MASARYKOVA UNIVERZITA

PRÁVNICKÁ FAKULTA

Ústav práva a technologií

PRÁVO A KYBERNETICKÁ BEZPEČNOST ČESKÉ REPUBLIKY

DIPLOMOVÁ PRÁCE

VEDOUCÍ PRÁCE: doc. JUDr. Radim POLČÁK, Ph.D.

Jiří PLATOVSKÝ

akademický rok 2012/2013

Můj dík za podporu a pochopení při zpracovávání této diplomové práce patří doc. Radimu Polčákovi, vedoucímu práce. Děkuji všem blízkým přátelům i kolegům spolužákům, kteří mi v různých okamžicích poskytli povzbuzení nebo inspiraci slovem nebo činem. Děkuji svým rodičům a prarodičům, kteří po celou dobu vzniku této práce trpělivě snášeli všechny mé strasti a nářky.

Čestně prohlašuji, že jsem diplomovou práci s názvem „Právo a kybernetická bezpečnost České republiky“ zpracoval sám a že jsem uvedl veškeré použité prameny.

OBSAH

1. ÚVOD ... 5

2. **KYBERNETICKÁ BEZPEČNOST ... 7**

2.1. Pojem kybernetické bezpečnosti ... 7

2.2. Předmět ochrany ...13

2.3. Přehled účinné právní úpravy ...15

2.4. Věcný záměr zákona ČR o kybernetické bezpečnosti ...22

3. **AKTUÁLNÍ PROBLÉMY KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ...25**

3.1. Narušení kybernetické bezpečnosti: Rozsah a dosah jurisdikce orgánů České republiky ...25

3.2. Mezinárodní kybernetický konflikt ...32

3.3. Ústavní konformita navrhované regulace kybernetické bezpečnosti v ČR ...36

***4.* ZÁVĚR ...44**

POUŽITÉ ZDROJE ...46

Abstrakt. Narůstající závislost nejen soukromých subjektů, ale též orgánů veřejné moci na informačních technologiích staví do popředí naléhavou otázku zabezpečení fyzické informační infrastruktury a uložených, často velmi citlivých dat. Práce analyzuje pojem kybernetické bezpečnosti jak z hlediska technického (aktuálních hrozeb a možností zabezpečení), tak z hlediska právního, přičemž důraz je kladen na připravovaný Zákon České republiky o kybernetické bezpečnosti a dosah jurisdikce správních a soudních orgánů České republiky v prostředí informačních sítí (kyberprostoru). Práce se zabývá též fenomény úzce souvisejícími, konkrétně kybernetickým terorismem, právní odpovědností poskytovatelů služeb informační společnosti (ISP) a hodnocením přeshraničních kybernetických útoků z pohledu mezinárodního práva (veřejného).

Mimo rozsah práce naopak zůstávají např. otázky mezinárodního práva soukromého na internetu, kyberkriminality a patologických sociálních jevů v prostředí informačních sítí.

Klíčová slova. Česká republika, kybernetická bezpečnost, kyberprostor, internet, infrastruktura, zabezpečení, věcný záměr, zákon, právo, mezinárodní, veřejné, terorismus, informační, komunikační, technologie, síť

Abstract. *Law and Cybersecurity of the Czech Republic (Master Thesis)* addresses an urging question of security of IT infrastructure and (in some cases very sensitive) data stored in the Czech Republic, given the rising dependence of both private and public entities on IT resources and tools. The thesis analyzes the term „cybersecurity“ from both technical (current threats and countermeasures available) and legal point of view. In the latter emphasis is put on Czech Republic Draft Bill on Cybersecurity and a scope of jurisdiction of Czech courts and administrative bodies in cyberspace.

The thesis also briefly examines some related topics, particularly cyberterrorism, legal liability of Information Services Providers (ISPs) and assessment of cross-border cyberattacks under current international (public) law.

On the other hand, from the scope of the thesis are excluded, but for possible exceptional remarks, topics of international private law in cyberspace, cybercrime and misbehaviour in cyberspace.

The language of the thesis is Czech.

