním opatření správním úřadem vyrozuměny, anebo kdokoli, jehož práva, povinnosti nebo zájmy mohou být reaktivním opatřením dotčeny. Zřejmá není ani forma připomínek.

Soulad reaktivního opatření ve formě opatření obecné povahy s právními předpisy lze posoudit v přezkumném řízení.[983] Dotčené osoby se rovněž mohou obrátit na soud s žádostí o soudní přezkum vydaných aktů NÚKIB. Jelikož ochrana veřejných subjektivních práv poskytovaná správními soudy je subsidiární, tj. přichází v úvahu až po vyčerpání řádných opravných prostředků, připouští-li je zvláštní zákon,[984] bude nutné před podáním žaloby proti rozhodnutí o reaktivním opatření proti němu podat rozklad. V případě reaktivního opatření ve formě opatření obecné povahy zákon opravný prostředek nepřipouští.[985] Příslušný návrh však dosud nebyl ke správnímu soudu podán.

NÚKIB zatím zveřejnil na své úřední desce tři reaktivní opatření ve formě opatření obecné povahy.[986] První reaktivní opatření z 16. 12. 2020 se týkalo zranitelností aplikací platformy Orion společnosti SolarWinds[987] a bylo určeno jak k řešení nastalého kybernetického bezpečnostního incidentu, tak k zabezpečení informačních systémů nebo sítí a služeb elektronických komunikací před tímto incidentem. Dle odůvodnění NÚKIB byly aktualizace aplikací platformy Orion po delší čas již kompromitovány a zákazníci využívající daný software společnosti SolarWinds byli vystaveni vysokému riziku narušení jejich sítí malwarem typu backdoor. Ohrožena byla především důvěrnost informací a dat, neboť útočníci se po průniku do sítě obětí dostali skrze službu Office 365 do e-mailové komunikace i k souborům v cloudovém úložišti.[988] Správní úřad proto nařídil provedení potřebných aktualizací software platformy Orion. Část nařizovaných úkonů přitom převzal z doporučení výrobce kompromitované platformy. Ve zbytku správní úřad doporučil řídit se dalšími doporučeními společnosti SolarWinds, na něž v odůvodnění citovaného opatření odkázal.

---

[983] Jak stanoví § 174 odst. 2 správního řádu, usnesení o zahájení přezkumného řízení musí být vydáno do 1 roku od účinnosti opatření.

[984] § 5 s. ř. s.

[985] § 173 odst. 2 správního řádu.

[986] Počet vydaných reaktivních opatření ve formě rozhodnutí není veřejně uváděn s ohledem na neveřejnou povahu správního řízení.

[987] NÚKIB. *Reaktivní opatření formou opatření obecné povahy* [online]. 16. 12. 2020. Dostupné: https://www.nukib.cz/cs/uredni-deska/ [Cit. 2022-11-22].

[988] Tamtéž, str. 5.

Vzhledem k povaze kybernetického bezpečnostního incidentu byly povinnosti stanoveny všem správcům a provozovatelům informačního nebo komunikačního systému kritické informační infrastruktury, významného informačního systému nebo informačního systému základní služby. Reaktivní opatření se nevztahovalo na poskytovatele služby elektronických komunikací ani na subjekty zajišťující sítě elektronických komunikací a orgány nebo osoby zajišťující významné sítě ve smyslu § 3 písm. a) a b) ZKB. Tyto subjekty by byly povinny reaktivní opatření provádět pouze za nouzového stavu vyhlášeného kvůli kybernetickému bezpečnostnímu incidentu. V daném okamžiku však byl nouzový stav vyhlášen „pouze" s ohledem na právě probíhající pandemii koronaviru. Povinným orgánům a osobám uvedeným v § 3 písm. c) až f) ZKB uložil NÚKIB povinnost provést bezpečnostní opatření bezodkladně, respektive v krátkých lhůtách - pro část úkonů ve lhůtě 6 dnů od nabytí účinnosti opatření, pro další části úkonů do 1 týdne od zveřejnění dalších opatření.[989] Tento způsob stanovení povinnosti je ojedinělý, neboť k okamžiku nabytí účinnosti reaktivního opatření nebyl v podstatě znám přesný obsah ukládané povinnosti ani stanovená lhůta pro její splnění. Ač lze pochopit důvody pro zvolený postup, takový způsob stanovení povinnosti by bylo možné správnímu úřadu vytknout.

Další z vydaných reaktivních opatření se týkala zabezpečení kyberprostoru v souvislosti se zjištěnými zranitelnostmi Microsoft Exchange Server.[990] Na příkladu druhého z vydaných reaktivních opatření lze vidět postup správního úřadu od mírnějších forem doporučení a upozornění, na zjištěné zranitelnosti, až k vydání reaktivního opatření. Poté, kdy nestačilo na zranitelnosti opakovaně upozorňovat na webových stránkách úřadu,[991] přistoupil teprve NÚKIB k vydání reaktivního opatření ve formě opatření obecné povahy. V něm stanovil sadu úkonů nezbytných k zabezpečení informačních systémů a sítí i služeb elektronických komunikací. Zároveň NÚKIB požadoval zaslat informace, které se ukázaly pro vládní CERT jako nezbytné k vyhledávání a hodnocení výskytu řešených zranitelností a hodnocení souvisejících hrozeb. Druhé reaktivní opatření tedy nestanovilo pouze povinnosti týkající se zabezpečení vlastních systémů a sítí

---

[989] Na str. 4 citovaného reaktivního opatření se uvádí: *„Další indikátory kompromitace, které budou Úřadem bezodkladně po jejich zjištění uveřejněny na internetových stránkách www.nukib.cz (konkrétně zde: https://www.nukib.cz/cs/infoservis/hrozby/), je povinná osoba povinna prověřit bezodkladně po seznámení se s nimi, nejpozději však do 1 týdne od jejich uveřejnění."*

[990] NÚKIB. *Reaktivní opatření formou opatření obecné povahy* [online]. 12. 03. 2021. Dostupné: https://www.nukib.cz/cs/uredni-deska/ [Cit. 2022-11-22].

[991] Viz odůvodnění citovaného opatření: *„I přes toto upozornění Úřad zjistil stále přetrvávající vysoké množství neaktualizovaných systémů, což významně zvyšuje riziko vážných útoků prostřednictvím využití této zranitelnosti Microsoft Exchange Server v České republice. S ohledem na povahu a význam výše uvedených zranitelností má Úřad důvodné podezření, že zranitelnost Microsoft Exchange Server může být plošně zneužita zejména k rozsáhlým ransomware útokům jak přímo ze strany kyberkriminálních skupin nebo jednotlivců, tak ve formě ransomware nebo access-as-a-service, kdy kyberkriminální skupiny za poplatek poskytují svůj získaný přístup do sítí obětí třetím stranám."* Tamtéž, odst. 2 odůvodnění.

povinných osob, ale i povinnosti, jež by bylo možné chápat jako nutnou spolupráci při zajištění bezpečného kyberprostoru činností správního úřadu.[992]

Dosud poslední z uveřejněných reaktivních opatření se vztahuje k zjištěné zranitelnosti komponenty Log4j.[993] Ta se nachází v řadě systémů vytvořených v programovacím jazyce Java, pročež se týká vysokého množství komerčních i open-source systémů. Vlivem zranitelnosti jsou tyto systémy snadno ovladatelné útočníky.[994] Reaktivním opatřením byly stanoveny úkony nutné k opravě zranitelností a znemožnění útoku, jakož i úkony preventivní (např. zálohování potenciálně zranitelných aktiv za účelem prevence ztráty dat u útoku ve formě ransomware).

Lze uzavřít, že dosud uveřejněná reaktivní opatření obsahují podrobná zdůvodnění závažnosti kybernetických bezpečnostních incidentů a poukazují na zásadní důvody, pro které správní úřad přistoupil k jejich vydání. Opatření obecné povahy se ukazuje jako vhodná právní forma správního aktu, jelikož zjištěné zranitelnosti počítačových systémů nebo sítí a služeb elektronických komunikací, které zpravidla mohou za nastalé kybernetické bezpečnostní incidenty, je zapotřebí řešit ve vztahu k širokému okruhu orgánů a osob. Tyto orgány a osoby by mohly být jen obtížně jednotlivě určeny ve správním rozhodnutí, a ani by to nemuselo být dostatečně efektivní.

3.2.2.3. Ochranné opatření (§§ 14 a 15 ZKB)

Poslední z opatření v užším slova smyslu, které uvádí § 11 odst. 2 ZKB, je ochranné opatření. Z hlediska ohrožení kybernetické bezpečnosti ochranné opatření přichází na řadu jako poslední, neboť již čerpá z provedené analýzy kybernetického bezpečnostního incidentu, který byl vyřešen.

Jak název napovídá, smyslem ochranného opatření je zvýšit ochranu informačních systémů nebo služeb a sítí elektronických komunikací. Ochranné opatření je v podstatě prostředkem, jak se hromadně poučit z vlastních chyb, přičemž toto ponaučení je autoritativně nařízeno shora. NÚKIB totiž orgánům a osobám uvedeným v § 3 písm. c) až f) ZKB stanoví konkrétní způsob, jak mají v určené lhůtě zvýšit ochranu informačních systémů nebo služeb a sítí elektronických komunikací.[995]

---

[992] Tamtéž, odst. 9 odůvodnění.

[993] NÚKIB. *Reaktivní opatření formou opatření obecné povahy - Log4Shell* [online]. 15. 12. 2021. Dostupné: https://www.nukib.cz/cs/uredni-deska/ [Cit. 2022-11-22].

[994] Viz odůvodnění citovaného opatření: *„V současné době Úřad eviduje řadu pokusů o skenování systémů i aktivní zneužívání této zranitelnosti, stejně tak jsou tyto činnosti hlášeny i mezinárodně a jejich výskyt narůstá exponenciální rychlostí."* Tamtéž, odst. 2 odůvodnění.

[995] Srov. § 14 ZKB.

Nesplnění povinnosti stanovené ochranným opatřením je přestupkem, za nějž lze uložit pokutu až 1 000 000 Kč.[996]

Z hlediska právní formy, okamžiku účinnosti i způsobu vydání platí pro ochranné opatření to, co bylo uvedeno shora u reaktivního opatření: NÚKIB jej vydá ve formě opatření obecné povahy, připomínkové ani námitkové řízení se nevede, resp. připomínky lze uplatnit *ex post,* tj. teprve poté, kdy je ochranné opatření vyvěšeno na úřední desce správního úřadu.[997] Účinnosti nabývá opatření obecné povahy již v okamžiku vyvěšení na úřední desce NÚKIB. O jeho vydání NÚKIB rovněž vyrozumí orgány a osoby uvedené v § 3 ZKB, má-li jejich kontaktní údaje k dispozici. Soulad ochranného opatření s právními předpisy lze posoudit v přezkumném řízení, k dispozici je dále soudní přezkum opatření obecné povahy.

Narozdíl od reaktivního opatření však není možné zvolit u ochranného opatření formu správního rozhodnutí. Je to logické, uvážíme-li, že smyslem ochranného opatření je zvýšit ochranu informačních systémů a služeb i sítí elektronických komunikací, a zamezit opakování kybernetického bezpečnostního incidentu. Vztahovat se proto musí na širší, individuálně neurčený okruh orgánů a osob.

Dosud NÚKIB uveřejnil na své úřední desce jediné ochranné opatření.[998] Podává se v něm, že na základě analýzy vyřešeného kybernetického bezpečnostního incidentu z 20. 2. 2020, v jehož rámci útočník narušil důvěrnost přenášených elektronických zpráv, je nutné u orgánů a osob uvedených v § 3 písm. c) až f) ZKB zabezpečit elektronickou poštu. Ochranné opatření jim nařizuje provést úkony nezbytné k zajištění důvěrnosti a integrity přenášených dat a k prevenci podvržení e-mailové komunikace (zasílání zpráv s podvrženou doménou).[999] V opačném případě by povinné subjekty byly ohroženy narušením důvěrnosti a integrity zasílané elektronické komunikace, čímž by mohla být poškozena jejich důvěryhodnost i schopnost fungování. Orgánům veřejné moci podílejícím se na předsednictví ČR v Radě EU opatření určilo kratší lhůtu vzhledem k počátku předsednictví ČR. Zabezpečení bylo shledáno jako nutné u všech orgánů veřejné moci a povinných osob, neboť *„[m)á-li některé z požadovaných způsobů zvýšení ochrany zavedeny pouze jeden z komunikujících subjektů, probíhá celá komunikace v neadekvátně zabezpečené (nešifrované)*

---

[996] Srov. § 25 odst. 14, písm. b) ZKB.

[997] Z hlediska stručné úpravy připomínek srov. shora popsané připomínkové řízení u reaktivního opatření.

[998] NÚKIB. *Ochranné opatření formou opatření obecné povahy - Zabezpečení e-mailů* [online]. 11. 10. 2021. Dostupné: https://www.nukib.cz/cs/uredni-deska/ [Cit. 2022-11-22].

[999] Podrobněji tamtéž, odst. 3 odůvodnění.

podobě nebo je náchylná na útoky …"[1000] Forma opatření obecné povahy i u jediného dosud vydaného ochranného opatření slouží k efektivnějšímu zabezpečení informačních systémů, služeb a sítí elektronických komunikací před bezpečnostními incidenty.

Určitou zvláštností citovaného ochranného opatření je, že obsahuje část týkající se toliko technického odůvodnění výroku. Zatímco první část odůvodnění rozvádí důvody vydání ochranného opatření, dotčená právní ustanovení a povinnosti orgánů a osob, druhá část odůvodnění vysvětluje podrobněji jednotlivá technická opatření k zajištění důvěrnosti a integrity komunikace. S určitou nadsázkou by se dalo říci, že se citované opatření obecné povahy skládá z části určené pro právníky a z části určené pro informatiky. Opatření považuji takto za lépe přehledné. Podobný trend by se mohl u správních aktů z oblasti kybernetické bezpečnosti osvědčit i do budoucna.

Patrně ve snaze ještě více přiblížit obsah ukládaných povinností a zvýšit kybernetickou bezpečnost dále NÚKIB spolu s vydaným ochranným opatřením zveřejnil i odpovědi na často kladené otázky související s opatřením, a dále metodický návod ohledně zavedení ochranných prvků e-mailové komunikace vyplývajících z ochranného opatření. Uvedený počin správního úřadu lze hodnotit jako vstřícný krok vůči povinným subjektům i veřejnosti. Je nicméně nutné mít na paměti, že by tímto způsobem nemohly být nahrazeny případné nedostatky v odůvodnění samotného opatření obecné povahy, neboť se jedná o nezávazné úkony.

3.2.3. Nápravná opatření (§ 24 ZKB)

Dosud bylo pojednáno o bezpečnostních opatřeních, jejichž smysl je především preventivní, a o opatřeních v užším slova smyslu, kterými správní úřad reaguje na hrozbu kybernetického bezpečnostního incidentu i na situaci, kdy takový incident již probíhá, anebo kdy je třeba zamezit jeho opakování. Termínu opatření však zákon užívá i v rámci výkonu kontroly. Při ní je NÚKIB oprávněn uložit kontrolované osobě nápravné opatření. Nápravná opatření jsou tak spolu s deliktní odpovědností povinných subjektů součástí sankčního systému ZKB.

Podstatou nápravných opatření je zajistit včasné a kvalifikované odstranění nedostatků zjištěných při kontrole. Mimo její rámec nelze nápravné opatření uložit. Jelikož při výkonu kontroly postupují pověření zaměstnanci NÚKIB podle kontrolního řádu,[1001] je zaručena zákonná ochrana práv a zájmů kontrolovaných subjektů. Kontrola se týká způsobu plnění povinností, jež povinným orgánům a osobám ukládá ZKB, jakož i těch, které stanoví rozhodnutí a opatření obecné povahy

[1000] Tamtéž, odst. 4 odůvodnění.

[1001] Zákon č. 255/2012 Sb., o kontrole (kontrolní řád), ve znění pozdějších předpisů.

vydaná NÚKIB na základě ZKB. Jde tedy zejména o kontrolu plnění povinností stanovených reaktivními a ochrannými opatřeními, jakož i rozhodnutími o povinnosti předat data, provozní údaje a informace (§ 15a ZKB).[1002] Dále se kontrola zaměřuje i na dodržování prováděcích právních předpisů.[1003] Zatímco však u orgánů a osob uvedených v § 3 písm. a) až g) ZKB lze vykonat kontrolu bez dalších podmínek, ve vztahu k poskytovatelům digitální služby lze kontrolu provést až v případě důvodného podezření, že poskytovatel digitální služby neplní zákonné povinnosti.[1004] Poskytovatele digitální služby tedy nelze kontrolovat preventivně jako jiné povinné subjekty. Tento speciální kontrolní režim odpovídá čl. 17 odst. 1 směrnice NIS.

Nápravné opatření lze uložit tehdy, zjistí-li NÚKIB při kontrole nedostatky. V takovém případě uloží kontrolovanému orgánu nebo osobě, aby je ve stanovené lhůtě odstranily, a může i určit, jakým způsobem tak mají učinit.[1005] Obsah a rozsah nápravných opatření musí respektovat zásadu proporcionality.[1006]

Nápravným opatřením může být uložen i zákaz kontrolovanému orgánu nebo osobě vůbec používat informační nebo komunikační systém kritické informační infrastruktury, informační systém základní služby nebo významný informační systém. Podmínkou tohoto zákazu je zjištění natolik zásadních nedostatků při kontrole, jež znamenají pro daný systém bezprostřední ohrožení kybernetickým bezpečnostním incidentem, který by mohl systém významně poškodit nebo zničit. Zákaz používání se může vztahovat na celý systém nebo jen na jeho části a platí až do doby odstranění zjištěných nedostatků.[1007] Lze jej vnímat jako citelné omezení vlastnického práva, resp. i práva na informace, anebo práva podnikat či provozovat hospodářskou činnost. Zákaz používat

---

[1002] Na základě ZKB je však NÚKIB oprávněn vydat i jiná správní rozhodnutí, jako např. rozhodnutí o určení provozovatele základní služby a informačního systému základní služby (§22a), rozhodnutí o vyhlášení stavu kybernetického nebezpečí (§ 21), či rozhodnutí o pozastavení vykonatelnosti, o změně nebo o zrušení rozhodnutí o autorizaci (§22b). Tato rozhodnutí však primárně neslouží k ukládání povinností. Povinnosti zde stanoví dotčeným subjektům již přímo ZKB.

[1003] Kromě vyhlášky o kybernetické bezpečnosti se řadí mezi právní prováděcí předpisy vyhláška NBÚ a Ministerstva vnitra č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, vyhláška NÚKIB č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby, vyhláška NÚKIB č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu, vyhláška NÚKIB č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci, a prováděcí nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018, kterým se stanoví pravidla pro uplatňování směrnice NIS, a jež stanoví bezpečnostní opatření a parametry významnosti dopadu incidentu pro poskytovatele digitálních služeb.

[1004] Srov. § 23 odst. 1 ZKB.

[1005] § 24 odst. 1 ZKB.

[1006] VLÁDA. Důvodová zpráva k zákonu č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony, č. 205/2017 Dz.

[1007] § 24 odst. 2 ZKB.

dotčené systémy by proto měl přicházet úvahu až mezi posledními možnostmi, nebude-li jinak možné donutit správce a provozovatele systémů k nápravě zjištěných nedostatků. Výjimečnost zákazu dokládá i skutečnost, že v rámci připomínek k návrhu ZKB požadovaly oslovené subjekty zpřísnění i zpřesnění kritérií, za kterých bude možné nápravným opatřením zakázat provozování systému.[1008]

Náklady spojené s provedením nápravného opatření nese kontrolovaná osoba či orgán, kterým byly uloženy.[1009] Nesplnění některé z povinností uložených nápravným opatřením představuje skutkovou podstatu přestupku, za který zákon stanoví pokutu až do výše 1 000 000 Kč.[1010] Proti případnému rozhodnutí o přestupku lze podat rozklad, jež má odkladný účinek, jakož i další opravné prostředky podle správního řádu. Po vyčerpání řádných opravných prostředků se lze domáhat soudního přezkumu rozhodnutí vydaných NÚKIB.

Při výkonu kontroly a ukládání nápravných opatření mají kontrolované orgány a osoby k dispozici klasické prostředky ochrany svých práv a zájmů zakotvené v kontrolním řádu. Jedná se zejména o právo namítat podjatost kontrolujícího či osoby přizvané ke kontrole, právo seznámit se s obsahem protokolu o kontrole a právo podávat písemné odůvodněné námitky proti kontrolním zjištěním v protokole uvedeným.[1011] Současně je však kontrolovaná osoba povinna poskytnout při kontrole potřebnou součinnost a vytvořit podmínky pro její zdárný průběh.[1012]

Na základě kontrolních zjištění může být s kontrolovaným subjektem zahájeno správní řízení o uložení sankce za přestupek, a v souvislosti se skutečností uvedenou v protokolu o kontrole může být uloženo také nápravné opatření podle § 24 ZKB. Případné námitky proti kontrolním zjištěním uvedeným v protokolu by bylo možné, za souhlasu nadřízené osoby kontrolujícího, vyřídit i v rámci probíhajícího správního řízení. Vyřízení námitek by se poté uvedlo v odůvodnění rozhodnutí vydaného v rámci správního řízení.[1013] V případě nesouhlasu s obsahem rozhodnutí NÚKIB má kontrolovaná osoba možnost podat proti rozhodnutí rozklad.

V případě, kdy budou námitky vypořádány nikoli v odůvodnění správního rozhodnutí, nýbrž v samostatném sdělení správního orgánu (typicky sdělení o zamítnutí námitek), je nutné mít na

---

[1008] Důvodová zpráva k ZKB. Obecná část. Op. cit., str. 47.

[1009] Důvodová zpráva k ZKB. Zvláštní část. Op. cit., str. 86.

[1010] Srov. § 25 odst. 1 písm. d), odst. 2 písm. f), odst. 3 písm. l), odst. 4 písm. p), odst. 5 písm. j), odst. 6 písm. n), odst. 7 písm. j), odst. 8 písm. j), odst. 9 písm. f), odst. 10 písm. f), odst. 14 písm. b) ZKB.

[1011] Srov. § 10 odst. 1 a § 13 kontrolního řádu.

[1012] Srov. § 10 odst. 2 a 3 kontrolního řádu.

[1013] Srov. § 14 odst. 3 kontrolního řádu.

paměti, že sdělením o zamítnutí námitek proti protokolu zpravidla nejsou uloženy žádné povinnosti ani žádná opatření. Protokol ani vyřízení námitek nezakládají kontrolovanému žádná práva ani povinnosti, a proto se nelze domáhat jejich zrušení žalobou u správního soudu.[1014] Jak uvedl již Nejvyšší správní soud ve svém rozsudku ze dne 29. 2. 2008, č. j. 8 Afs 152/2006-144: *„Zamítnutí námitek kontrolovaného subjektu má pouze ten následek, že se nemění závěr kontrolního protokolu. Za rozhodnutí zasahující do práv stěžovatele lze v daném případě považovat až takové rozhodnutí, jímž mu byla uložena konkrétní povinnost“*. Případnou žalobu proti vyřízení námitek by proto správní soud odmítl podle § 46 odst. 1 písm. d) s. ř. s. v návaznosti na § 70 písm. a) s. ř. s.

Opačným případem by však byla situace, v níž by kontrolované osobě bylo v rámci kontrolního zjištění uloženo nápravné opatření podle § 24 ZKB. Nápravným opatřením by již mohlo dojít k zásahu do práv kontrolovaného, jemuž by mohl být uložen například i zákaz používat informační systém (srov. výše). V takovém případě nelze vyloučit, že by se jednalo materiálně o rozhodnutí s dopady do hmotných práv kontrolovaného, proti němuž by žaloba ve správním soudnictví měla být přípustná. Lze se tudíž domnívat, že taková žaloba by neměla být správním soudem odmítnuta jako nepřípustná.

3.2.4. Rozhodnutí o uložení povinnosti předat data, provozní údaje a informace (§ 15a ZKB)

Možnost nařídit provozovateli informačního systému povinnost předat data, provozní údaje a informace byla do zákona doplněna novelou účinnou od 1. 7. 2017.[1015] Na základě vloženého ustanovení § 15a ZKB je NÚKIB oprávněn, v případě hrozícího kybernetického bezpečnostního incidentu, na návrh správce informačního systému vydat rozhodnutí, jímž uloží provozovateli informačního nebo komunikačního systému kritické informační infrastruktury nebo významného informačního systému, předat správci data, provozní údaje a informace, jež má provozovatel k dispozici v souvislosti s provozováním systému.[1016]

Smyslem institutu je předejít situaci, v níž by v důsledku neshod mezi správcem a provozovatelem zmíněných systémů byla ohrožena jejich bezpečnost, neboť správce by postrádal potřebná data k tomu, aby mohl plnit své zákonné povinnosti. Správce totiž může pověřit provozováním informačního systému kritické informační infrastruktury, komunikačního systému

---

[1014] Srov. rozsudek Krajského soudu v Hradci Králové ze dne 28. 7. 2022, č. j. 30 A 76/2021-83.

[1015] Srov. čl. III, bod 6 zákona č. 104/2017 Sb., kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a některé další zákony.

[1016] § 15a odst. 1 ZKB.

kritické informační infrastruktury nebo významného informačního systému jiný orgán nebo osobu, pokud to jiný zákon nevylučuje.[1017] Aby se však následně správce neocitl v nebezpečné situaci, kdy by neměl k datům přístup - v literatuře se lze setkat s výrazem „uzamčení dat", či (*vendor*) „*lock-in*",[1018] stanoví nyní § 6a ZKB mandatorní migraci dat. Provozovatel je totiž povinen předat správci na vyžádání bez zbytečného odkladu a v dohodnutém formátu data, provozní údaje a informace, které má k dispozici v souvislosti s provozováním tohoto systému.[1019] Riziková situace by mohla nastat i při skončení smlouvy s provozovatelem. I v tomto případě je však provozovatel povinen předat potřebná data, provozní údaje a informace správci.[1020] Jak přitom uvádí důvodová zpráva, *„[a]bsence smluvních povinností migrovat data a případně poskytnout další součinnost při změně dodavatele v těchto případech vede k tomu, že je správcům de facto znemožněno vybrat lepšího dodavatele technologií nebo služeb. Zákon o kybernetické bezpečnosti by měl tedy především ošetřit případy, kdy tento „lock-in" efekt může představovat bezpečnostní riziko pro systémy a sítě spadající pod jeho věcný rozsah."*[1021] Zákonem stanovenou mandatorní migraci dat lze proto hodnotit výslovně kladně.

Co činit v případě, kdy provozovatel nereaguje na stanovenou mandatorní migraci dat? Nyní přichází na řadu správní rozhodnutí vydané NÚKIB: zákon tím reaguje na situaci, kdy provozovatel nesplní svoji povinnost předat data, provozní údaje a informace ani na základě ustanovení § 6a ZKB. K vydání takového rozhodnutí by však správní úřad neměl přistoupit bez určité aktivity správce informačního systému. Zákon jednak požaduje, aby NÚKIB vydal rozhodnutí na návrh správce, jednak aby k rozhodnutí přistoupil teprve poté, kdy správce marně vyzve provozovatele ke splnění povinnosti předat mu data, provozní údaje a informace. Rozhodnutí je proto svojí povahou subsidiární k (u)jednání mezi provozovatelem a správcem. Zákon z toho důvodu správci ukládá, aby v návrhu podrobně popsal předchozí jednání s provozovatelem zejména s ohledem na nesplnění smluvní povinnosti provozovatele. Současně správce musí v návrhu odůvodnit i požadavek na vydání rozhodnutí vzhledem k hrozícímu kybernetickému bezpečnostnímu incidentu a možným

---

[1017] § 6a odst. 1 ZKB.

[1018] SVOBODA, Jan. *Vybrané právní aspekty migrace dat: Jak předejít vendor lock-inu* [online]. SystemOnLine.cz. Dostupné: https://www.systemonline.cz/it-pravo/vybrane-pravni-aspekty-migrace-dat.htm?mobilelayout=false [Cit. 2022-11-22].

[1019] § 6a odst. 2 ZKB.

[1020] § 6a odst. 3 ZKB.

[1021] VLÁDA. Důvodová zpráva k zákonu č. 104/2017 Sb., kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a některé další zákony, č. 104/2017 Dz.

následkům nepředání dat, provozních údajů a informací.[1022] Správní rozhodnutí by nemělo suplovat nedostatek vůle provozovatele vždy, nýbrž jen tehdy, kdy bude znamenat zvýšené riziko pro bezpečnost informačního systému vzhledem k hrozícímu kybernetickému incidentu.

S ohledem na nutnost rychlého předání požadovaných dat bude vydané rozhodnutí o uložení povinnosti předat data, provozní údaje a informace prvním úkonem v řízení, přičemž vykonatelnost rozhodnutí nastane již dnem jeho doručení. Důraz na rychlost je zřejmá i z toho, že zákonodárce vyloučil u případného rozkladu odkladný účinek.[1023]

3.3. Computer Emergency Response Team (CERT)

Vzrůstající výskyt kybernetických útoků a nutnost přijetí bezpečnostních opatření u osob soukromého práva i u orgánů veřejné moci zapříčinila vznik specializovaných týmů, jejichž úkolem je řešit kybernetické bezpečnostní incidenty, spolupracovat při zajišťování kybernetické bezpečnosti a adekvátně reagovat na související hrozby.[1024] Pro zajištění kybernetické bezpečnosti jakéhokoli subjektu je fungující dohledové pracoviště klíčové.[1025] Tím je v širším slova smyslu v podstatě jakákoli kapacita, jejíž úlohou je řešení bezpečnostních incidentů.[1026] Vznikají tak skupiny reagující na počítačové bezpečnostní incidenty, známé pod anglickým termínem *Computer Security Incident Response Team*, neboli CSIRT. Lze se však setkat i s termínem *Computer Emergency Response Team*, neboli CERT, popřípadě s jinými názvy. Vždy jde však o týmy odborníků na informační bezpečnost, které nabízejí klientům služby při řešení bezpečnostních incidentů, při následné obnově systémů, při prevenci a vzdělávání, přičemž informují o odhalených slabinách užívaných hardwarových i softwarových prostředků a o možných útocích.[1027]

Ve většině států působí na vrcholné úrovni určitý bezpečnostní tým. Důležitou úlohu CERT/ CSIRT týmů zdůraznila i směrnice NIS.[1028] Státy však mohou mít různý postoj ke kybernetické bezpečnosti a souvisejícím hrozbám, od čehož se odvíjí i působnost národních či vládních

---

[1022] Srov. § 15a odst. 1 ZKB.

[1023] Srov. § 15a odst. 2 ZKB.

[1024] Důvodová zpráva k ZKB. Obecná část. Op. cit., str. 23.

[1025] HARAŠTA, Jakub. Právní aspekty kybernetické bezpečnosti ČR [online]. *Revue pro právo a technologie,* 2013, č. 8, str. 81. Dostupné: https://journals.muni.cz/revue/article/view/5015 [Cit. 2022-11-22].

[1026] HARAŠTA, Jakub, MÍŠEK, Jakub. Op. cit., str. 21-42.

[1027] DOUCEK, Petr, KONEČNÝ, Martin, NOVÁK, Luděk. Op. cit., str. 53.

[1028] Podle rec. 34 směrnice NIS by členské státy *„měly zajistit, aby dobře fungovaly jejich týmy CSIRT, rovněž označované jako týmy CERT (Computer Emergency Response Team), které budou splňovat základní požadavky tak, aby byly zaručeny jejich efektivní a kompatibilní schopnosti pro řešení incidentů a rizik a aby byla zajištěna účinná spolupráce na úrovni Unie."*

kybernetických bezpečnostních týmů. Například Ruský vládní CERT (gov-cert.ru) se zaměřuje na informační bezpečnost a doporučení, jak *„neutralizovat určité informačně-bezpečnostní hrozby, které zahrnují použití informačních a komunikačních technologií k zásahům do vnitřních záležitostí suverénního státu a narušování veřejného pořádku"*.[1029] Spíše než na zabezpečení kybernetického prostředí před kybernetickými útoky a trestnou činností tak Rusko klade důraz na zabezpečení vnitřních záležitostí státu.

Již před přijetím ZKB působilo v ČR množství zkušených týmů typu CSIRT/CERT, které byly součástí mezinárodních struktur a spolupracovaly v rámci skupiny CSIRT.CZ koordinované sdružením CZ.NIC. Sdružení CZ.NIC je zájmovým sdružením právnických osob působících v ČR v oblasti doménových jmen a na trhu služeb elektronických komunikací, zabývající se správou národní domény nejvyšší úrovně (.cz) a bezpečností Internetu i počítačů.[1030] První oficiální CERT vznikl v ČR roku 2004, v roce 2007 následoval vznik CSIRT.CZ v rámci grantu financovaného Ministerstvem vnitra.[1031] Po dohodě s Ministerstvem vnitra, které bylo tehdy ústředním orgánem státní správy pro oblast informačních systémů veřejné správy i koordinátorem pro informační a komunikační technologie,[1032] sdružení CZ.NIC převzalo agendu národního CSIRT, čímž se zapojilo do řešení kybernetických bezpečnostních incidentů v ČR provozovaných sítích, přičemž zároveň poskytovalo pomoc při jejich řešení koncovým uživatelům, tyto incidenty analyzovalo a zajišťovalo i odpovídající vzdělávání.[1033] Memorandum se stalo příkladem počínající spolupráce při výkonu státní správy v oblasti kybernetické bezpečnosti.

Ačkoli zákon nestanoví povinnost zajistit v rámci výkonu určité činnosti také fungování bezpečnostního týmu tymu CSIRT/CERT, u subjektů, jimž ZKB ukládá zavést a provádět bezpečnostní opatření, je vytvoření takových pracovišť za účelem řádného plnění zákonných povinností více než žádoucí. Nebylo by proto překvapením, pokud by jejich existence byla v budoucnu zakotvena přímo zákonem.

[1029] PAČKA, Roman. *Role CERT/CSIRT v národní bezpečnosti* [online]. Masarykova univerzita: Prezentace k předmětu Kybernetická bezpečnost, str. 47. Dostupné: https://is.muni.cz/el/fss/podzim2018/BSS469/um/bss_23.10.2018.pdf [Cit. 2022-11-22].

[1030] CZ.NIC. *O sdružení* [online]. Dostupné: https://www.nic.cz/page/351/ [Cit. 2022-11-22].

[1031] Podrobněji k historii CERT/CSIRT týmu v ČR srov. PAČKA, Roman. Op. cit., str. 56 a násl.

[1032] (NESIG.) *Memorandum o Computer Security Incident Response Team České republiky ze dne 9. prosince 2010, uzavřené mezi Ministerstvem vnitra ČR a sdružením CZ.NIC, z.s.p.o.* [online]. Dostupné: https://www.nic.cz/files/nic/doc/Memorandum_CSIRT.CZ.pdf [Cit. 2022-11-22].

[1033] Důvodová zpráva k ZKB. Obecná část. Op. cit., str. 14.

3.3.1. Národní CERT – příklad privatizace veřejné správy

Podmínky vzájemné spolupráce mezi soukromým sektorem a orgánem veřejné moci při zajišťování kybernetické bezpečnosti, která byla předmětem memoranda uzavřeného mezi Ministerstvem vnitra a sdružením CZ.NIC, jsou nyní upraveny zákonem. Zakotvení podmínek v zákoně přineslo větší transparentnost a předvídatelnost výběru partnera pro veřejnou správu, jakož i snížení rizika výběru nepovolaných osob. Současně zákon podle některých reagoval na *„poptávku soukromoprávních subjektů po centralizovaném řešení sběru informací o kybernetické bezpečnosti, které by bylo nemělo veřejnoprávní charakter."*[1034]

Podmínkou provozování národního CERT je uzavření veřejnoprávní smlouvy s NÚKIB,[1035] což odpovídá předpokladu, že provozovatelem bude osoba soukromého práva. Ačkoli je větší část závazků národního CERT soukromoprávní povahy a odpovídá činnostem, kterým se věnovalo sdružení CZ.NIC již před přijetím ZKB, vůči poskytovatelům služeb elektronických komunikací, subjektům zajišťujícím sítě elektronických komunikací i významné sítě, jedná provozovatel národního CERT z pozice subjektu, jehož prostřednictvím povinné orgány a osoby plní část svých zákonných povinností (zejména hlášení kybernetických bezpečnostních incidentů).[1036]

Zákon stanoví pro právnickou osobu, která jediná se může stát provozovatelem národního CERT, řadu podmínek. Bezpečnostním zájmům ČR odpovídá klíčový požadavek, aby šlo o osobu, jež *„nevyvíjí ani nevyvíjela činnost proti zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací"*.[1037] Jde o relativně široký pojem, neboť tímto zájmem ČR se rozumí *„zachování její ústavnosti, svrchovanosti a územní celistvosti, zajištění vnitřního pořádku a bezpečnosti, mezinárodních závazků a obrany, ochrana ekonomiky a ochrana života nebo zdraví fyzických osob"*.[1038] K tomu se přidává podmínka bezúhonnosti a neexistence splatných finančních závazků vůči státu,[1039] což jsou však standardní požadavky pro spolupráci osob soukromého práva a státu.[1040] Pravomoci v zajišťování bezpečného kyberprostoru v ČR rovněž nemohou být svěřeny zahraniční právnické osobě,[1041] ani osobě bez náležitých zkušeností a praxe. Zákon požaduje, aby

---

[1034] HARAŠTA, Jakub, MÍŠEK, Jakub. Op. cit., str. 25.

[1035] § 18 odst. 1 písm. b) ZKB. Náležitosti veřejnoprávní smlouvy blíže určuje § 19 ZKB.

[1036] Důvodová zpráva k ZKB. Zvláštní část. Op. cit., str. 82.

[1037] § 18 odst. 2 písm. a) ZKB.

[1038] § 2 písm. b) zákona o ochraně utajovaných informací.

[1039] § 18 odst. 2 písm. e), f) ZKB.

[1040] Důvodová zpráva k ZKB. Zvláštní část. Op. cit., str. 82.

[1041] § 18 odst. 2 písm. g) ZKB.

daná osoba prokázala nejméně pětileté zkušenosti s provozem či správou informačních systémů nebo služeb a sítí elektronických komunikací, jakož i technické předpoklady a členství v nadnárodní organizaci působící v oblasti kybernetické bezpečnosti.[1042] Rovněž se nepředpokládá výlučně ziskový charakter provozovatele národního CERT, byť mu zákon nezakazuje v oblasti podnikat. Ostatně část činností vykonává bezúplatně.[1043] Případná další hospodářská činnost však nesmí narušit plnění zákonných povinností provozovatele národního CERT ani ohrozit jeho nestranné vystupování.[1044]

Návrh na uzavření veřejnoprávní smlouvy o provozování národního CERT či výzva k jeho předložení mohou být směřovány vůči neurčitému počtu osob, na základě výzvy NÚKIB učiněné ve smyslu § 146 odst. 2 správního řádu. Zákon tedy odkazuje na právní úpravu řízení o výběru žádosti ve správním řádu.[1045] Odkazem na relativně podrobnou úpravu specifik řízení o výběru žádosti zákon přispívá k transparentnějšímu výkonu veřejné správy.[1046] Návrh musí být učiněn vždy v písemné formě, musí být dostatečně určitý a musí z něj vyplývat vůle toho, kdo návrh činí, být jím v případě jeho přijetí vázán.[1047]

V současnosti je provozovatelem národního CERT sdružení CZ.NIC, jehož žádost NBÚ vybral v řízení o výběru žádosti vyhlášeném dne 15. 4. 2015. Do okamžiku následného uzavření veřejnoprávní smlouvy dne 18. 12. 2015 (dále jen „Veřejnoprávní smlouva")[1048] vykonával bezpečnostní tým CSIRT.CZ téhož sdružení na základě memoranda ze dne 19. 12. 2012. Veřejnoprávní smlouva byla uzavřena na dobu neurčitou, přičemž možnosti ukončení zahrnují kromě dohody, výpovědi či odstoupení v případě podstatného porušení smlouvy druhou smluvní stranou, také zrušení smlouvy ve smyslu § 167 odst. 1 správního řádu. Důvody k návrhu na zrušení smlouvy uvedené ve Veřejnoprávní smlouvě jsou shodné s těmi, jež uvádí správní řád.[1049] Nad

---

[1042] § 18 odst. 2 písm. b), c), d) ZKB.

[1043] § 18 odst. 5 ZKB.

[1044] Srov. § 17 odst. 3 a 5 a § 18 odst. 2 písm. h) ZKB.

[1045] Srov. § 19 odst. 1 ZKB, § 163 odst. 4 a § 146 odst. 2 správního řádu.

[1046] Důvodová zpráva k ZKB. Zvláštní část. Op. cit., str. 83.

[1047] HEJČ, David. § 163 [Návrh veřejnoprávní smlouvy]. In: POTĚŠIL, Lukáš, HEJČ, David, RIGEL, Filip, MAREK, David. Op. cit., str. 796, marg. č. 2.

[1048] Celé znění veřejnoprávní smlouvy z 18. 12. 2015, jejíž přílohou je žádost CZ.NIC o uzavření veřejnoprávní smlouvy za účelem spolupráce v oblasti kybernetické bezpečnosti a zajištění provozu národního bezpečnostního týmu, je dostupné zde: https://csirt.cz/media/filer_public/d5/ab/d5aba5fa-f20d-4fa9-b725-899eb81cde80/nbu-smlouva-narodni-cert-201512.pdf [Cit. 2022-11-22].

[1049] Srov. Čl. IX. Veřejnoprávní smlouvy.

rámec uvedených případů by však Veřejnoprávní smlouva mohla být zrušena i v přezkumném řízení podle § 165 správního řádu.

Veřejnoprávní smlouvou se sdružení CZ.NIC zavázalo k řádnému provozování národního CERT v souladu s nejlepší praxí CERT/CSIRT týmů a národními i mezinárodními standardy kybernetické bezpečnosti. Kromě vyhledávání zranitelností v rámci prevence kyberútoků, mezinárodní spolupráce či informování o vlastní činnosti se sdružení CZ.NIC zavázalo k ochraně utajovaných informací zajištěním oprávnění přístupu k utajovaným informacím ve stupni Vyhrazené, jakož i zajištěním, aby příslušné fyzické osoby byly držitelem platného osvědčení pro přístup k utajovaným informacím požadovaného stupně. Veřejnoprávní smlouva dále upravuje povinnost mlčenlivosti, jež se vztahuje i na údaje o evidovaných kybernetických incidentech.[1050] Kontrola výkonu činnosti národního CERT je smluvně zajištěna skrze povinnost předložit nejaktuálnější auditní zprávu k ochraně informací, případně možností kontroly provedené přímo NÚKIB dle obecného ustanovení § 23 ZKB.[1051]

Zákon stanoví bezpečnostnímu týmu typu národního CERT širokou škálu povinností, které rozvádí i Veřejnoprávní smlouva. Patří mezi ně zejména příjem hlášení o kybernetických bezpečnostních incidentech a jejich evidování, analýza, podpora a pomoc při jejich výskytu, sdílení informací na národní i mezinárodní úrovni, hodnocení zranitelností v oblasti kybernetické bezpečnosti, účast na jednání Rady pro kybernetickou bezpečnost, atp. Evidence údajů a příjem hlášení o incidentech se však týká pouze poskytovatelů služby elektronických komunikací a subjektů zajišťujících síť elektronických komunikací, orgánů nebo osob zajišťujících významnou síť, a poskytovatelů digitální služby.[1052] Svou činnost je národní CERT povinen koordinovat s ústředním správním úřadem (NÚKIB), zejména může-li být ohrožena bezpečnost ČR. Náklady provozování národního CERT se zavázalo nést sdružení CZ.NIC, přičemž k financování jsou využívány zejména nejrůznější granty.[1053]

ZKB dále zakotvil vzájemnou spolupráci národního a vládního CERT především na výměně informací o řešení kybernetických bezpečnostních incidentů, na vzdělávání, výzkumu a vývoji. Za klíčovou úlohu národního CERT lze považovat přijímání hlášení o kybernetických bezpečnostních

[1050] Čl. VIII. Veřejnoprávní smlouvy.

[1051] Čl. II. Veřejnoprávní smlouvy.

[1052] Srov. § 17 odst. 1 a 2 ZKB.

[1053] Čl. V. Veřejnoprávní smlouvy.

incidentech, na něž správní úřad reaguje varováním i reaktivními a ochrannými opatřeními, o kterých bylo shora pojednáno.[1054]

3.3.2. Vládní CERT

Bezpečnostním týmem zaměřeným na ochranu kritické informační infrastruktury a informačních systémů veřejné správy[1055] je vládní CERT. Jeho úlohou je přispívat k národnímu i mezinárodnímu systému včasného varování před kybernetickými bezpečnostními hrozbami.[1056]

Vládní CERT slouží jako veřejnoprávní jednotné kontaktní místo pro oblast kybernetické bezpečnosti, které požadovala zřídit i směrnice NIS[1057] vedle požadavku vytvoření jednoho či více bezpečnostních týmů typu CSIRT.[1058] V ČR byl zvolen model vzájemně spolupracujících týmů CSIRT na úrovni osoby soukromého a veřejného práva. Úloha zajistit přeshraniční spolupráci orgánů členských států s relevantními orgány a sítí týmů CSIRT v jiných členských státech a se skupinou pro spolupráci[1059] byla v ČR svěřena vládnímu CERT.

Pracoviště původně vzniklo v rámci Národního centra kybernetické bezpečnosti, jež bylo součástí NBÚ.[1060] V současné době je Národní centrum kybernetické bezpečnosti sekcí NÚKIB, jejíž součástí je i odbor vládního CERT (GovCERT). Jeho oddělení se zabývají kromě řešení kybernetických bezpečnostních incidentů také analýzou síťového provozu, analýzou dat a malware, reverzním inženýrstvím, penetračním testováním, kybernetickou bezpečností průmyslově orientovaných technologií a řídících systémů (SCADA), jakož i vývojem vlastních aplikací pro vnitřní potřebu vládního CERT i pro potřeby spolupráce s externími subjekty.[1061] Informace o

---

[1054] Důvodová zpráva k ZKB. Obecná část. Op. cit., str. 60 a 65.

[1055] Osobní působnost vládního CERT týmu je v § 20 ZKB vymezena orgány a osobami uvedenými v § 3 písm. c) až g) ZKB. Jde o správce a provozovatele informačního i komunikačního systému kritické informační infrastruktury, významného informačního systému, informačního systému základní služby a o provozovatele základní služby.

[1056] Důvodová zpráva k ZKB. Obecná část. Op. cit., str. 15.

[1057] Čl. 1 odst. 2 písm. e) směrnice NIS.

[1058] Čl. 9 směrnice NIS. Úkoly a požadavky na bezpečnostní týmy typu CSIRT jsou uvedeny v příloze I směrnice NIS.

[1059] Čl. 8 odst. 4 a čl. 11 směrnice NIS.

[1060] Usnesením vlády č. 781 ze dne 19. 10. 2011 byl ředitel NBÚ pověřen vybudováním Národního centra kybernetické bezpečnosti, jehož součástí mělo být i vládní koordinační místo pro okamžitou reakci na počítačové incidenty, a to do konce roku 2015. Důvodová zpráva k ZKB. Zvláštní část. Op. cit., str. 83.

[1061] NÚKIB. *Organizační struktura* [online]. Dostupné: https://www.nukib.cz/cs/o-nukib/organizacni-struktura-uradu/ [Cit. 2022-11-22].

hrozbách v oblasti kybernetické bezpečnosti získává vládní CERT nejen z vlastní činnosti, ale i od jiných CERT týmů i z diskuzních fór, studií či analýz antivirových společností.[1062]

Pravomoc a působnost vládního CERT vymezuje § 20 ZKB. Patří sem zejména příjem hlášení o kybernetických bezpečnostních událostech a incidentech, jejich vyhodnocování, metodická podpora a pomoc i součinnost při jejich řešení. Obdobně jako národní CERT se vládní CERT věnuje hodnocení zranitelností v oblasti kybernetické bezpečnosti a vyhodnocování podnětů od dalších orgánů a osob. Eviduje, dále vyhodnocuje, a v případě potřeby též poskytuje údaje týkající se kybernetické bezpečnosti (zejména incidentů), ať se již jedná o informace od národního CERT nebo od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí. Přispívá k zajištění kybernetické bezpečnosti i v jiných členských státech EU tím, že informuje příslušné orgány o kybernetickém bezpečnostním incidentu s významným dopadem na kontinuitu poskytování základních služeb či s dopadem na poskytování digitálních služeb v tomto členském státě. Aby nebyly především osoby soukromého práva odrazeny od sdílení potřebných informací, zákon ukládá vládnímu CERT při sdílení informací zachovávat soukromí, bezpečnost a obchodní zájmy ohlašovatele. V neposlední řadě vládní CERT plní roli týmu CSIRT podle směrnice NIS a spolupracuje s týmy CSIRT ostatních členských států (viz shora).[1063]

3.4. Zvláštní kontrolní orgán Poslanecké sněmovny Parlamentu ČR

Pravomoci NÚKIB lze označit za *„činnosti, které jsou natolik specifické a citlivé, že jejich protiprávní výkon by mohl zasáhnout do ústavně garantovaných práv a svobod”*.[1064] V roce 2017 se NÚKIB vlivem novelizace ZKB[1065] zařadil mezi subjekty, nad nimiž vykonává zvláštní kontrolní pravomoc Poslanecká sněmovna Parlamentu ČR (dále jen „Poslanecká sněmovna”). Navázání nezávislého kontrolního orgánu ústředního správního úřadu na moc zákonodárnou se jeví vhodné i s ohledem na zachování rovnováhy moci výkonné, zákonodárné a soudní ve státě. Zřízení kontrolního orgánu pouze v rámci moci výkonné by s sebou přineslo riziko vychýlení rovnováhy ve prospěch exekutivy.

[1062] PAČKA, Roman. Op. cit., str. 70.

[1063] Srov. § 20 písm. a) až n) ZKB.

[1064] VLÁDA. Důvodová zpráva k zákonu č. 35/2018 Sb. o změně některých zákonů upravujících počet členů zvláštních kontrolních orgánů Poslanecké sněmovny, č. 35/2018 Dz. Obdobně vykonává Poslanecká sněmovna kontrolu nad činností zpravodajských služeb, nakládáním s utajovanými informacemi, či nad činnostmi Finančního analytického úřadu.

[1065] VLÁDA. Důvodová zpráva k zákonu č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony, č. 205/2017 Dz.

V rámci zákonodárné moci se problematiky kybernetické bezpečnosti dotýká rovněž další zvláštní orgán zřízený Poslaneckou sněmovnou PČR, a sice Stálá komise pro hybridní hrozby. Její působení se však neopírá o ustanovení ZKB, jako je tomu v případě kontrolního orgánu NÚKIB. Stálá komise pro hybridní hrozby je zaměřena především na boj s dezinformacemi a na hybridní hrozby ve smyslu operací v oblasti diplomatické, informační, ekonomické, finanční a legislativní.[1066] Následující text se proto zaměří na parlamentní kontrolu NÚKIB zakotvenou v ZKB, kterou provádí Stálá komise pro kontrolu NÚKIB ustavená na půdě Poslanecké sněmovny.

Kontrolu činnosti NÚKIB upravují ustanovení § 24a až 24c ZKB. Zákonná úprava je prakticky shodná s úpravou kontroly činnosti NBÚ stanovenou v § 145 až 147 zákona o ochraně utajovaných informací, která byla předchůdcem kontroly NÚKIB.[1067] Poté, kdy se NÚKIB vyčlenil z NBÚ a stal se samostatným ústředním správním úřadem, považoval zákonodárce za vhodné vzhledem k citlivé povaze jeho činností upravit samostatně i parlamentní kontrolu NÚKIB.

Poslanecká sněmovna vykonává kontrolu NÚKIB skrze svůj zvláštní orgán, který za tím účelem zřizuje. Jeho členové jsou především v kontaktu s ředitelem NÚKIB, který je seznamuje s činností úřadu a předkládá jim návrh jeho rozpočtu i podklady potřebné ke kontrole jeho plnění.[1068] Zákon však nesvěřuje kontrolnímu orgánu ve vztahu k rozpočtu NÚKIB žádné konkrétní pravomoci, byť ukládá jeho kontrolu. Kontrolní orgán tak může případně toliko doporučit vládě navýšení rozpočtu, pokud to považuje za potřebné.[1069]

Kontrolní orgán si rovněž může od ředitele NÚKIB vyžádat zprávu o jednotlivých kybernetických incidentech z kritické informační infrastruktury, významných informačních systémů a informačních systémů základní služby.[1070] Jde o informace, jež nejsou veřejně dostupné. Jelikož jsou schůze kontrolního orgánu neveřejné a jeho členové jsou vázáni povinností mlčenlivosti,[1071] lze se jen dohadovat, do jaké hloubky probíhá faktická kontrola činností NÚKIB při řešení jednotlivých kybernetických bezpečnostních incidentů. Podrobnější informace nelze zjistit ani z

---

[1066] PSPČR. *Stálá komise pro hybridní hrozby: O komisi* [online]. Dostupné: https://www.psp.cz/sqw/hp.sqw?k=8309&o=8 [Cit. 2022-11-22].

[1067] Jediný podstatný rozdíl odpovídá činnosti NÚKIB, neboť se týká možnosti komise vyžádat si zprávu o jednotlivých kybernetických bezpečnostních incidentech, namísto zpráv o řízeních podle zákona o ochraně utajovaných informací.

[1068] § 24a odst. 5 písm. a), b), c) ZKB.

[1069] Po seznámení se s podklady tak učinila např. Stálá komise v aktuálním volební období, když doporučila vládě podpořit činnost NÚKIB zajištěním finančních prostředků. STÁLÁ KOMISE PSPČR PRO KONTROLU ČINNOSTI NÚKIB. *Usnesení č. 4, Ke koncepci rozvoje NÚKIB* [online]. 31. 3. 2022. Digitální depozitář. Dostupné: https://www.psp.cz/sqw/hp.sqw?k=7802 [Cit. 2022-11-22].

[1070] Srov. § 24a odst. 5 písm. e) ZKB.

[1071] § 24c ZKB.

veřejně dostupných dokumentů. Pozvánky na schůze kontrolního orgánu uvádějí jednotlivé body programu k projednání toliko obecně, případně využívají krycích označení projektů.[1072] Bližší informace neuvádějí ani přijatá usnesení, jejichž obsahem je zpravidla údaj o tom, že Stálá komise pro kontrolu NÚKIB vzala na vědomí určitou informaci (např. zprávu o kontrole v oblasti kybernetické bezpečnosti, návrh rozpočtu NÚKIB, apod.).[1073] Obdobně tomu bylo v minulém volebním období za působení předchozího kontrolního orgánu.[1074] Tehdejší kontrolní orgán se však jeví jako aktivnější ve vztahu k počtu vyžádaných zpráv od ředitele NÚKIB i počtu přijatých usnesení.[1075] Vyžádal si například zprávy o kontrolách v oblasti kybernetické bezpečnosti na příslušných ministerstvech i obecně ve státní správě,[1076] jimiž se posléze zabýval.[1077] Dále se věnoval metodické práci NÚKIB, či doporučil seznámit s výsledky kontrol předsedu vlády ČR a ministerstva.[1078] Tehdejší místopředseda kontrolního orgánu v reakci na varování NÚKIB ohledně technologií Huawei a ZTE začal prosazovat využití otevřeného hardware ve státní správě.[1079]

[1072] Např. program pozvánky Stálé komise pro kontrolu NÚKIB na 4. neveřejnou schůzi uvádí projednání informací o aktuálním vývoji projektu BIVOJ. Až z usnesení č. 15 Bezpečnostní rady státu ze dne 12. 4. 2022 vyplývá, že má jít o projekt zajišťující bezpečnost a odolnost klíčové infrastruktury státu prostřednictvím vybudování jednotné komunikační platformy. VLÁDA. *Usnesení č. 15 ze dne 12. 4. 2022* [online]. Dostupné: https://www.vlada.cz/cz/ppov/brs/cinnost/zaznamy-z-jednani/zaznam-ze-schuze-brs-konane-dne-12--dubna-2022-195782/ [Cit. 2022-11-22].

[1073] Pozvánky na schůze Stálé komise pro kontrolu činnosti NÚKIB a její usnesení zveřejňuje Poslanecká sněmovna na svých webových stránkách zde: https://www.psp.cz/sqw/hp.sqw?k=7802 [Cit. 2022-11-22].

[1074] Z uveřejněných usnesení Stálé komise pro kontrolu činnosti NÚKIB pro volební období v letech 2017 až 2021 lze pouze zjistit, že kontrolní orgán přijal informace o zabezpečení voleb do PS, o koncepci rozvoje NÚKIB, projednal stížnost prezidenta VNICTP na postup NÚKIB a neshledal žádné pochybení, zabýval se účastí poslanců z kontrolního orgánu při cestě do Izraele, apod. Konkrétní informace však uveřejněné dokumenty neobsahují. Srov. STÁLÁ KOMISE PSPČR PRO KONTROLU ČINNOSTI NÚKIB. *Usnesení č. 23* [online]. 17. 3. 2021. Digitální depozitář. Dostupné: https://www.psp.cz/sqw/text/text2.sqw?idd=188678 [Cit. 2022-11-22].

[1075] Ačkoli v digitálním depozitáři Poslanecké sněmovny PČR chybí usnesení č. 2, 3 a 4 přijatá v první roce působení kontrolního orgánu, byl kontrolní orgán zejména ve 2. roce svého působení (2019), s počtem 10 přijatých usnesení dotýkajících se nejrůznějších kontrol, poměrně aktivní. Současný kontrolní orgán se dosud v prvním roce svého působení (2022) zabýval, kromě organizačních záležitostí, pouze rozpočtem NÚKIB, koncepcí jeho rozvoje a zprávou o stavu kybernetické bezpečnosti ČR za rok 2021. Viz STÁLÁ KOMISE PSPČR PRO KONTROLU ČINNOSTI NÚKIB. *Usnesení č. 1 až 6* [online]. 21.1.2022, 31.3.2022, 14.7.2022. Digitální depozitář. Dostupné: https://www.psp.cz/sqw/hp.sqw?k=7805&kk=5 [Cit. 2022-11-22].

[1076] STÁLÁ KOMISE PSPČR PRO KONTROLU ČINNOSTI NÚKIB. *Usnesení č. 6* [online]. 25. 4. 2019. Digitální depozitář. Dostupné: https://www.psp.cz/sqw/text/text2.sqw?idd=157640 [Cit. 2022-11-22]. STÁLÁ KOMISE PSPČR PRO KONTROLU ČINNOSTI NÚKIB. *Usnesení č. 10 a č. 11* [online]. 12. 7. 2019. Digitální depozitář. Dostupné: https://www.psp.cz/sqw/hp.sqw?k=7805&o=8&kk=5 [Cit. 2022-11-22].

[1077] Viz kontrola NÚKIB na ministerstvu financí. STÁLÁ KOMISE PSPČR PRO KONTROLU ČINNOSTI NÚKIB. *Usnesení č. 9* [online]. 12. 7. 2019. Digitální depozitář. Dostupné: https://www.psp.cz/sqw/text/text2.sqw?idd=159355 [Cit. 2022-11-22].

[1078] STÁLÁ KOMISE PSPČR PRO KONTROLU ČINNOSTI NÚKIB. *Usnesení č. 7* [online]. 6. 6. 2019. Digitální depozitář. Dostupné: https://www.psp.cz/sqw/text/text2.sqw?idd=158439 [Cit. 2022-11-22].

[1079] Poslanec Ondřej Profant se tématem otevřeného hardware, tedy hardware založeného na otevřeném designu umožňujícího důkladné prozkoumání ze strany uživatelů, zabýval i mimo kontrolní orgán a propagoval jej na svém blogu. SEDLÁK, Jan. *Piráti chtějí v reakci na Huawei a ZTE ve státní správě nasazovat otevřený hardware* [online]. Lupa.cz, 10. 1. 2019. Dostupné: https://www.lupa.cz/aktuality/pirati-chteji-v-reakci-na-huawei-a-zte-ve-statni-sprave-nasazovat-otevreny-hardware/ [Cit. 2022-11-22].

Další pravomocí, která by obecně měla usnadnit výkon kontroly, je oprávnění jednotlivých členů kontrolního orgánu vstupovat v doprovodu ředitele či pověřeného zaměstnance do objektů NÚKIB.[1080] Vůči řediteli NÚKIB disponuje kontrolní orgán jako celek také oprávněním požadovat potřebná vysvětlení, má-li za to, že činnost NÚKIB nezákonně omezuje nebo poškozuje práva a svobody občanů, anebo domnívá-li se, že rozhodovací činnost v rámci správního řízení je stižena vadami.[1081] Pokud by kontrolní orgán jako celek dospěl k závěru, že zaměstnanec NÚKIB porušil zákon při plnění svých povinností upravených v ZKB či v zákoně o ochraně utajovaných informací, musí o tom informovat ředitele NÚKIB a předsedu vlády. Povinnost mlčenlivosti se na oznámení zjištěných pochybení zaměstnanců NÚKIB nevztahuje.[1082]

Vzhledem k povaze parlamentní kontroly zaměřené na exekutivní činnost je vhodné zajistit, aby složení kontrolního orgánu odpovídalo i složení Poslanecké sněmovny podle výsledků posledních voleb. ZKB stanoví, že se zvláštní kontrolní orgán zřízený Poslaneckou sněmovnou skládá nejméně ze sedmi členů, přičemž jeho členem se může stát pouze poslanec Poslanecké sněmovny.[1083] Aby složení kontrolního orgánu NÚKIB odpovídalo politické reprezentaci ČR a aktuálním volebním výsledkům, stanoví ZKB od roku 2018[1084] minimální počet členů kontrolního orgánu na sedm. Úmyslem zákonodárce bylo stanovit konkrétní počet členů tak, *„…, aby byl zastoupen každý poslanecký klub ustavený podle příslušnosti k politické straně nebo politickému hnutí, za něž poslanci kandidovali ve volbách"*.[1085]

V současné době plní funkci kontrolního orgánu Stálá komise pro kontrolu činnosti Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „Stálá komise"), která byla poprvé ustanovena v minulém volebním období (2017 - 2021). Stálá komise působící v současném volebním období se skládá z devíti členů, kteří pocházejí z pěti poslaneckých klubů. Tři poslanci jsou z klubu ANO, dva poslanci z klubu ODS, dva poslanci z klubu STAN, jeden poslanec zastupuje klub KDU-ČSL a jeden poslanec klub SPD.[1086] Mezi členy Stálé komise nejsou

---

[1080] § 24a odst. 4 ZKB.

[1081] § 24b odst. 1 ZKB.

[1082] § 24c ZKB.

[1083] § 24a odst. 1 a 2 ZKB.

[1084] Novelu provedl zákon č. 35/2018 Sb. o změně některých zákonů upravujících počet členů zvláštních kontrolních orgánů Poslanecké sněmovny. Novelu předložil Jan Chvojka, tehdejší poslanec Poslanecké sněmovny a předseda poslaneckého klubu ČSSD.

[1085] § 24a odst. 2 ZKB, věta druhá před středníkem.

[1086] PSPČR. *Stálá komise pro kontrolu činnosti Národního úřadu pro kybernetickou a informační bezpečnost* [online]. Dostupné: https://www.psp.cz/sqw/hp.sqw?k=7801 [Cit. 2022-11-22].

zastoupeni poslanci poslaneckého klubu České pirátské strany ani TOP 09, ačkoli tyto kluby byly na půdě Poslanecké sněmovny v současném volebním období ustaveny. Přesto má poslanecký klub ANO 2011 ve Stálé komisi tři členy. Ačkoli došlo k navýšení počtu členů Stálé komise na devět, její aktuální složení neodpovídá účelu novelizované zákonné úpravy, jímž je zajistit v kontrolních komisích zastoupení všech poslaneckých klubů, a tím reflektovat volební výsledky i ve zvláštních orgánech Poslanecké sněmovny.

Lze souhlasit s myšlenkou, podle níž by se vůle voličů měla promítnout nejen do složení Poslanecké sněmovny, ale i do složení jejích zvláštních orgánů tak, aby v nich měly zajištěnu účast i opoziční poslanci. Zároveň nelze považovat přílišné navyšování počtu členů za efektivní. Zákon sice stanoví jako pojistku pro patové situace nutnost lichého počtu členů, jejich vysoký počet by však mohl paralyzovat faktickou kontrolní činnost orgánu. Nadto u kontrolních orgánů, jejichž členové se seznamují s utajovanými informacemi, by s ohledem na související rizika nebylo rozumné, aby docházelo k navyšování počtu osob obeznámených o utajovaných skutečnostech. Navýšení počtu členů nyní působící Stálé komise o dva členy, aniž by zároveň došlo k zajištění účasti poslanců ze všech poslaneckých klubů, se tudíž nejeví jako odůvodněné a neodpovídá ani smyslu zákonné úpravy.

Závěr

V dizertační práci jsem si kladla za cíl zkoumat problematiku kybernetické bezpečnosti v širších teoretických i praktických souvislostech. Ačkoli lze Českou republiku označit za vyspělou zemi s vysokou mírou rozšíření a využívání moderních technologií, která má od roku 2014 i vlastní zákonnou úpravu kybernetické bezpečnosti, zůstává právní úprava kybernetické bezpečnosti z hlediska akademické obce opomíjenou oblastí, jak jsem podrobněji popsala v úvodu této práce. Především to platí o zákonných institutech zajištění kybernetické bezpečnosti. Proto jsem považovala za účelné pojednat o právní úpravě kybernetické bezpečnosti, potažmo bezpečnosti informací v kyberprostoru, v širších souvislostech a nabídnout vlastní úvahy k tématu.

Úvodem disertační práce jsem si stanovila několik dílčích cílů:

1. Popsat a objasnit společenské proměny související s globalizací a technologickým pokrokem, klíčové hodnoty a principy informační společnosti a působení právních norem v kyberprostoru, neboť bez detailnějšího rozboru uvedených témat by nebylo možné komplexně pojednat o právní úpravě kybernetické bezpečnosti.

2. Objasnit úlohu státu a limity veřejné moci při zajištění kybernetické bezpečnosti nejen z pohledu občanů ČR, ale i z hlediska mezinárodního společenství suverénních států, neboť kybernetické operace mohou zapříčinit vznik mezinárodní odpovědnosti státu.

3. Pojednat o českém zákoně o kybernetické bezpečnosti, o jeho vývoji a o klíčových zákonných institutech zajištění kybernetické bezpečnosti, tj. zejména o různých opatřeních, včetně těch, která může vydat NÚKIB, ústřední správní úřad kybernetické bezpečnosti.

1. Ke společenským proměnám, hodnotám a principům informační společnosti, a k působení právních norem v kyberprostoru:

Vlivem rozvoje ICT došlo k posunu ve významu pojmů jako veřejný prostor, okolní společnost, či zveřejnění informace. Řada veřejných politik rovněž vnímá nutnost reagovat na kybernetické incidenty a útoky, jež dopadají na fungování základních služeb ve státě. V EU i ČR je v oblasti kybernetické bezpečnosti a v oblasti regulace informačních a komunikačních systémů a sítí patrný ústup od liberálního smýšlení, a to ve prospěch zavádění právních institutů, které mají zajistit vyšší bezpečnost. Vzhledem k dosavadnímu rozšiřování orgánů a osob, jimž český zákonodárce uložil na poli kybernetické bezpečnosti povinnosti, a s ohledem na nárůst počtu systémů ICT přitom lze očekávat, že okruh povinných subjektů i povinností bude do budoucna stále narůstat.

Co se týče hodnot a principů ovlivňujících právní úpravu, klíčovou je pro informační společnost především informační svoboda, tj. svoboda projevu i svoboda šířit a přijímat informace. Dalším stěžejním principem je právo informačního sebeurčení zaručující možnost svobodně se rozhodnout, jaké informace a v jakém rozsahu bude jedinec sdílet s okolní společností. Jakkoli jde o stěžejní hodnoty, ve společnosti jsou více či méně vyvažovány důrazem na bezpečnost. Míra, v níž se společnost přikloní spíše k bezpečnosti či k informační svobodě a informačnímu sebeurčení, závisí na politické situaci a aktuálních bezpečnostních podmínkách dané země.

V oblasti kybernetické bezpečnosti nabývají zásadního významu dále principy technologické neutrality, ochrany nedistributivních práv, minimalizace státního donucení, autonomie vůle regulovaných subjektům a princip bdělosti státu vůči ostatním státům a mezinárodnímu společenství. Klíčové jsou i obecné principy správního práva, zejména principy dobré správy a související princip odpovědnosti veřejné správy, respektive odpovědnosti státu (*due diligence*). Právní úprava kybernetické bezpečnosti jako soubor právních norem, jimiž jsou ukládány povinnosti osobám odlišným od státu, je totiž zvláštním odvětvím veřejného práva, jehož základem je autoritativní rozhodování o právech a povinnostech jiných osob s cílem spravovat kyberprostor.

Co se týče působení právních norem v kyberprostoru, jeví se původní myšlenky zachovat část kyberprostoru - zejména Internet, bez státní regulace zvenčí jako nepřijatelné. Kybernetická bezpečnost je jako součást národní bezpečnosti příkladem veřejného dobra. Rezignovat na jakékoli kontrolní mechanismy by znamenalo volit cestu, v níž přežijí ti silnější. Taková úvaha není v moderním státě, který respektuje hodnoty lidství a chrání práva a svobody svých občanů, přípustná. Byť je faktická vymahatelnost právních norem ve virtuálním prostředí obtížná, nesmí se stát důvodem rezignace na regulaci právních vztahů a ochranu základních práv a svobod i veřejného zájmu. Specifika kybernetického prostředí nemohou automaticky vést k negaci práva.

Nahrazení právní normy kódem či technickými normami se nezdá pro kyberprostor vhodné. Ačkoli by se kód či technická pravidla mohly jevit efektivnějším způsobem regulace kybernetického prostředí, problémem by bylo prvotní zakódování hodnot, neboť to se nutně odvíjí od konkrétních hodnotových hledisek definiční autority. Výsledné kódování by tak mohlo vést k neférové regulaci a nespravedlnostem.

2. K úloze státu a k limitům veřejné moci při zajištění kybernetické bezpečnosti:

Stát nemůže rezignovat na ochranu svých zájmů v kyberprostoru, a nesmí tak učinit ani ve vztahu k zabezpečení základních práv a svobod svých občanů. Výkon státní moci však nesmí překročit zákonné mantinely. Přes specifika kybernetického prostředí není důvodu, aby se v něm neuplatil ústavní princip vázanosti státní moci zákonem. Případ činnosti Vojenského zpravodajství na poli kybernetické obrany ČR před okamžikem nabytí účinnosti v práci rozebírané novely ZVZ dokládá, že je nutné na uvedeném základním ústavním principu bezpodmínečně trvat i v kyberprostoru.

V rámci mezinárodního společenství suverénních států se mnohé státy uchylují k prosazování svých politických cílů kybernetickými prostředky. I v kyberprostoru jsou však státy povinny respektovat mezinárodní právní řád. Z hlediska mezinárodního práva nabývá na důležitosti zejména druhá verze Tallinnského manuálu, soft law dokumentu, který dosud není v českém jazyce dostupný a jehož vybraná ustanovení jsem pro potřeby této práce přeložila a rozebrala.

Původci i oběťmi kybernetických útoků jsou kromě států i soukromé subjekty, jejichž působení některé státy na svém území z různých důvodů tolerují, a jejichž úloha bude v kybernetické bezpečnosti i nadále významná. Státy však mají z hlediska mezinárodního práva povinnost neumožnit zneužití svého území k páchání protiprávních činů vůči ostatním státům. Ačkoli mezinárodní právo dopadá na kybernetické operace nestátních aktérů v omezené míře, za určitých podmínek lze činy nestátních aktérů přičíst konkrétnímu státu a založit jeho mezinárodněprávní odpovědnost. Státům se však přičítají především kybernetické operace prováděné státními orgány, tj. orgány moci zákonodárné, výkonné a soudní. Mezinárodní odpovědnost státu bude v zásadě dovozena i v případech překročení svěřených pravomocí k výkonu státní moci.

Rozhodne-li se stát reagovat na kybernetický útok jiného státu, měl by mít k dispozici důkazní prostředky k prokázání přičitatelnosti kybernetického útoku jinému státu, což bývá obtížné. Lze se proto setkat s postojem, který v případě kybernetického útoku obhajuje využití zpětného hackingu (*hack-back*) jako alternativy přicházející v úvahu namísto výkonu veřejné moci. Pokud se však státy či nestátní aktéři ke zpětnému hackingu uchýlí, musejí být schopni obhájit, že jednají po právu. Mezinárodní právní řád se totiž vztahuje na veškeré kybernetické operace. Na základě rozboru argumentů pro i proti jsem v práci dospěla k závěru, že zpětný hacking by neměl být umožněn jako běžná reakce na kybernetický útok, tedy reakce, kterou lze automaticky považovat jako po právu a k níž se lze běžně uchýlit.

3. K českému zákonu o kybernetické bezpečnosti a k opatřením NÚKIB k zajištění kybernetické bezpečnosti:

ČR zajišťuje prevenci před narušením bezpečnosti informací v informačních systémech, bezpečnosti služeb a bezpečnosti a integrity sítí elektronických komunikací především skrze správní činnost NÚKIB, který je ústředním správním úřadem v oblasti kybernetické bezpečnosti. K zajištění kybernetické bezpečnosti NÚKIB vydává opatření v užším slova smyslu, tedy varování, reaktivní opatření a ochranné opatření. Z hlediska odborné literatury jde o opomíjenou správní činnost. Narozdíl od bezpečnostních opatření reagují opatření v užším slova smyslu již na konkrétní kybernetickou bezpečnostní hrozbu či kybernetický bezpečnostní incident. U opatřeních v užším slova smyslu jsem dospěla k následujícím závěrům:

Varování lze právní formou zařadit mezi tzv. jiné úkony podle části čtvrté správního řádu. Institut varování má značný potenciál ovlivnit politickou, ekonomickou i bezpečnostní situaci v ČR. Kromě informování o doporučených postupech obrany před kybernetickými útoky dosud NÚKIB varoval před dvěma konkrétními technologickými společnostmi i před neplněním smluvních závazků dodavatelů s významným vztahem k Ruské federaci, a rovněž ovlivnil zadávání veřejných zakázek. Ačkoli se varování jeví jako doporučení, jeho nezohlednění může mít pro povinné subjekty negativní dopady. S ohledem na právní formu varování je individuální právní ochrana komplikovanější, jelikož varování nelze napadnout samostatnou správní žalobou.

Reaktivní opatření umožňuje autoritativně nařídit zavedení bezpečnostních opatření u konkrétního orgánu či osoby, které jsou dotčeny kybernetickým bezpečnostním incidentem, případně u okruhu orgánů nebo osob určených podle daného kritéria. Narozdíl od varování lze reaktivním opatřením již přímo zasáhnout do práv a povinností jiných osob. Dosud uveřejněná reaktivní opatření ve formě opatření obecné povahy obsahují podrobná zdůvodnění závažnosti kybernetických bezpečnostních incidentů a poukazují na zásadní důvody, pro které správní úřad přistoupil k jejich vydání. Opatření obecné povahy se ukazuje jako vhodná právní forma správního aktu, jelikož zjištěné zranitelnosti počítačových systémů nebo sítí a služeb elektronických komunikací, které zpravidla mohou za nastalé kybernetické bezpečnostní incidenty, je zapotřebí řešit ve vztahu k širokému okruhu orgánů a osob. Tyto orgány a osoby by mohly být jen obtížně jednotlivě určeny ve správním rozhodnutí, a ani by to nemuselo být dostatečně efektivní.

Smyslem ochranného opatření je zvýšit ochranu informačních systémů nebo služeb a sítí elektronických komunikací. Ochranné opatření je v podstatě prostředkem, který umožňuje hromadně se poučit z vlastních chyb. Ústřední správní úřad vybraným povinným subjektům toto

hromadné ponaučení autoritativně nařizuje. Narozdíl od reaktivního opatření není možné u ochranného opatření zvolit formu správního rozhodnutí. Právní forma odpovídá logikou smyslu ochranného opatření a snaze zamezit opakování kybernetického bezpečnostního incidentu. Ochranné opatření se proto musí vztahovat na širší, individuálně neurčený okruh orgánů a osob. Dosud NÚKIB uveřejnil na své úřední desce jediné ochranné opatření, jehož odůvodnění mimo jiné obsahuje i relativně samostatnou část týkající se toliko technického odůvodnění výroku opatření obecné povahy. S určitou nadsázkou se tak skládá z části určené pro právníky a z části určené pro informatiky. Tato úprava přispívá k přehlednosti a srozumitelnosti. Mohla by se u správních aktů z oblasti kybernetické bezpečnosti do budoucna osvědčit, pokud budeme předpokládat vzrůstající nároky na jejich technické odůvodnění.

Kromě nastavení pravidel systému zajišťujícímu kybernetickou bezpečnost přispěl český zákon o kybernetické bezpečnosti také k větší transparentnosti provozu národního bezpečnostního počítačového týmu. Zákon totiž obsahuje podmínky pro uzavírání veřejnoprávní smlouvy k provozování národního CERT. Zákonná úprava je tak důkazem, že na poli kybernetické bezpečnosti dochází zčásti k přesunu pravomocí veřejné správy na soukromé subjekty. Příkladem privatizace veřejné správy je právě působnost bezpečnostního týmu - národního CERT.

Po novele z roku 2017 zákon o kybernetické bezpečnosti upravuje též podmínky kontroly ústředního správního úřadu kybernetické bezpečnosti. NÚKIB zařadil mezi subjekty, nad nimiž vykonává zvláštní kontrolní pravomoc Poslanecká sněmovna Parlamentu ČR. Navázání nezávislého kontrolního orgánu ústředního správního úřadu na moc zákonodárnou lze hodnotit jako vhodné, a to s ohledem na zachování rovnováhy moci výkonné, zákonodárné a soudní ve státě. Text nicméně ukazuje, že v současném volebním období složení kontrolního orgánu nereflektuje složení Poslanecké sněmovny Parlamentu ČR, ačkoli právě to bylo smyslem novelizace zákona o kybernetické bezpečnosti upravující počet členů Stálé komise pro kontrolu činnosti NÚKIB.

Lze uzavřít, že přes značná specifika kybernetického prostředí zůstává právo vhodným nástrojem jeho regulace. Současně je nutné i v kyberprostoru důsledně trvat na ústavním principu vázanosti státní moci zákonem.

Seznam zkratek

Akt EU o kybernetické bezpečnosti	Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA (Agentuře Evropské unie pro kybernetickou bezpečnost) a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií (akt o kybernetické bezpečnosti)
BIS	Bezpečnostní informační služba
ČLR	Čínská lidová republika
ČR	Česká republika
Důvodová zpráva k ZKB	VLÁDA. Důvodová zpráva k zákonu č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), č. 181/2014 Dz.
ENISA	Agentura Evropské unie pro bezpečnost sítí a informací
ESLP	Evropský soud pro lidská práva
EU/Unie	Evropská unie
EÚLP	Evropská úmluva o ochraně základních lidských práv a svobod
ICT	Informační a komunikační technologie
Kontrolní řád	Zákon č. 255/2012 Sb., o kontrole (kontrolní řád)
Krizový zákon	Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů
Listina základních práv a svobod	Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky
Listina základních práv EU	Listina základních práv Evropské unie, 2012/C 326/02, Dokument 12016P/TXT
NATO	Severoatlantická aliance
NÚKIB	Národní úřad pro informační a kybernetickou bezpečnost
OECD	Organizace pro hospodářskou spolupráce a rozvoj
Sb.	Sbírka zákonů
Směrnice NIS/ směrnice o kybernetické	

bezpečnosti sítí a informačních systémů	Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii
správní řád	Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů
s.ř.s.	Zákon č. 150/2002 Sb., soudní řád správní, ve znění pozdějších předpisů
Trestní zákoník	Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů
USA	Spojené státy americké
Úmluva o počítačové kriminalitě	Úmluva Rady Evropy č. 185 ze dne 23. listopadu 2001 o počítačové kriminalitě. Ministerstvem zahraničních věcí ČR vyhlášena pod č. 104/2013 Sb. m. s.
Ústava ČR	Ústavní zákon č. 1/1993 Sb., Ústava České republiky
Ústavní zákon o bezpečnosti ČR	Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky
ÚZSI	Úřad pro zahraniční styky a informace
Vyhláška o kybernetické bezpečnosti	Vyhláška NÚKIB č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat
Vyhláška o bezpečnosti ICT	Vyhláška NBÚ č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor
VZ	Vojenské zpravodajství
Zákon o odpovědnosti za škodu	Zákon č. 82/1998 Sb., o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem a o změně zákona České národní rady č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád)
Zákon o ochraně	

utajovaných informací	Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti
Zákon o technických požadavcích	Zákon č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů
Zákon o zpravodajských službách	Zákon č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů
ZEK	Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů
ZKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů
ZVZ	Zákon č. 289/2005 Sb., o Vojenském zpravodajství

Seznam použitých zdrojů

1. Seznam použité literatury

Monografie a kolektivní monografie, včetně vybraných kapitol:

AWAN, Imran, BLAKEMORE, Brian (eds.). *Policing cyber hate, cyber threats and cyber terrorism*. 1. vyd. Farnham: Ashgate, 2012.

BARTOŇ, Michal. *Svoboda projevu a její meze v právu ČR.* Praha: Linde, 2002.

BIRKINSHAW, Patrick. *Freedom of information: the law, the practice, and the ideal.* 4th ed. Cambridge University Press, 2010.

CASTELLS, Manuel. *The Information Age: Economy, Society and Culture, vol. I, The rise of the network society.* 1. vydání. Malden: Blackwell, 1996.

CASTELLS, Manuel. *End of Millennium, The Information Age: Economy, Society and Culture, vol. III.* 2. vydání. Chichester: Blackwell Publishers, 2010.

DWORKIN, Ronald. *Law's empire*. London: Fontana Press, 1991.

EICHLER, Jan. *Terorismus a války v době globalizace*. 2., dopl. vyd. Praha: Karolinum, 2010.

HALLEVY, Gabriel. *Liability for Crimes Involving Artificial Intelligence Systems*. Springer International Publishing Switzerland, 2015.

KASL, František. *Porušení bezpečnosti osobních údajů v kontextu internetu věcí.* Brno: Masarykova univerzita, 2021.

KNAPP, Viktor. *O možnosti použití kybernetických metod v právu.* 1. vydání. Praha: Nakladatelství československé akademie věd, 1963.

KNAPP, Viktor a kolektiv. *Právo a informace.* Praha: Academia, 1988.

KNAPP, Viktor. *Velké právní systémy: Úvod do srovnávací právní vědy*. Praha: Beck, 1996.

KOLB, Robert. *The international law of state responsibility: an introduction*. Cheltenham, UK: Edward Elgar Publishing, 2017.

KOLOUCH, Jan. *Cybercrime* [online]. Praha: CZ.NIC, 2016. Dostupné: https://knihy.nic.cz/files/edice/cybercrime.pdf. [Cit. 2022-10-22].

KOLOUCH, Jan, BAŠTA, Pavel a kol. *CyberSecurity* [online]. Edice CZ.NIC, 2019. Dostupné: https://knihy.nic.cz/files/edice/cybersecurity.pdf. Všechny odkazy [Cit. 2022-09-21].

KOOPS, Bert-Jaap (ed.). *Cybercrime and jurisdiction: a global survey*. 1. vyd. The Hague: T.M.C. Asser press, 2006.

KOOPS, Bert-Jaap. Ten Dimensions of Technology Regulation - Finding Your Bearings in the Research Space of an Emerging Discipline [online]. In: GOODWIN, Morag E. A. et al. (eds.). *Dimensions of Technology Regulation*. Nijmegen: WLP, 2010. Tilburg Law School Research Paper No. 015/2010. Dostupné: https://ssrn.com/abstract=1633985 [Cit. 2022-11-01].

LESSIG, Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999.

LESSIG, Lawrence. *Code. Version 2.0* [online]. New York: Basic Books, 2006. Dostupné: https://lessig.org/product/codev2/ [Cit. 2022-10-27].

MAISNER, Martin, VANÍČEK, Zdeněk. *Odpovědnost za obsah přenosu v elektronických komunikacích*. 1. vyd. Praha: Wolters Kluwer Česká republika, 2012.

MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí* [online]. 1. vyd. Praha: CZ.NIC, 2013. Dostupné: https://knihy.nic.cz/files/edice/internet_jako_objekt_prava.pdf [Cit. 2022-10-27].

POLČÁK, Radim. *Právo na internetu: spam a odpovědnost ISP*. 1. vyd. Brno: Computer Press, 2007.

POLČÁK, Radim. Autoritativní regulace kyberprostoru a legitimita trestního práva. In: GŘIVNA, Tomáš; POLČÁK, Radim (eds.). *Kyberkriminalita a právo*. 1. vyd. Praha: Auditorium, 2008.

POLČÁK, Radim. *Internet a proměny práva.* 1. vyd. Praha: Auditorium, 2012.

POLČÁK, Radim, HARAŠTA, Jakub, STUPKA, Václav. *Právní problémy kybernetické bezpečnosti*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2016.

POMAHAČ, Richard. Právní principy dobré správy – imaginace či realita? In: KUČERA, Stanislav, BOGUSZAK, Jiří (eds). *Právní principy: kolokvium*. Pelhřimov: Vydavatelství 999, 1999.

RAMEŠOVÁ, Kristina. Kyberprostor a projevy moci výkonné, aneb nenápadné vytěžení vlivu definičních autorit. In: TRYZNA, Jan (ed.). *Dělba moci a její proměny*. Praha: Auditorium, 2019.

SALEM, Fadi. *The Arab World Online 2017: Digital Transformations and Societal Trends in the Age of the 4th Industrial Revolution* [online]. Vol. 3. Dubai: MBR School of Government, 2017. Dostupné: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3059445 [Cit. 2021-10-31].

SEDLÁK, Petr, KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021.

SMEJKAL, Vladimír; SOKOL, Tomáš; VLČEK, Martin. *Počítačové právo*. 1. vyd. Praha: C.H. Beck, 1995.

SMEJKAL, Vladimír. *Právo informačních a telekomunikačních systémů*. 2. vyd. Praha: C.H. Beck, 2004.

SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Aleš Čeněk, 2015.

SMEJKAL, Vladimír, SOKOL, Tomáš, KODL, Jindřich. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti.* Plzeň: Aleš Čeněk, 2019.

SOLIS, Gary D. *The Law of Armed Conflict: International Humanitarian Law in War.* 3. vydání. Cambridge: Cambridge University Press, 2021.

ŠTURMA, Pavel. Mezinárodní odpovědnost za škodlivé následky činností nezakázaných mezinárodním právem. *Mezinárodní odpovědnost*. 1. vyd. Brno : Masarykova univerzita, 2003.

ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o, 2018.

TRYZNA, Jan. *Právní principy a právní argumentace: k vlivu právních principů na právní argumentaci při aplikaci práva*. Praha: Auditorium, 2010.

YAR, Majid. *Cybercrime and society: crime and punishment in the information age*. 2. vyd. Thousand Oaks, CA: SAGE Publications, 2013.

WALL, David. *Cybercrime: the transformation of crime in the information age*. 1. vyd. Cambridge: Polity, 2007.

WINTR, Jan. *Říše principů: obecné a odvětvové principy současného českého práva*. Praha: Karolinum, 2006.

WOLTAG, Johann-Christoph. Computer Network Operations During an International Armed Conflict. In: *Cyber Warfare: Military Cross-Border Computer Network Operations under International Law.* Intersentia, 2014.

ZIOLKOWSKI, Katharina. *Confidence Building Measures for Cyberspace - Legal Implications* [online]. Tallinn: NATO CCD COE, 2013. Dostupné: https://ccdcoe.org/uploads/2018/10/CBMs.pdf [Cit. 2022-11-12].

ZAVRŠNIK, Aleš. Definiční problémy a kriminologická specifika kyberzločinu. In: GŘIVNA, Tomáš; POLČÁK, Radim (eds.). *Kyberkriminalita a právo*. 1. vyd. Praha: Auditorium, 2008.

Učebnice a komentáře:

CRAWFORD, James. *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries.* Cambridge: Cambridge University Press, 2003.

ČEPELKA, Čestmír, ŠTURMA, Pavel. *Mezinárodní právo veřejné*. Praha: Eurolex Bohemia, 2003.

ČEPELKA, Čestmír, JÍLEK Dalibor, ŠTURMA, Pavel. *Mezinárodní odpovědnost*. Brno: Masarykova univerzita, 2003.

ČEPELKA, Čestmír, ŠTURMA, Pavel, BÍLKOVÁ, Veronika. *Kodifikace a rozvoj mezinárodního práva: kodifikace mezinárodního práva, právo mezinárodních smluv, právo mezinárodní odpovědnosti*. Praha: Eva Rozkotová - IFEC, 2008.

GERLOCH, Aleš. *Teorie práva*. 7. vyd. Plzeň: Aleš Čeněk, 2017.

HUSSEINI, Faisal, BARTOŇ, Michal, KOKEŠ, Marian, KOPA, Martin a kol. *Listina základních práv a svobod.* 1. vydání (1. aktualizace). Praha: C. H. Beck, 2021.

FILIP, Jan. *Vybrané kapitoly ke studiu ústavního práva.* Brno: Masarykova univerzita, 2001.

GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana. *Kriminologie*. 4. aktualizované vydání Praha: Wolters Kluwer, 2014.

HENDRYCH, Dušan a kol. *Správní právo. Obecná část.* 9. vydání. Praha: C. H. Beck, 2016.

JELÍNEK, Jiří, DANKOVÁ, Katarína, TLAPÁK NAVRÁTILOVÁ, Jana, PELC, Vladimír, ŘÍHA, Jiří, STEJSKAL, Vojtěch. *Trestní právo hmotné: obecná část, zvláštní část*. 5. aktualizované a doplněné vydání. Praha: Leges, 2016.

JEMELKA, Luboš, PONDĚLÍČKOVÁ, Klára, BOHADLO, David. *Správní řád*. 6. vydání. Praha: C. H. Beck, 2019.

KLÍMA, Karel a kol. *Evropské právo.* Plzeň: Aleš Čeněk, 2011.

KLOUČKOVÁ, Světlana, FENYK, Jaroslav. *Mezinárodní justiční spolupráce v trestních věcech*. 2., aktualiz. a dopl. vyd. Praha: Linde, 2005.

MAISNER, Martin. VLACHOVÁ, Barbora. *Zákon o kybernetické bezpečnosti: Komentář*. Praha: Wolters Kluwer, 2015.

MORAND-DEVILLER, Jacqueline. *Cours de droit administratif.* Paris: Montchrestien, 1989.

POLČÁK, Radim, ŠKOP, Martin, MACEK, Jakub. *Normativní systémy v kyberprostoru: (úvod do studia).* 1. vyd. Brno: Masarykova univerzita, 2005.

POLICEJNÍ AKADEMIE ČR. *Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech*. Praha: Policejní akademie České republiky v Praze, 2020.

POLICEJNÍ AKADEMIE ČR. *Bezpečnostní výzvy současného světa.* Praha: Policejní akademie České republiky v Praze, 2020.

POMAHAČ, Richard, HANDRLICA, Jakub. *Evropské správní právo*. Praha: C.H. Beck, 2012.

PORADA, Viktor a kol. *Bezpečnostní vědy. Úvod do teorie a metodologie*. Plzeň: Aleš Čeněk, 2017.

POTĚŠIL, Lukáš, HEJČ, David, RIGEL, Filip, MAREK, David. *Správní řád*. 2. vydání. Praha: C. H. Beck, 2020.

SLÁDEČEK, Vladimír, MIKULE, Vladimír, SUCHÁNEK, Radovan, SYLLOVÁ, Jindřiška. *Ústava České republiky*. 2. vydání. Praha: C. H. Beck, 2016

ŠÁMAL, Pavel. *Trestní zákoník: komentář*. Sv. 1, § 1 – 139. [Obecná část]. 2. vyd. V Praze: C.H. Beck, 2012.

TOMÁŠEK, Michal, TÝČ, Vladimír, PETRLÍK, David a kol. *Právo Evropské unie*. 3. aktualizované vydání. Praha: Leges, 2021.

VOJTEK, Petr, BIČÁK, Vít. *Odpovědnost za škodu při výkonu veřejné moci.* 4. vydání. Praha: C. H. Beck, 2017.

WÁGNEROVÁ, Eliška, ŠIMÍČEK, Vojtěch, LANGÁŠEK, Tomáš, POSPÍŠIL, Ivo a kol. *Listina základních práv a svobod. Komentář.* Praha: Wolters Kluwer, 2014.

Sborníky:

BROADHURST, Roderic, GRABOSKY, Peter, ALAZAB, Mamoun, BOUHOURS, Brigitte, CHON, Steve, DA, Chen. Crime in Cyberspace: Offenders and the Role of Organized Crime Groups [online]. *Australian National University Cybercrime Observatory,* 2013. Dostupné: http://ssrn.com/abstract=2211842 [Cit. 2022-11-11].

BUCHAN, Russell. Cyber Espionage and International Law. In: TSAGOURIAS, Nicholas, BUCHAN, Russell. *Research Handbook on International Law and Cyberspace*. Edward Elgar, 2015.

ČAPEK, Jan, HUB, Miloslav, ROUDNÝ, Radim, KOPÁČKOVÁ, Hana, FUKA, Jan, IBL, Martin. *Vybrané aspekty kybernetické bezpečnosti*. Pardubice: Univerzita Pardubice, Ekonomicko-správní fakulta, 2015.

HANDRLICA, Jakub. Veřejná správa na rozcestí administrativního pluralismu. In: PAPÁČOVÁ, I. (ed). *Verejná správa na rázcestí*. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta. 2018

KUČERA, Stanislav, BOGUSZAK, Jiří. (eds.). *Právní principy: kolokvium*. Pelhřimov: Vydavatelství 999, 1999.

PORADA, Viktor, RAIS, Karel, SMEJKAL, Vladimír. *Právní, kriminalistické a kybernetické aspekty kybernetické kriminality a bezpečnosti: pocta Vladimíru Smejkalovi*. Brno: Akademické nakladatelství CERM, 2021.

Slovníky a encyklopedie:

CNSS. *Committee on National Security Systems (CNSS) Glossary* [online]. April 6, 2015. Dostupné: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf [Cit. 2022-11-10].

COHEN-ALMAGOR, Raphael. Cyberterrorism [online]. In: WARF, Barney (eds.) *SAGE Encyclopedia of the Internet.* Thousand Oaks, California, 2018. Dostupné: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3192089 [Cit. 2022-10-24].

HENDRYCH, Dušan a kol. *Právnický slovník*. 3. vydání. Praha: C. H. Beck, 2009.

HINDLS, Richard, HOLMAN, Robert, HRONOVÁ, Stanislava. *Ekonomický slovník*. 1. vyd. Praha: Beck, 2003.

JIRÁSEK, Petr, NOVÁK, Luděk, POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti* [online]. 3. aktualizované vydání. Praha: AFCEA, 2015. Dostupné: https://afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf [Cit. 2022-11-10].

WIKIPEDIA : The Free Encyclopedia. *Cyberattack* [online]. St. Petersburg (Florida) : Wikimedia Foundation, 2001-. Anglická verze. Dostupné: https://en.wikipedia.org/wiki/Cyberattack [Cit. 2022-11-10].

ZOUHAR, Jiří, WOODCOCK, JoAnne. *Slovník výpočetní techniky*. 1. vyd. Praha: Microsoft Press, Plus s.r.o., 1993.

Ostatní publikace:

BEZDÍČEK, Viktor. O zveřejňování nezveřejnitelného: Clintonova aféra a informační společnost. In: BĚLOHRADSKÝ, V. *Mezi světy & mezisvěty: reloaded 2013*. 2., opr. a rozšíř. vyd. Praha: Novela bohemica, 2013.

DONÁT, Josef, TOMÍŠEK, Jan. *Právo v síti: průvodce právem na internetu*. V Praze: C.H. Beck, 2016.

DOUCEK, Petr, KONEČNÝ, Martin, NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnost informací*. 1. vydání. Praha: Professional Publishing s.r.o., 2019.

DOYLE, Arthur Conan. *Údolí strachu* [online]. 1. vyd. Praha : Městská knihovna v Praze, 2012. Dostupné: <http://web2.mlp.cz/koweb/00/03/34/76/87/udoli_strachu.pdf> [Cit. 2022-11-08].

EVROPSKÁ KOMISE. *Společné sdělení Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů. Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor /* JOIN/2013/01 final */* . Dokument 52013JC0001.

HÁLA, Vojtěch. *Rozvoj ICT v ČR a jeho regionální aspekty* [online]. Brno, 2009. Diplomová práce. Masarykova univerzita, Ekonomicko-správní fakulta. Vedoucí práce prof. RNDr. Milan Viturka, CSc. Dostupné: https://thesis.cz/id/hi76m0/ [Cit. 2022-10-23].

HOBBES, Thomas; CHOTAŠ, Jiří; MASOPUST, Zdeněk; BARABAS, Marina (eds.). *Leviathan, aneb, Látka, forma a moc státu církevního a politického*. 1. vyd. Překlad Karel Berka. Praha: OIKOYMENH, 2009.

HOMÉR. *Ílias*. 9. vydání. Praha: Odeon 1980.

HUSOVEC, Martin. *Zodpovednosť na internete* [online]. Edice CZ.NIC, 2014. Dostupné: https://knihy.nic.cz/files/edice/zodpovednost_na_internete.pdf [Cit. 2022-10-24].

CHANG, Lennon Y. C. *Cybercrime in the Greater China Region: Regulatory Response and Crime Prevention across the Taiwan Strait* [online]. Edward Elgar, 2012. Dostupné: https://www.researchgate.net/publication/301693009_Cybercrime_in_the_Greater_China_Region_Regulatory_Response_and_Crime_Prevention_across_the_Taiwan_Strait [Cit. 2022-11-11].

ILC. Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, 2001, UN Doc. A/56/10.

JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* 1. vyd. Praha: Grada, 2007.

KAYUMBA, David, *State Sovereignty Versus Individual Rights in the Case of the 1994 Genocide in Rwanda* [online]. Entebbe, 2006. Diplomová práce. Nkumba University, School of Social Sciences. Vedoucí práce Dr. Michael Mawa. Dostupné: https://ssrn.com/abstract=1831542 [Cit. 2022-11-15].

KISLINGEROVÁ, Eva. *Nová ekonomika: nové příležitosti?*. V Praze: C.H. Beck, 2011.

KLIMBURG, Alexander (ed). *National Cyber Security Framework Manual, NATO CCD COE Publication* [online]. Tallinn 2012. Dostupné: https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf [Cit. 2022-11-10].

KŘOVÁK, Jiří. *Nová ekonomika, sociálně-ekonomická implikace, implikace pro statistiku.* Praha: Český statistický úřad - případová studie, 2001.

MOC, Michal. *Bezpečné užívání internetu: metodická příručka*. Praha: Centrum pro studium vysokého školství, v.v.i, 2015.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Managing Information Security Risk: Organization, Mission, and Information System View* [online]. March 2011. Dostupné: https://csrc.nist.gov/publications/detail/sp/800-39/final [Cit. 2022-11-10].

RADEMACHEROVÁ, Kristina. *Právní rámec vyšetřování počítačové kriminality* [online]. Praha, 2016. Diplomová práce. Karlova univerzita, Právnická fakulta, Katedra trestního práva. Vedoucí práce doc. JUDr. Bc. Tomáš Gřivna, Ph.D. Dostupné: https://dspace.cuni.cz/handle/20.500.11956/81814 [Cit. 2022-10-24].

RADEMACHEROVÁ, Kristina. *Počítačová kriminalita: Vybrané aspekty postihu v mezinárodním prostředí* [online]. Praha, 2017. Rigorózní práce. Karlova univerzita, Právnická fakulta, Katedra trestního práva. Vedoucí práce prof. JUDr. Jiří Jelínek, CSc. Dostupné: https://dspace.cuni.cz/handle/20.500.11956/73331 [Cit. 2022-10-24].

RADEMACHEROVÁ, Kristina. *Principy a východiska kybernetické bezpečnosti de lege lata.* Praha, 2018. Studentská vědecká odborná činnost. Karlova Univerzita, Právnická fakulta, 2018-04-16.

SCHMITT, Michael N. *Tallinn manual on the international law applicable to cyber warfare: prepared by the international group of experts at the invitation of the NATO cooperative cyber defence centre of excellence*. Cambridge: Cambridge University Press, 2013.

SCHMITT, Michael. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* [online]. 2. vydání. Cambridge: Cambridge University Press, 2017. Dostupné: https://www.cambridge.org/core/books/abs/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/law-of-international-responsibility/99E333F8578ADCC567A92BECF932E4C3 [Cit. 2022-11-04].

SLÁDEKOVÁ, Stanislava. Když je v sázce národní bezpečnost. Ohrožení bezpečnosti státu jako důvod pro neudělení pobytového oprávnění cizinci, se zaměřením na krátkodobá víza. In: POŘÍZEK, Pavel, JÍLEK, Dalibor. *Ročenka uprchlického a cizineckého práva 2018: ročenku tvoří příspěvky, které zazněly na vědeckém semináři konaném ve dnech 20. a 21. září 2018 v Kanceláři veřejného ochránce práv - Současné otázky a odpovědi uprchlického a cizineckého práva, a další odborné příspěvky, které souvisí s tématem uprchlického a cizineckého práva* [online]. Brno: Kancelář veřejného ochránce práv ve spolupráci s Wolters Kluwer ČR, 2019.

SMEJKAL, Vladimír. *Internet a §§§*. 1. vyd. Praha: Grada, 2001.

SVOBODA, Petr. *Právo na spravedlivý proces a české správní řízení*. Praha: Univerzita Karlova v Praze. Dizertační práce, 2006.

UN GA. *Special Report of the Disarmament Commission to the General Assembly at its Third Special Session Devoted to Disarmament*, UN Doc A/S-15/3 (28 May 1988) 28-33 (endorsed by UNGA Res 43/78H, 7 December 1988).

VEŘEJNÝ OCHRÁNCE PRÁV. *Souhrnná zpráva o činnosti veřejného ochránce práv za rok 2006*. Brno: Masarykova univerzita, Kancelář veřejného ochránce práv, 1. vydání, 2007.

WIENER, Norbert. *Cybernetics, or Control and Communication in the Animal and Machine.* New York: The Technology Press, 1950.

Články v odborných periodikách:

ABELOVSKÝ, Tomáš. Počítač ako sudca [online]. *Revue pro právo a technologie,* 2016, č. 14. Dostupné: https://journals.muni.cz/revue/article/view/6119 [Cit. 2022-11-03].

AKOTO, Evelyne. Les cyberattaques étatiques constituent - elles des actes d'agression en vertu du droit international public?: Première Partie [online]. *Ottawa Law Review*, Vol. 46, č. 1, 2015. Dostupné: https://ssrn.com/abstract=2685249 [Cit. 2022-11-14].

ALBERSHEIM, Renee. The Legal Implications of Corporate Reverse Hacking. *Preventive Law Reporter*, vol. 18, 1999.

ANDERSON, Ross. Why Information Security is Hard – An Economic Perspective [online]. *Proceedings of the 17th Annual Computer Security Applications Conference*. New Orleans, LA, 2001. Dostupné: https://www.acsac.org/2001/papers/110.pdf [Cit. 2022-11-02].

ARNBAK, Axel, VAN EIJK, N.A.N.M. *Certificate Authority Collapse: Regulating Systemic Vulnerabilities in the HTTPS Value Chain* [online]. TRPC, 15. 8. 2012, str. 2-6. Dostupné: http://dx.doi.org/10.2139/ssrn.2031409 [Cit. 2022-11-05].

BANNELIER, Karine, CHRISTAKIS, Theodore. Cyberattaques - Prévention-Réactions : Rôles des Etats et des acteurs privés [online]. *Les Cahiers de la Revue Défense Nationale*, Paris, 2017. Dostupné: https://ssrn.com/abstract=2957795 [Cit. 2022-11-14].

BARLOW, John Perry. Crime and Puzzlement: in advance of the law on the electronic frontier. *Whole Earth Review.* Sausalito: New Whole Earth, 1990, (68), 44.

BRAUNER, Jan. Dopady technologického vývoje na povinnosti advokáta na úseku kybernetické bezpečnosti. *Bulletin advokacie*, 2022, č. 6.

BRUNER, Tomáš, FAIX, Martin. Problém přičitatelnosti jako nástroj lawfare [online]. *Obrana a strategie*. Brno: University of Defence, 2018, 2018(1). Dostupné: https://www-ceeol-com.ezproxy.is.cuni.cz/search/journal-detail?id=139 [Cit. 2022-11-14].

DELUCA, Christopher D. The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors [online]. *Pace International Law Review Online Companion.* 2013, Vol. 3, Issue 9. Dostupné: https://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1033&context=pilronline [Cit. 2022-10-24].

FÈVRE, Victor. Review of TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS [online]. *Politique Étrangère*, vol. 82, no. 4, 2017. Dostupné: *JSTOR*, https://www.jstor.org/stable/48562377 [Cit. 2022-11-04].

FIALOVÁ, Eva. Právo na přístup k internetu [online]. *Právní prostor*, 1. 7. 2019. Dostupné: https://www.pravniprostor.cz/clanky/pravo-it/pravo-na-pristup-k-internetu [Cit. 2022-10-22].

FREDLAND, John S. Building a Better cybersecurity Act: Empowering the Executive Branch Against Cybersecurity Emergencies. *Military Law Review*, 2010, č. 206.

GRABOSKY, Peter. Virtual criminality: Old wine in new bottles? [online]. *Social and legal studies*. 2001, (10). Dostupné: http://sls.sagepub.com/content/10/2/243.full.pdf [Cit. 2022-10-23].

GRAHAM, Mark. There are No Rights 'in' Cyberspace [online]. *Research Handbook on Human Rights and Digital Technology.* Elgar, January 2019. Dostupné: https://ssrn.com/abstract=3323660 [Cit. 2022-10-23].

GREENBERG, Brad A. Rethinking Technology Neutrality [online]. *Minnesota Law Review*, č. 100, 2016. Dostupné: https://ssrn.com/abstract=2748932 [Cit. 2022-11-01].

GOLDSMITH, Jack L. Against Cyberanarchy. *The University of Chicago Law Review*. Chicago, Ill: University of Chicago Law School, 1998, 65(4).

HANDEYSIDE, Hugh. *T*he Lotus Principle in ICJ Jurisprudence: Was the Ship Ever Afloat? [online]. *Michigan Journal of International Law*. Vol. 29, č. 1 (2007). Dostupné: https://repository.law.umich.edu/mjil/vol29/iss1/3/ [Cit. 2022-11-03].

HARAŠTA, Jakub. Právní aspekty kybernetické bezpečnosti ČR [online]. *Revue pro právo a technologie,* 2013, č. 8. Dostupné: https://journals.muni.cz/revue/article/view/5015 [Cit. 2022-11-22].

HARAŠTA, Jakub, MÍŠEK, Jakub. IP adresy v kybernetické bezpečnosti [online]. *Revue pro právo a technologie*, 2015, č. 12. Dostupné: https://journals.muni.cz/revue/article/view/4091/pdf. [Cit. 2022-10-22].

HART, Herbert Lionel Adolphus. Positivism and the Separation of Law and Morals. *Harvard Law Review*, č. 71, 1958.

HILBERT, Martin., LÓPEZ Priscila. The World's Technological Capacity to Store, Communicate, and Compute Information [online]. *Science* 332, no. 6025 (April 1, 2011). Dostupné: https://www.martinhilbert.net/worldinfocapacity-html/ [Cit. 2022-10-24].

KAMINSKA, Monica, BROEDERS, Dennis, CRISTIANO, Fabio. Limiting Viral Spread: Automated Cyber Operations and the Principles of Distinction and Discrimination in the Grey Zone [online]. *13th International Conference on Cyber Conflict: 'Going Viral'*, 30. 5. 2021. Dostupné: https://ssrn.com/abstract=3856623 [Cit. 2022-11-11].

KASL, František. Internet věcí a ochrana dat v evropském kontextu [online]. *Revue pro právo a technologie*. 2016, č. 13. Dostupné: https://journals.muni.cz/revue/article/view/5422 [Cit. 2022-10-24].

KASL, František. Blockchain, společenská smlouva digitálního věku? [online]. *Revue pro právo a technologie*, 2018, č. 17. Dostupné: https://journals.muni.cz/revue/article/view/8922 [Cit. 2022-11-06].

KLODWIG, Jakub. Varování NÚKIB v systematice zákona o kybernetické bezpečnosti a možnosti jeho zohlednění v zadávacím řízení [online]. *Revue pro právo a technologie,* 2021, č. 23. Dostupné: https://journals.muni.cz/revue/article/view/14590. [Cit. 2022-10-22].

KOOPS, Bert-Jaap. The Internet and its Opportunities for Cybercrime: Tilburg Law School Research Paper No. 09/2011 [online]. *Transnational Criminology Manual*. Nijmegen: WLP, 2010, (1). Dostupné: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1738223 [Cit. 2022-10-24].

LESSIG, Lawrence, RESNICK, Paul. Zoning Speech on the Internet: A Legal and Technical Model [online]. *Michigan law review*. Ann Arbor: University of Michigan Law School, 1999, 98(2). Dostupné: https://cyber.harvard.edu/wg_home/uploads/200/1999-06.pdf [Cit. 2022-11-06].

MESSERSCHMIDT, Jan, E. Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm. *Columbia Journal of Transnational Law,* Vol. 52, No 1, 2013.

MOORE, Gordon E. Cramming more components onto integrated circuits. *Electronics*, 1965 (38/8).

OMER, Tene. What Google Knows: Privacy and Internet Search Engines [online]. *Utah Law Review*, October 1, 2007. Dostupné: https://ssrn.com/abstract=1021490 [Cit. 2022-10-26].

OSBORNE, Martin J. *Selected chapters from draft of An Introduction to Game Theory* [online]. Oxford University Press, 2000. Dostupné: https://mathematicalolympiads.files.wordpress.com/2012/08/martin_j-_osborne-an_introduction_to_game_theory-oxford_university_press_usa2003.pdf [Cit. 2022-11-02].

OSULA, Anna-Maria. Transborder Access and Territorial Sovereignty. *Computer Law and Security Review*. 2015, 31 (6).

PAVELKA, Ivan. Institucionální zajištění ochrany utajovaných informací v ČR. *Správní právo*, č. 3/2018.

PAVLIKOVÁ, Miroslava. Estonsko-ruský incident v kontextu kyberterorismu [online]. *Global Politics: Časopis pro politiku a mezinárodní vztahy,* 2014. Dostupné: http://www.globalpolitics.cz/clanky/estonsko-rusky-incident-v-kontextu-kyberterorismu [Cit. 2017-03-24].

PICOTTI, Lorenzo. Biens juridiques protégés et techniques de formulation des incriminations en droit pénal de l´informatique. *Ramonville Sainte Agne: Révue internationale de droit pénal*, 2006.

POMAHAČ, Richard. *Správní spravedlnost*. Právník, č. 144/5, 2005.

POLČÁK, Radim. Informace a data v právu [online]. *Revue pro právo a technologie,* 2016, č. 13. Dostupné: https://journals.muni.cz/revue/article/view/4946 [Cit. 2022-10-22].

POLČÁK, Radim. Kybernetická bezpečnost jako aktuální fenomén českého práva* [online]. *Revue pro právo a technologie*, 2015, č. 11. Dostupné: https://journals.muni.cz/revue/article/view/2980 [Cit. 2022-09-21].

POTĚŠIL, Lukáš. „Dobrá správa" v dokumentech Rady Evropy [online]. *Veřejná správa,* 2008, č. 12. Dostupné: https://www.mvcr.cz/clanek/verejna-sprava-obsah-cisla-12-2008.aspx [Cit. 2022-10-30].

POWELL, Benjamin. *Is Cybersecurity a Public Good? Evidence from the Financial Services Industry* [online]. The Independent Institute Working Paper Number 57, 15. 3. 2005. Dostupné: http://www.independent.org/pdf/working_papers/57_cyber.pdf [Cit. 2022-11-01].

RADEMACHEROVÁ, Kristina. Je svoboda šířit a přijímat informace ve virtuálním prostředí svobodou virtuální? *Jurisprudence*, 2018, č. 3.

RAMEŠOVÁ, Kristina. Public provocation to commit a terrorist offence: balancing between the liberties and the security [online]. *Masaryk Journal of Law and Technology.* 2020, č. 14/1. Dostupné: https://journals.muni.cz/mujlt/article/view/11626 [Cit. 2022-10-23].

ROSCINI, Marco. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations [online]. *Texas International Law Journal*, 2015, č. 50. Dostupné: https://ssrn.com/abstract=2611753 [Cit. 2022-11-02].

SABHARWAL, Alakshendra, SAIFULLAH, Mohammad, GROVER, Priyanka, BATRA, Neha. Comparative Study of Blockchain Techniques in Electronic Voting System [online]. *Proceedings of the International Conference on Innovative Computing & Communication (ICICC) 202*1, July 11, 2021. Dostupné: https://ssrn.com/abstract=3884390 [Cit. 2022-11-16].

SEITZ, Nicolai. Transborder Search: A New Perspective in Law Enforcement? [online]. *Yale Journal of Law and Technology,* 2005, č. 7(1). Dostupné: http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1016&context=yjolt [Cit. 2022-11-03].

SCHMITZ-BERNDT Sandra, ANHEIER Fabian. Synergies in Cybersecurity Incident Reporting – The NIS Cooperation Group Publication 04/20 in Context [online]. *European Data Protection Law Review,* 2021, Vol. 7 (1). Dostupné: https://edpl.lexxion.eu/data/article/16999/pdf/edpl_2021_01-014.pdf [Cit. 2022-11-05].

SIMON, Matthew, CHOO, Kim-Kwang Raimond. Digital Forensics: Challenges and Future Research Directions [online]. *Contemporary Trends in Asian Criminal Justice: Paving the Way for the Future*. Seoul: South Korea, Korean Institute of Criminology, April 7, 2014. Dostupné: https://ssrn.com/abstract=2421339 [Cit. 2022-10-22].

SUBRENAT, Jean-Jacques. *Estonia: identity and independence*. New York: Rodopi, 2004.

TÁBOROVÁ, Alice. Veřejnoprávní ochrana informační společnosti a místní působnost práva [online]. *Revue pro právo a technologie,* 2010, č. 1. Dostupné: https://journals.muni.cz/revue/article/view/3983 [Cit. 2022-10-24].

TANODOMDEJ Papawadee. The Tallinn Manuals and the Making of the International Law on Cyber Operations. [online] *Masaryk Journal of Law and Technology,* 2019, č. 13(1). Dostupné: https://journals.muni.cz/mujlt/issue/view/992 [Cit. 2022-11-04].

VOSTOUPAL, Jakub. Certifikace kyberbezpečnostních technologií [online]. *Revue pro právo a technologie*, 2019, č. 20. Dostupné: https://journals.muni.cz/revue/article/view/12570. [Cit. 2022-10-22].

ZARSKY, Tal. Transparent Predictions [online]. *University of Illinois Law Review*. Sv. 2013, č. 4. Dostupné: https://ssrn.com/abstract=2324240 [Cit. 2022-10-25].

2. Seznam použitých internetových zdrojů

ACRESIA. *Implementace ZKB* [online]. Dostupné: https://www.acresia.com/index.php/sluzby/68-implementace-zakona-o-kyberneticke-bezpecnosti [2022-11-21].

BARLOW, John Perry. The economy of ideas: a framework for rethinking patents and copyrights in the digital age (Everything you know about intellectual property is wrong). *Wired*, 1994, 2(3).

BARLOW, John, Perry. *A Declaration of the Independence of Cyberspace* [online]. Electronic Frontier Foundation, 8. 2. 1996. Dostupné: https://www.eff.org/cyberspace-independence [Cit. 2022-11-03].

BRADSHER, Keith. *China Blocks WhatsApp, Broadening Online Censorship* [online]. The New York Times, 25. 9. 2017. Dostupné: https://www.nytimes.com/2017/09/25/business/china-whatsapp-blocked.html [Cit. 2022-11-06].

BRESSAN, Stephane, LEE, Thomas. *Information Brokering On The World Wide Web* [online]. Cambridge, MA: The Sloan School of Management Massachusetts Institute of Technology, 1997. Dostupné: http://dspace.mit.edu/bitstream/handle/1721.1/2663/SWP-3963-37617980-CISL-9708.pdf;sequence=1 [Cit. 2022-10-24].

CCDOE. *The Tallinn Manual* [online]. Dostupné: https://ccdcoe.org/research/tallinn-manual/ [Cit. 2022-11-04].

CENTRUM KYBERNETICKÉ BEZPEČNOSTI. *Úřad pro kybernetickou bezpečnost varoval před výrobky firem Huawei a ZTE* [online]. 18. 12. 2022. Dostupné: https://centrumkyberbezpecnosti.cz/urad-pro-kybernetickou-bezpecnost-varoval-pred-vyrobky-firem-huawei-a-zte/ [Cit. 2022-11-22].

C. H. BECK. Certifikace kybernetické bezpečnosti. *Právní zpravodaj*, 8. 2. 2022. Dostupné: beck-online.cz [Cit. 2022-11-08].

COUNCIL OF EUROPE. *Recommendation CM/Rec(2007)7 of the Committee of Ministers to member states on good administration* [online]. Dostupné: https://rm.coe.int/0900001680707096b9 [Cit. 2022-10-30].

COUNCIL OF EUROPE. *Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet* [online]. Dostupné: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2f8 [Cit. 2022-11-18].

COUNCIL OF EUROPE. *Declaration of the Committee of Ministers on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers* [online]. Dostupné: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805cb844 [Cit. 2022-11-18].

COUNCIL OF EUROPE. *12 Principles of Good Governance and European Label of Governance Excellence* [online]. Dostupné: https://www.coe.int/en/web/good-governance/12-principles [Cit. 2022-10-30].

CPJ. *10 Most Censored Countries* [online]. Commitee to Protect Journalists. Dostupné: https://cpj.org/2015/04/10-most-censored-countries/ Aktualizované údaje k roku 2019 dostupné: https://cpj.org/reports/2019/09/10-most-censored-eritrea-north-korea-turkmenistan-journalist/ [Cit. 2022-10-27].

CSIRT.CZ. *Zpráva o činnosti CSIRT.CZ (Národního CSIRT ČR) za rok 2020* [online], str. 10. Dostupné: https://www.csirt.cz/media/filer_public/c1/64/c1642df8-32f0-4976-9062-ac259f7a43b4/210304_csirt_vyrocni_zprava_2020.pdf [Cit. 2022-11-03].

CYBERSECURITY. *Braňte se kybernetickým hrozbám. Systematicky a účinně: komplexní řešení kybernetické bezpečnosti pro vaši společnost* [online]. Dostupné: https://www.cybersecuritycompliance.cz/?gclid=CjwKCAjwyaWZBhBGEiwACslQo82pLjca7QhC7WRlN9J8pHsmvNgBJayp-GsY8hs2dTyUdWPcPBHiTRoCNR0QAvD_BwE [Cit. 2022-11-21].

CZ.NIC. *O sdružení* [online]. Dostupné: https://www.nic.cz/page/351/ [Cit. 2022-11-22].

ČERNÝ, Michal. *Hodnocení informací* [online]. Metodický portál RVP.CZ., 21.12.2020. Dostupné: https://clanky.rvp.cz/clanek/c/G/22721/hodnoceni-informaci.html [Cit. 2022-10-27].

DANCHEV, Dancho. *Study finds the average price for renting a botnet* [online]. ZDNet, 26. 5. 2010. Dostupné: http://www.zdnet.com/article/study-finds-the-average-price-for-renting-a-botnet/ [Cit. 2022-11-11].

DELL TECHNOLOGIES. *Global Data Protection Index 2021: Key Findings - July 2021* [online]. Dostupné: https://www.delltechnologies.com/en-us/data-protection/gdpi/index.htm#pdf-overlay=//www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/global-data-protection-index-key-findings.pdf [Cit. 2021-11-12].

DELOITTE. *Soulad se zákonem o kybernetické bezpečnosti* [online]. Dostupné: https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/technology/cz_soulad_se_zakonem_o_kyberneticke_bezpecnosti.pdf [Cit. 2022-11-21].

DIMUN, Petr. *O blokování „dezinformačních" webů vláda nerozhodla, chybí zákonná úprava* [online]. Česká justice, 3. března 2022. Dostupné: https://www.ceska-justice.cz/2022/03/o-blokovani-dezinformacnich-webu-vlada-nerozhodla-chybi-zakonna-uprava/ [Cit. 2022-11-08].

DVOŘÁKOVÁ, Renata, IGNÁCIKOVÁ, Jaroslava. Co lze čekat od zákona o kybernetické bezpečnosti [online]. *IT Systems,* 2014. Dostupné: https://www.systemonline.cz/clanky/co-lze-cekat-od-zakona-o-kyberneticke-bezpecnosti-1.htm [Cit. 2022-11-02].

ENISA. *Definition of Cybersecurity: Gaps and overlaps in standardisation* [online], 2016. Dostupné: https://www.enisa.europa.eu/publications/definition-of-cybersecurity [Cit. 2022-11-07].

ENISA. *Reference Incident Classification Taxonomy: Task Force Status and Way Forward* [online]. January 2018, str. 9. Dostupné: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy [Cit. 2022-11-10].

EUR-LEX. *Akt EU o kybernetické bezpečnosti: Shrnutí dokumentů* [online]. Dostupné https://eur-lex.europa.eu/legal-content/CS/LSU/?qid=1652275836404&uri=CELEX%3A32019R0881 [Cit. 2022-11-08].

EVROPSKÁ KOMISE. European governance - A white paper /* COM/2001/0428 final */. Official Journal 287, 12/10/2001 P. 0001 - 0029. Dostupné: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52001DC0428&qid=1488203863476 [Cit. 2022-10-30].

EVROPSKÝ VEŘEJNÝ OCHRÁNCE PRÁV. *Zásady veřejné služby pro úředníky EU* [online]. Evropská unie, 2012. Dostupné: https://www.ombudsman.europa.eu [Cit. 2022-10-30].

FIŠER, Miloslav. *Kybernetická válka: Anonymous napadli 2500 ruských a běloruských cílů* [online]. novinky.cz, 4. 3. 2022. Dostupné: https://www.novinky.cz/valka-na-ukrajine/clanek/kyberneticka-valka-anonymous-napadli-2500-ruskych-a-beloruskych-cilu-40389280 [Cit. 2022-11-11].

HALCIN, Jakub. *Příběh počítače: 1. díl* [online]. Galaxie, 24. 6. 2005. Dostupné: http://www.galaxie.name/index.php?clanek=pribeh-pocitace-1-dil [Cit. 2022-10-27].

HILBERT, Martin. *The World's Technological Capacity to Store, Communicate, and Compute Information* [online]. Dostupné: https://www.martinhilbert.net/worldinfocapacity-html/ [2021-11-30].

ICT REVUE. Závislost na ICT pronikla do všech oborů. Zrychlují práci, ale potírají myšlení a paměť [online]. *Hospodářské noviny,* 25. 2. 2019. Dostupné: https://ictrevue.hn.cz/c3-66493870-0ICT00_d-66493870-zavislost-na-ict-pronikla-do-vsech-oboru-zrychluji-praci-ale-potiraji-mysleni-a-pamet [Cit. 2022-10-22].

IDNES. *Čekejte kyberútok, vzkázali Anonymous Putinovi* [online]. 27. 2. 2022. Dostupné: https://tv.idnes.cz/zahranicni/rusko-ukrajina-anonymous-kyberutok-hrozba-putin-vladimir.V220227_104405_idnestv_vojt [Cit. 2022-11-11].

INTERNATIONAL TELECOMMUNICATION UNION. Internet usage keeps growing, but barriers lie ahead. [online]. *Facts and figures 2019: Measuring digital development*. Dostupné: https://itu.foleon.com/itu/measuring-digital-development/internet-use/ [Cit. 2022-10-24].

KASPERSKY. Stuxnet: Victims Zero [online]. *Kaspersky Daily*, 18. 11. 2014. Dostupné: https://www.kaspersky.com/blog/stuxnet-victims-zero/6775/ [Cit. 2022-11-11].

KEJLOVÁ, Tamara, SVITÁK, Matěj. *Írán může potkat osud Sovětského svazu. Nemáme co ztratit, hlásá generace Z a riskuje své životy* [online]. ČT24, 26. 10. 2022. Dostupné: https://ct24.ceskatelevize.cz/svet/3538284-iran-muze-potkat-osud-sovetskeho-svazu-nemame-co-ztratit-hlasa-generace-z-a-riskuje-sve [2022-10-27].

KOMISE EU. *2021 annual report on the application of the Charter of fundamental rights* [online]. Dostupné: https://ec.europa.eu/info/files/2021-annual-report-application-charter-fundamental-rights_en [Cit. 2022-11-08].

LEWIS, James Andrew. *Confidence-building and international agreement in cybersecurity* [online]. Disarmament forum. Dostupné: https://citizenlab.ca/cybernorms2012/Lewis2011.pdf [Cit. 2022-11-12].

LIN, Patrick. *Ethics of Hacking Back: Six Arguments from Armed Conflict to Zombies* [online]. 26. 9. 2016. Dostupné: http://ethics.calpoly.edu/hackingback.pdf [Cit. 2022-11-16].

MAGDOŇOVÁ, Jana, ANDRLE, Vít. *Hackeři zaútočili na běloruské železnice. Výrazně zpomalili přesun ruské vojenské techniky k Ukrajině* [online]. irozhlas.cz, 6. 3. 2022. Dostupné: https://www.irozhlas.cz/zpravy-svet/hackeri-kyberneticky-partizan-ukrajina-belorusko-vlaky_2203061205_ban [Cit. 2022-11-11].

MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČR. *Bezpečnostní strategie České republiky 2015* [online]. Praha, 2015, str. 23. Dostupné: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf [Cit. 2022-11-06].

MMR. *Jak využít chytrá řešení ve vašem městě?* [online]. Dostupné: https://mmr.cz/cs/microsites/sc/smart-cities [Cit. 2022-11-08].

MO. *Národní centrum kybernetických operací vypracovalo strategii kybernetické obrany ČR* [online], 6. 8. 2018. Dostupné: https://mocr.army.cz/informacni-servis/zpravodajstvi/narodni-centrum-kybernetickych-operaci-vypracovalo-strategii-kyberneticke-obrany-cr-201906/ [Cit. 2022-11-09].

NATO. *Cyber defence* [online]. 2018. Dostupné: https://www.nato.int/cps/en/natohq/topics_78170.htm [Cit. 2022-10-23].

NATO. *NATO Summit Guide, Warsaw 2016* [online]. Dostupné: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160715_1607-warsaw-summit-guide_2016_eng.pdf [Cit. 2022-10-23].

NBÚ. *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 - 2020* [online], str. 5. Dostupné: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/ [2022-11-07].

(NESIG.) *Memorandum o Computer Security Incident Response Team České republiky ze dne 9. prosince 2010, uzavřené mezi Ministerstvem vnitra ČR a sdružením CZ.NIC, z.s.p.o.* [online]. Dostupné: https://www.nic.cz/files/nic/doc/Memorandum_CSIRT.CZ.pdf [Cit. 2022-11-22].

(NESIG.) *Veřejnoprávní smlouva z 18. 12. 2015, jejíž přílohou je žádost CZ.NIC o uzavření veřejnoprávní smlouvy za účelem spolupráce v oblasti kybernetické bezpečnosti a zajištění provozu národního bezpečnostního týmu* [online]. Dostupné: https://csirt.cz/media/filer_public/d5/ab/d5aba5fa-f20d-4fa9-b725-899eb81cde80/nbu-smlouva-narodni-cert-201512.pdf [Cit. 2022-11-22].

(NESIG.) *Česká terminologická databáze knihovnictví a informační vědy* [online]. Dostupné: http://aleph22.nkp.cz/F/?func=file&file_name=find-b&local_base=ktd [Cit. 2022-10-23].

(NESIG.) *Wikipédia : slobodná encyklopédia* [online]. St. Petersburg (Florida) : Wikimedia Foundation, 2001- . Slovenská verze. Dostupné: https://sk.wikipedia.org/wiki/Exabajt [Cit. 2022-10-24].

NIS COOPERATION GROUP. *Annual Report NIS Directive Incidents 2019* [online]. CG Publication 03/20, December 2020. Dostupné: https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group [Cit. 2022-01-22].

NÚKIB. *Varování před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation* [online]. 17. 12. 2018. Dostupné: https://www.nukib.cz/cs/uredni-deska/ [Cit. 2022-11-21].

NÚKIB. *Metodika k varování ze dne 17. prosince 2018* [online]. Dostupné: https://www.govcert.cz/download/kii-vis/2019_01_04_metodika_k_varov%C3%A1n%C3%AD_z_17-12-2018_v1.0.pdf [Cit. 2022-11-22].

NÚKIB. *Koncepce rozvoje Národního úřadu pro kybernetickou a informační bezpečnost* [online]. 2020. Dostupné: https://www.nukib.cz/download/publikace/strategie_akcni_plany/Koncepce_rozvoje_NUKIB.pdf [Cit. 2022-11-21].

NÚKIB. *Varování před hrozbou kybernetických útoků na nemocnice a jiné významné cíle ČR* [online]. 16. 4. 2020. Dostupné: https://www.nukib.cz/cs/uredni-deska/ [Cit. 2022-11-22].

NÚKIB. *Bezpečná práce na dálku - doporučení pro firmy i zaměstnance* [online]. 20. 5. 2020. Dostupné: https://www.nukib.cz/cs/infoservis/doporuceni/ [Cit. 2022-10-05].

NÚKIB. *Ukončení účinnosti varování ze dne 16. dubna 2020* [online]. 20. 5. 2020. Dostupné: https://www.nukib.cz/cs/uredni-deska/ [Cit. 2022-11-22].

NÚKIB. *Zadávání veřejných zakázek v oblasti ICT a kybernetická bezpečnost v 1.3* [online]. 31. 7. 2020. Dostupné: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/ [Cit. 2022-11-21].

NÚKIB. *Reaktivní opatření formou opatření obecné povahy* [online]. 16. 12. 2020. Dostupné: https://www.nukib.cz/cs/uredni-deska/ [Cit. 2022-11-22].

NÚKIB. *Reaktivní opatření formou opatření obecné povahy* [online]. 12. 03. 2021. Dostupné: https://www.nukib.cz/cs/uredni-deska/ [Cit. 2022-11-22].

NÚKIB. *Ochranné opatření formou opatření obecné povahy - Zabezpečení e-mailů* [online]. 11. 10. 2021. Dostupné: https://www.nukib.cz/cs/uredni-deska/ [Cit. 2022-11-22].

NÚKIB. *Reaktivní opatření formou opatření obecné povahy - Log4Shell* [online]. 15. 12. 2021. Dostupné: https://www.nukib.cz/cs/uredni-deska/ [Cit. 2022-11-22].

NÚKIB. *Národní strategie kybernetické bezpečnosti České republiky na období let 2021 - 2025* [online]. Dostupné: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/ [Cit. 2022-03-05].

NÚKIB. *Akční plán k Národní strategii kybernetické bezpečnosti ČR na období let 2021 až 2025* [online]. Dostupné: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/ [Cit. 2022-11-08].

NÚKIB. *Zohlednění varování ze dne 17. 12. 2018 v zadávacím řízení* [online]. 14. 1. 2022. Dostupné: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/ [Cit. 2022-11-21].

NÚKIB. *Varování před hrozbou kybernetických útoků na strategické organizace v České republice* [online]. 25. 2. 2022. Dostupné: https://www.nukib.cz/cs/uredni-deska/ [Cit. 2022-11-22].

NÚKIB. *Varování v souvislosti s ekonomickými sankcemi spojenými s Ruskou federací* [online]. 21. 3. 2022. Dostupné: https://www.nukib.cz/cs/uredni-deska/ [Cit. 2022-11-22].

NÚKIB. *NÚKIB v rámci preventivních kroků vydal v souvislosti s ozbrojeným konfliktem mezi Ruskou federací a Ukrajinou Varování* [online]. Dostupné: https://www.nukib.cz/cs/uredni-deska/ [Cit. 2022-11-06].

NÚKIB. *Varování před použitím chytrých elektroměrů ze zemí s nedůvěryhodným právním prostředím* [online]. 30. 5. 2022. Dostupné: https://www.nukib.cz/cs/uredni-deska/ [Cit. 2022-11-22].

NÚKIB. *Kybernetické incidenty pohledem NÚKIB: červen 2022* [online]. Dostupné: https://www.nukib.cz/download/publikace/vyzkum/NUKIB_incidenty-2022-06.pdf [Cit. 2022-11-10].

NÚKIB. *Doporučení k používání protokolu TLP ke sdílení chráněných informací* [online]. 10. 8. 2022. Dostupné: https://www.nukib.cz/cs/infoservis/doporuceni/ [Cit. 2022-10-05].

NÚKIB. *Vzorové hodnocení rizik pro veřejnou zakázku* [online]. 22. 8. 2022. Dostupné: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/ [Cit. 2022-11-21].

NÚKIB. *NÚKIB představuje evropskou směrnici NIS2* [online]. 7. 9. 2022. Dostupné: https://www.nukib.cz/cs/infoservis/aktuality/1874-nukib-predstavuje-evropskou-smernici-nis2/ [Cit. 2022-10-15].

NÚKIB. *Kybernetické incidenty pohledem NÚKIB: říjen 2022* [online]. Dostupné: https://www.nukib.cz/download/publikace/vyzkum/2022-10.pdf [Cit. 2022-11-10].

NÚKIB. *V Praze proběhla prestižní Prague Cyber Security Conference* [online]. 4. 11. 2022. Dostupné: https://nukib.cz/cs/infoservis/aktuality/1903-v-praze-probehla-prestizni-prague-cyber-security-conference/ [Cit. 2022-11-08].

NÚKIB. *Národní výzkum a vývoj* [online]. Dostupné: https://nukib.cz/cs/kyberneticka-bezpecnost/vyzkum/narodni-vyzkum-a-vyvoj/ [Cit. 2022-10-17].

NÚKIB. *Kybernetická cvičení* [online]. Dostupné: https://www.nukib.cz/cs/kyberneticka-bezpecnost/cviceni/kyberneticka-cviceni/ [Cit. 2022-11-08].

NÚKIB. *DoS / DDoS útoky: Doporučení pro případ napadení DDoS útokem - jak se zachovat a jak postupovat* [online]. Dostupné: https://nukib.cz/download/publikace/doporuceni/Doporuceni_DDoS.pdf [Cit. 2022-11-11].

NÚKIB. *Organizační struktura* [online]. Dostupné: https://www.nukib.cz/cs/o-nukib/organizacni-struktura-uradu/ [Cit. 2022-11-22].

OECD. *European Principles for Public Administration* [online]. SIGMA Papers, No. 27. Paris: OECD Publishing, 1999. Dostupné: https://doi.org/10.1787/5kml60zwdr7h-en [Cit. 2022-10-30].

PAČKA, Roman. *Role CERT/CSIRT v národní bezpečnosti* [online]. Masarykova univerzita: Prezentace k předmětu Kybernetická bezpečnost. Dostupné: https://is.muni.cz/el/fss/podzim2018/BSS469/um/bss_23.10.2018.pdf [Cit. 2022-11-22].

PENDER-BEY, Georgie. *The Parkerian Hexad: The CIA Triad Model Expanded* [online]. Dostupné: http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf [Cit. 2022-11-10].

PSPČR. *Stálá komise pro hybridní hrozby: O komisi* [online]. Dostupné: https://www.psp.cz/sqw/hp.sqw?k=8309&o=8 [Cit. 2022-11-22].

PSPČR. *Stálá komise pro kontrolu činnosti Národního úřadu pro kybernetickou a informační bezpečnost* [online]. Dostupné: https://www.psp.cz/sqw/hp.sqw?k=7801 [Cit. 2022-11-22].

RADA EU. *Výběr sídla Evropského centra kompetencí pro kybernetickou bezpečnost* [online]. Dostupné: https://www.consilium.europa.eu/cs/policies/cybersecurity/seat-selection-cybersecurity-centre/ [Cit. 2022-10-16].

RADA EVROPY. *Explanatory Report - ETS 185 - Cybercrime (Convention)* [online]. Dostupné: https://rm.coe.int/16800cce5b [Cit. 2022-11-09].

RICE, Denis. *Google wins out in challenge to its website rating system* [online]. Lexology.com, 12. 10. 2016. Dostupné: http://www.internationallawoffice.com/Newsletters/E-commerce/USA/Howard-Rice-Nemerovski-Canady-Falk-Rabkin/Google-Wins-Out-in-Challenge-to-its-Website-Rating-System [Cit. 2022-10-26].

ROPERT, Samuel. Internet of things: Outlook for the top 8 vertical markets [online]. *IDATE DigiWorld*, 7 April 2016. Dostupné: https://en.idate.org/internet-of-things-2/ [Cit. 2022-10-25].

SEDLÁK, Jan. *Piráti chtějí v reakci na Huawei a ZTE ve státní správě nasazovat otevřený hardware* [online]. Lupa.cz, 10. 1. 2019. Dostupné: https://www.lupa.cz/aktuality/pirati-chteji-v-reakci-na-huawei-a-zte-ve-statni-sprave-nasazovat-otevreny-hardware/ [Cit. 2022-11-22].

SEDLÁK, Jan. *Vláda jmenovala inspektora kybernetické obrany, bude hlídat Vojenské zpravodajství* [online]. Lupa.cz, 7. 4. 2022. Dostupné: https://www.lupa.cz/aktuality/vlada-jmenovala-inspektora-kyberneticke-obrany-bude-hlidat-vojenske-zpravodajstvi/ [Cit. 2022-11-09].

SEDLÁK, Jan. *Huaewei v Česku kvůli sankcím a varování spadly tržby skoro o tři miliardy* [online]. Lupa.cz, 9.9.2022. Dostupné: https://www.lupa.cz/aktuality/huawei-v-cesku-kvuli-sankcim-a-varovani-spadly-trzby-skoro-o-tri-miliardy/?opinionsListing-extraParameters%5BadditionalAdvertPositions%5D%5B0%5D=rectangle-top&opinionsListing-extraParameters%5BadditionalAdvertPositions%5D%5B1%5D=opinions-list-behind-3rd-item&opinionsListing-order=insert&do=opinionsListing-reorder [Cit. 2022-11-22].

STÁLÁ KOMISE PSPČR PRO KONTROLU ČINNOSTI NÚKIB. *Usnesení č. 6* [online]. 25. 4. 2019. Digitální depozitář. Dostupné: https://www.psp.cz/sqw/text/text2.sqw?idd=157640 [Cit. 2022-11-22].

STÁLÁ KOMISE PSPČR PRO KONTROLU ČINNOSTI NÚKIB. *Usnesení č. 7* [online]. 6. 6. 2019. Digitální depozitář. Dostupné: https://www.psp.cz/sqw/text/text2.sqw?idd=158439 [Cit. 2022-11-22].

STÁLÁ KOMISE PSPČR PRO KONTROLU ČINNOSTI NÚKIB. *Usnesení č. 9* [online]. 12. 7. 2019. Digitální depozitář. Dostupné: https://www.psp.cz/sqw/text/text2.sqw?idd=159355 [Cit. 2022-11-22].

STÁLÁ KOMISE PSPČR PRO KONTROLU ČINNOSTI NÚKIB. *Usnesení č. 10 a č. 11* [online]. 12. 7. 2019. Digitální depozitář. Dostupné: https://www.psp.cz/sqw/hp.sqw?k=7805&o=8&kk=5 [Cit. 2022-11-22].

STÁLÁ KOMISE PSPČR PRO KONTROLU ČINNOSTI NÚKIB. *Usnesení č. 23* [online]. 17. 3. 2021. Digitální depozitář. Dostupné: https://www.psp.cz/sqw/text/text2.sqw?idd=188678 [Cit. 2022-11-22].

STÁLÁ KOMISE PSPČR PRO KONTROLU ČINNOSTI NÚKIB. *Usnesení č. 4, Ke koncepci rozvoje NÚKIB* [online]. 31. 3. 2022. Digitální depozitář. Dostupné: https://www.psp.cz/sqw/hp.sqw?k=7802 [Cit. 2022-11-22].

STÁLÁ KOMISE PSPČR PRO KONTROLU ČINNOSTI NÚKIB. *Usnesení č. 1 až 6* [online]. 21.1.2022, 31.3.2022, 14.7.2022. Digitální depozitář. Dostupné: https://www.psp.cz/sqw/hp.sqw?k=7805&kk=5 [Cit. 2022-11-22].

SVOBODA, Jan. *Vybrané právní aspekty migrace dat: Jak předejít vendor lock-inu* [online]. SystemOnLine.cz. Dostupné: https://www.systemonline.cz/it-pravo/vybrane-pravni-aspekty-migrace-dat.htm?mobilelayout=false [Cit. 2022-11-22].

SCHNEIER, Bruce. *The Internet of Things Will Turn Large - Scale Hacks into a Real World Disasters* [online]. Vice, 25. 7. 2016. Dostupné: https://www.vice.com/en/article/qkjzwp/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster [Cit. 2022-11-10].

ŠMÍD, Jaroslav. Implementace ZKB [online]. *Egovernment*. Praha: info*com, 2015, č. 2. Dostupné: https://www.egovernment.cz/soubor/2015-2/ [Cit. 2022-11-20].

THE WHITE HOUSE. *Notice on the Continuation Of The National Emergency With Respect To Specified Harmful Foreign Activities Of The Government Of The Russian Federation* [online]. April 13, 2022, Statements and Releases. Dostupné: https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/13/notice-on-the-continuation-of-the-national-emergency-with-respect-to-specified-harmful-foreign-activities-of-the-government-of-the-russian-federation/ [Cit. 2022-11-12].

TF-CSIRT: Trusted Introducer. *Services for Security and Incident Response Teams* [online]. Dostupné: https://www.trusted-introducer.org/services/overview/czech.html [Cit. 2022-11-03].

TOR. *Hidden Service Protocol* [online]. Dostupné: https://support.torproject.org [Cit. 2022-10-24].

UNODC. *Comprehensive Study on Cybercrime* [online]. United Nations Office on Drugs and Crime, Draft - February 2013, str. 26. Dostupné: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [Cit. 2022-10-24].

UN OFFICE FOR DISARMAMENT AFFAIRS. *Developments in the field of information and telecommunications in the context of international security* [online]. Dostupné: https://www.un.org/disarmament/ict-security/ [Cit. 2022-11-12].

UN OFFICE FOR DISARMAMENT AFFAIRS. *Fact Sheet: Developments in the Field of Information and Telecommunications in the Context of International Security* [online]. July 2019. Dostupné: https://front.un-arm.org/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf [Cit. 2022-11-12].

VÁCLAVÍK, Lukáš. Před 25 lety se Československo připojilo k Internetu. Připoměňme si hlavní milníky [online]. *cnews.cz,* 13. 2. 2017. Dostupné: https://www.cnews.cz/pred-25-lety-se-ceskoslovensko-pripojilo-k-internetu-pripomente-si-hlavni-milniky/ [Cit. 2022-10-23].

VLÁDA. *Jednání vlády - archiv* [online]. Aplikace ODok. Dostupné: https://apps.odok.cz/djv-agenda-list?year=2022 [Cit. 2022-11-09].

VLÁDA. *Vláda pozastavuje ratifikaci dohody ACTA* [online]. Vláda ČR, 6. 2. 2012. Dostupné: https://www.vlada.cz/cz/media-centrum/aktualne/vlada-pozastavuje-ratifikaci-dohody-acta-92694/ [Cit. 2022-11-11].

VLÁDA. *Usnesení č. 15 ze dne 12. 4. 2022* [online]. Dostupné: https://www.vlada.cz/cz/ppov/brs/cinnost/zaznamy-z-jednani/zaznam-ze-schuze-brs-konane-dne-12--dubna-2022-195782/ [Cit. 2022-11-22].

VOŘÍŠEK, Lukáš. *Obyčejné smazání nestačí, data dokáže obnovit kdokoli: Jak bezpečně smazat soubory a zničit pevný disk?* [online]. inSmart.cz, 7. 6. 2019. Dostupné: https://insmart.cz/jak-trvale-smazat-data/ [Cit. 2022-11-12].

VZ. *Novela zákona o vojenském zpravodajství* [online]. Dostupné: https://www.vzcr.cz/novela-zakona-o-vojenskem-zpravodajstvi-151 [Cit. 2022-11-09].

WOODS, Eoin. *Secure by Design - the Architect's Guide to Security Design Principles* [online]. GOTO 2016. Dostupné: https://www.youtube.com/watch?v=4qN3JBGd1g8 [Cit. 2022-11-08].

YOUNG, Xu. *Deconstructing the Great Firewall of China* [online]. ThousandEyes Blog, 8. 3. 2016. Dostupné: https://www.thousandeyes.com/blog/deconstructing-great-firewall-china [Cit. 2022-11-06].

3. Seznam použitých právních předpisů

Unijní předpisy:

(všechny právní předpisy EU dostupné: https://eur-lex.europa.eu [Cit. 2022-10-29])

Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu).

Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích).

Směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu (Text s významem pro EHP).

Směrnice Evropského parlamentu a Rady 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii.

Listina základních práv Evropské unie, 2012/C 326/02, Dokument 12016P/TXT.

Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

Prováděcí nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148, pokud jde o bližší upřesnění prvků, které musí poskytovatelé digitálních služeb zohledňovat při řízení bezpečnostních rizik, jimiž jsou vystaveny sítě a informační systémy, a parametrů pro posuzování toho, zda je dopad incidentu významný.

Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA (Agentuře Evropské unie pro kybernetickou bezpečnost) a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií (akt o kybernetické bezpečnosti).

Smlouva o fungování Evropské unie (konsolidované znění), C 202/1, Dokument 12016E/TXT, 1. 3. 2020.

Smlouva o Evropské unii (konsolidované znění), C 202/1, Dokument 12016M/TXT, 1.3.2020.

Nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center.

Vnitrostátní zákony:

Vyhláška[1087] ministra zahraničních věcí č. 30/1947 Sb., ze dne 16. ledna 1947 o chartě Spojených národů a statutu Mezinárodního soudního dvora, sjednaných dne 26. června 1945 na konferenci Spojených národů o mezinárodní organisaci, konané v San Francisku.

Zákon České národní rady č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění pozdějších předpisů.

Vyhláška[1088] ministra zahraničních věcí ze dne 4. září 1987 č. 15/1988 Sb., o Vídeňské úmluvě o smluvním právu.

Usnesení předsednictva České národní rady č. 2 ze dne 28. prosince 1992 o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky.

[1087] Příloha této vyhlášky uveřejňuje český překlad charty a statutu a jde o součást Sbírky zákonů ČR.

[1088] Příloha této vyhlášky uveřejňuje český překlad úmluvy a jde o součást Sbírky zákonů ČR.

Zákon č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů.

Zákon č. 90/1995 Sb., o jednacím řádu Poslanecké sněmovny, ve znění pozdějších předpisů.

Zákon č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

Zákon č. 82/1998 Sb., o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem a o změně zákona České národní rady č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád), ve znění pozdějších předpisů.

Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění pozdějších předpisů.

Zákon č. 123/1998 Sb., o právu na informace o životním prostředí, ve znění pozdějších předpisů.

Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, ve znění pozdějších předpisů.

Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

Zákon č. 222/1999 Sb., o zajišťování obrany České republiky, ve znění pozdějších předpisů.

Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů, ve znění pozdějších předpisů.

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů.

Zákon č. 449/2001Sb., o myslivosti, ve znění pozdějších předpisů.

Zákon č. 150/2002 Sb., soudní řád správní, ve znění pozdějších předpisů.

Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů, ve znění pozdějších předpisů.

Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů.

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů.

Zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů.

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

Zákon č. 255/2012 Sb., o kontrole (kontrolní řád), ve znění pozdějších předpisů.

Sdělení č. 75/2013 Sb. m. s., Ministerstva zahraničních věcí o sjednání Úmluvy Organizace spojených národů ze dne 15. listopadu 2000 proti nadnárodnímu organizovanému zločinu.

Sdělení č. 104/2013 Sb. m. s., Ministerstva zahraničních věcí o sjednání Úmluvy Rady Evropy ze dne 23. listopadu 2001 o počítačové kriminalitě.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů.

Zákon č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů.

Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů.

Zákon č. 104/2017 Sb., kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a některé další zákony.

Zákon č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony.

Zákon č. 35/2018 Sb., o změně některých zákonů upravujících počet členů zvláštních kontrolních orgánů Poslanecké sněmovny.

Zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů.

Zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů.

Zákon č. 150/2021 Sb., kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, a některé další zákony.

Zákon č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci.

Zákon č. 226/2022 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.

Vnitrostátní podzákonné předpisy:

Vyhláška ministra zahraničních věcí č. 120/1976 Sb., o Mezinárodním paktu o občanských a politických právech a Mezinárodním paktu o hospodářských, sociálních a kulturních právech.

Vyhláška Národního bezpečnostního úřadu č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor.

Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

Vyhláška NBÚ a Ministerstva vnitra č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.

Nařízení vlády č. 341/2017, o platových poměrech zaměstnanců ve veřejných službách a správě, ve znění pozdějších předpisů.

Vyhláška NÚKIB č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby.

Vyhláška NÚKIB č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

Vyhláška NÚKIB č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci.

Vyhláška NÚKIB č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu.

Ostatní předpisy:

Metodika k certifikaci informačních systémů č. 1/2005/02/is Nbu ve znění účinném od 30. 4. 2005.

4. Seznam použité judikatury

Vnitrostátní:

Nález Ústavního soudu ze dne 3. 4. 1996, sp. zn. Pl. ÚS 32/95, odlišné stanovisko Pavla Höllandera.

Rozsudek Nejvyššího soudu ze dne 16. 1. 2001, sp. zn. 4 Tz 265/2000.

Nález Ústavního soudu ze dne 22. 1. 2001, sp. zn. II. ÚS 502/2000.

Nález Ústavního soudu ze dne 16. 10. 2001, Pl. ÚS 5/01.

Nález Ústavního soudu ze dne 13. 8. 2002, sp. zn. Pl. ÚS 3/02.

Rozsudek Nejvyššího správního soudu ze dne 27. 11. 2003, č. j. 4 Azs 27/2003-55.

Rozsudek Nejvyššího správního soudu ze dne 22. 1. 2004, č. j. 5 Azs 47/2003-48.

Rozsudek Nejvyššího správního soudu ze dne 26. 8. 2004, č. j. 5 Azs 170/2004-72.

Rozsudek Nejvyššího správního soudu ze dne 11. 11. 2004, č. j. 2 As 36/2004-46.

Rozsudek Nejvyššího správního soudu ze dne 22. 12. 2004, č. j. 4 As 31/2003-111.

Usnesení Nejvyššího správního soudu ze dne 23. 3. 2005, č.j. 6 A 25/2002-42.

Nález Ústavního soudu ze dne 28. 6. 2005, sp. zn. Pl. ÚS 24/04.

Nález Ústavního soudu ze dne 13. 6. 2006, sp. zn. I. ÚS 50/03.

Nález Ústavního soudu ze dne 17. 7. 2007, sp. zn. IV. ÚS 23/05.

Rozsudek Nejvyššího správního soudu ze dne 29. 2. 2008, č. j. 8 Afs 152/2006-144.

Nález Ústavního soudu ze dne 2. 11. 2009, sp. zn. II. ÚS 2048/09.

Nález Ústavního soudu ze dne 7. 4. 2010, sp. zn. I. ÚS 22/10.

Rozsudek Nejvyššího správního soudu ze dne 21. 7. 2010, č. j. 3 Ads 42/2010-92.

Nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10.

Rozsudek Nejvyššího správního soudu ze dne 25. 11. 2011, č. j. 7 As 31/2011-101.

Nález Ústavního soudu ze dne 6. 3. 2012, sp. zn. I. ÚS 1586/09.

Nález Ústavního soudu ze dne 15. 5. 2012, sp. zn. II. ÚS 171/12.

Rozsudek Nejvyššího správního soudu ze dne 21. 12. 2012, č. j. 7 As 117/2012-28.

Nález Ústavního soudu ze dne 27. 1. 2015, sp. zn. Pl. ÚS 19/14.

Rozsudek Nejvyššího správního soudu ze dne 11. 6. 2015, č. j. 7 Azs 113/2015 - 34.

Nález Ústavního soudu ze dne 28. 2. 2017, sp. zn. IV. ÚS 3638/15.

Rozsudek Nejvyššího správního soudu ze dne 29. 11. 2017, č. j. 1 As 214/2017 – 32.

Rozsudek Nejvyššího správního soudu ze dne 6. 3. 2019, č. j. 2 As 153/2018-31.

Nález Ústavního soudu ze dne 8. 10. 2019, sp. zn. IV. ÚS 2287/18.

Rozsudek Nejvyššího soudu ze dne 29. 4. 2020, sp. zn. 23 Cdo 3071/2019.

Rozsudek Krajského soudu v Hradci Králové, pobočka v Pardubicích ze dne 22. 2. 2021, č. j. 52 A 86/2020-69.

Usnesení Ústavního soudu ze dne 2. 6. 2021, sp. zn. II.ÚS 255/21.

Usnesení Ústavního soudu ze dne 24. 8. 2021, sp. zn. IV. ÚS 1547/21.

Nález Ústavního soudu ze dne 11. 10. 2021, sp. zn. II.ÚS 1022/21.

Rozsudek Krajského soudu v Hradci Králové ze dne 28. 7. 2022, č. j. 30 A 76/2021-83.

Soudní dvůr EU:

Rozsudek ESD ze dne 20. 2. 1979 ve věci C-120/78, *Rewe-Zentral AG proti Bundesmonopolverwaltung für Branntwein*.

Rozsudek ESD ze dne 19. 11. 1991 ve věci C-6/90 a C-9/90, *Francovitch a Bonifaci*.

Rozsudek SDEU ze dne 26. 2. 2013 ve věci C-617/10, *Åkerberg Fransson.*

Rozsudek SDEU ze dne 26. 2. 2013 ve věci C-399/11, *Melloni.*

Rozsudek SDEU ze dne 13. 5. 2014, ve věci C-131/12, *Google Spain SL a Google Inc. v. Agencia Española de Protección de Datos (AEPD) a Mario Costeja González*.

Rozsudek SDEU ze dne 24. 9. 2019 ve věci C-507/17, *Google LLC, právní nástupkyně Google Inc. v. Commission nationale de l'informatique et des libertés (CNIL).*

Evropský soud pro lidská práva:

Rozsudek ESLP ze dne 10. 1. 2013, *Ashby Donald and Others v. France*, stížnost č. 36769/08.

Rozsudek ESLP ze dne 16. 6. 2015, *Delfi AS v. Estonia*, stížnost č. 64569/09.

Rozsudek ESLP ze dne 1. 12. 2015, *Cengíz and others v. Turkey*, stížnosti č. 48226/10 a č. 14027/11.

Rozsudek ESLP ze dne 16. 1. 2016, *Kalda v. Estonia*, stížnost č. 17429/10.

Mezinárodní soudní dvůr (dříve Soudní dvůr mezinárodní spravedlnosti):

Rozsudek Stálého dvora mezinárodní spravedlnosti v Haagu ze dne 26. 7. 1927, *Factory at Chorzów (Germany v. Poland)*. Dostupný: https://jusmundi.com/en/document/decision/en-factory-at-chorzow-jurisdiction-judgment-tuesday-26th-july-1927 [Cit. 2022-11-16].

Rozsudek Stálého dvora mezinárodní spravedlnosti v Haagu ze dne 7. 9. 1927, *The Case of the S. S. Lotus (France v. Turkey)*. Dostupné: https://web.archive.org/web/20101210073754/http://www.worldcourts.com/pcij/eng/decisions/1927/1927.09.07_lotus.htm [Cit. 2022-11-03].

Rozsudek Mezinárodního soudního dvora ze dne 9. 4. 1949, *Corfu Channel Case (United Kingdom of Great Britain and Northern Ireland v. Albania)*. Dostupný: http://www.icj-cij.org/en/case/1/judgments [Cit. 2022-11-02].

Rozsudek Mezinárodního soudního dvora ze dne 27. 6. 1986, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*. Dostupný: https://www.icj-cij.org/en/case/70 [Cit. 2022-11-14].

Rozsudek Mezinárodního soudního dvora ze dne 25. 9. 1997, *Gabčíkovo-Nagymaros Project (Hungary v. Slovakia)*. Dostupný: https://www.icj-cij.org/en/decisions/judgment/1997/1997/desc [Cit. 2022-11-15].

Ostatní:

Nález Spolkového ústavního soudu ze dne 15. 12. 1983, č.j. BVerfGE 65, 1.

Rozsudek Nejvyššího soudu USA ze dne 11. 6. 2001, *Kyllo proti Spojeným státům americkým*, 533 U.S. 27. Dostupný: https://www.law.cornell.edu/supct/html/99-8508.ZO.html [Cit. 2022-10-29].

5. Seznam ostatních zdrojů

ČESKÝ ROZHLAS RADIOŽURNÁL. *František Vrabel: Více než 90 % dezinformačních webů v Česku jedná ve prospěch Ruska* [online]. Host Lucie Výborné, 27. 11. 2020. Dostupné: radiozurnal.rozhlas.cz [Cit. 2021-11-14].

Stanovisko generálního advokáta Soudního dvora EU Michala Bobka ve věci C-194/16, *Bolagsupplysningen OÜ Ingrid Ilsjan proti Svensk Handel AB*.

VLÁDA. Důvodová zpráva k návrhu ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky, č. 110/1998 Dz.

VLÁDA. Usnesení č. 781 ze dne 19. října 2011 o ustavení NBÚ gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast.

VLÁDA. Důvodová zpráva k zákonu č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), č. 181/2014 Dz.

VLÁDA. Důvodová zpráva k zákonu č. 104/2017 Sb., kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a některé další zákony, č. 104/2017 Dz.

VLÁDA. Důvodová zpráva k zákonu č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony, č. 205/2017 Dz.

VLÁDA. Důvodová zpráva k zákonu č. 35/2018 Sb. o změně některých zákonů upravujících počet členů zvláštních kontrolních orgánů Poslanecké sněmovny, č. 35/2018 Dz.

Kyberprostor a informační bezpečnost

Abstrakt

Disertační práce se věnuje bezpečnosti informací v kyberprostoru a kybernetické bezpečnosti. Z hlediska zájmu akademické obce se jedná o opomíjenou oblast, ačkoli kybernetická bezpečnost je jedním ze základních předpokladů nerušeného výkonu veřejné správy.

Práce pojednává o tématu v širších teoretických i praktických souvislostech. S ohledem na stěžejní vliv probíhajících technologických změn ve společnosti na právní úpravu i praxi nabízí první část vhled do problematiky pomocí rozboru klíčových společenských proměn souvisejících s digitální revolucí a globalizací, hodnot informační společnosti, principů právní úpravy kybernetické bezpečnosti i otázek působení práva v kyberprostoru.

Druhá část pojednává o úloze veřejné moci na zajištění informační bezpečnosti v kyberprostoru. Rozebrány jsou pojmy kybernetické obrany a kybernetické bezpečnosti. Bezpečnost informací a dat je v práci charakterizována skrze složky důvěrnosti, integrity (celistvosti) a dostupnosti. S ohledem na častý mezinárodní prvek se práce věnuje i pohledu mezinárodního práva na kybernetické operace díky rozboru vybraných pravidel druhé verze Tallinnského manuálu. Řešeny jsou zejména problémy přičitatelnosti kybernetických útoků státu, zpětný hacking (*hack-back*) a okolnosti vylučující protiprávnost kybernetických operací.

Třetí část se věnuje zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů. Zabývá se především systémem zajištění kybernetické bezpečnosti skrze bezpečnostní opatření preventivního charakteru i skrze opatření v užším slova smyslu, jimiž jsou varování, reaktivní opatření a ochranná opatření. Ve snaze propojit teoretickou a aplikační rovinu jsou rozebrána dosud vydaná opatření ústředního správního úřadu kybernetické bezpečnosti a analyzován jejich dopad v podmínkách České republiky. Prostor je věnován i souvisejícím zákonným institutům, jakými jsou povinnost předat data, provozní údaje a informace, nápravná opatření, týmy reagující na počítačové bezpečnostní incidenty a parlamentní kontrola výkonu správy v oblasti kybernetické bezpečnosti.

Disertační práce pojednává o případech narušení bezpečnosti informací, jurisdikčních konfliktech, mezinárodní odpovědnosti státu v kyberprostoru, a o dalších souvisejících tématech. Přes specifika kybernetického prostředí je právo obhajováno jako vhodný nástroj regulace, přičemž je současně zdůrazněn požadavek trvat na ústavním principu vázanosti státní moci zákonem i v kybernetickém prostředí.

Klíčová slova: informace, kybernetická bezpečnost, veřejná moc

Cyberspace and information security

Abstract

The dissertation deals with information security in cyberspace and cybersecurity. Within the academic community the topic is rather neglected, even though cybersecurity may be seen as a pillar-stone for the undisturbed performance of public administration.

The thesis deals with the topic in broader theoretical and practical contexts. Technological changes in society have major influence on legal regulation and practice. Because of that, the first part of the thesis focuses on the key social changes related to digital revolution and globalization, on the values of the information society and on the principles of cybersecurity regulation, as well as on the issues regarding the applicability of law within cyberspace.

The second part of the thesis discusses the role of public power in safeguarding the information security in cyberspace. The concepts of cyber defence and cybersecurity are discussed. The concept of information security is presented through the confidentiality, integrity and availability components. The international element is addressed with the perspective of selected rules of the second version of Tallinn Manual. In particular, the problems of attribution of cyber operations, reverse hacking (hack-back) or circumstances precluding wrongfulness of cyber operations are dealt with.

The third part of the thesis focuses on the Czech Cybersecurity Act (Act N. 181/2014 Coll. on the cybersecurity and on related changes). It mainly deals with the system of ensuring cybersecurity through administrative measures, which are the preventive security measures and the specific measures called warning, reactive measures and protective measures. The administrative measures issued so far by the Czech central administrative body, National Cyber and Information Security Agency, are analysed, as well as their impact in the Czech Republic. The thesis also deals with related topics, such as the legal obligation to hand over data, operational data and information, the remedy measures, the computer security incident response teams, or the parliamentary control over the National Cyber and Information Security Agency.

The examples of information security violations, conflicts of jurisdiction, international responsibility of states for cyber operations, and other related topics are discussed. Despite the specific features of cyberspace, the law is defended as a suitable instrument of regulation. The thesis also emphasises that the constitutional principle according to which state power has to be bound by the law needs to be applied in cyberspace as well.

Key words: information, cybersecurity, public authority