Keywords. Czech Republic, cybernetic, security, cybersecurity, cyberspace, Internet, infrastructure, security, protection, draft, bill, law, international, public, terrorism, cyberterrorism, information, communication, technology, IT, ICT, net

1. ÚVOD

Když se řekne „bezpečnost“, nabízí se hned vzápětí otázka „čeho?“. Bezpečnost, existence bezpečí, ochrana před škodlivými událostmi, zásahy a vlivy, doprovází lidstvo už od jeho počátků. S rozvojem lidské civilizace se ale dosah tohoto pojmu rozšiřuje: nestačí už pouhá ochrana života, přistupuje snaha ochránit majetek, lidskou důstojnost, výsledky lidské tvořivosti a konečně také chránit informace.

Sám pojem „informace“ je ale slovem značně obecným a proto mnohovýznamovým: nejblíže nám pak bude zřejmě pojetí informace jako smysluplného výroku o realitě (ať v podobě deskriptivní, tj. konstatování faktu nebo normativní, tj. stanovení pravidla) a dále jako protipólu chaosu (entropie)[1]. Za těchto okolností není objektivně možné a ani účelné chránit informace všechny – je nutné nalézt takové z nich, u kterých dává ochrana rozumný smysl a slouží účelu, který je podle našeho dosavadního poznání dostatečně závažný.

Novou dimenzi, pokud jde o existenci informací vůbec, ale též o jejich rozšiřování, resp. sdílení, dostupnost, ochranu, ale i ohrožení, přinesl bouřlivý rozvoj informačních technologií v posledních dvou desetiletích 20. století. Zrodily se výkonné osobní počítače, jejich sítě a konečně globální síť internet. Informační prostředí postavené na jedničkách a nulách pak zrodilo nové fenomény: kyberprostor a kód jako jeho určující normativně-kauzální hranici možného a nemožného, anebo, chceme-li, architekturu[2].

Kyberprostor je tím, co do jinak odosobněného prostředí bitů, bytů, rozhraní, pamětí a dat vnáší uvědomělý lidský prvek: především pak kontakt, interakci, smysluplnost a účelnost logických operací. Kyberprostor tedy omezujeme a zároveň (byť spíše pro potřeby vědecké než z hlediska reality) oddělujeme od světa reálného; to, co člověk v kyberprostoru vytváří, ať ve smyslu hmotném nebo sociálním, pak můžeme nazývat realitou virtuální.

Tak jako mantinely reálného světa jsou dány především přírodními zákony, pak mantinely kyberprostoru je kód – sled logických, silně formalizovaných instrukcí, které jednak vytvářejí virtuální prostředí (protokoly, weby, služby), jednak mají za úkol reagovat na činnost jednotlivce-uživatele, který se v tomto prostředí pohybuje a koná (přenáší data, vyhledává informace, vytváří autorská díla, využívá e-mailu, chatu apod.).

Kód, jak nám ho přibližuje kupř. americký konstitucionalista Lawrence Lessig[3], je fenoménem kdesi na pomezí normativity a kauzality: stanovuje limity lidského chování v kyberprostoru, ale i limity a zákonitosti kyberprostoru jako takového. Při charakteristice kódu jako definiční normy[4] kyberprostoru můžeme s ohledem na jeho původce – člověka – jít ještě o krok dál

---

1 Výsledkem působení informace jako elementu, který snižuje chaos, je organizace, resp. smysluplný řád. K podrobnějšímu výkladu srov. POLČÁK, R. *Internet a proměny práva.* 1. vyd. Praha: Auditorium, 2012. ISBN 9788087284223, zejm. str. 26-30.

2 Srov. LESSIG, L. *Code, version 2.0.* 2nd ed. New York: Basic Books, 2006. 410 str. ISBN 0465039146

3 Tamtéž.

4 Definiční normu je nutno oddělovat od definiční autority. Zatímco definiční normu kyberprostoru, formalizovanou do podoby kódu, může vytvářet relativně široké spektrum jednotlivců a jejich skupin po celé planetě, definiční autoritou rozumím zvláštní právnickou osobu, která zásadním způsobem zajišťuje a reguluje provoz internetu a přístup k němu.

a vyslovit filozofickou myšlenku, že člověk právě novým způsobem zúročil svoji schopnost tvořit, že vpravdě „stvořil nový svět“, který dále i jeho samého zpětně utváří. Zároveň stojí za povšimnutí, že kyberprostor by se podle hesla „Opakování, matka moudrosti“ mohl stát jistým, byť neuvědomělým odrazem lidské interakce, jak byla praktikována v primitivních pospolitostech na úsvitu dějin. Teprve reflexe celého tohoto vývoje ukáže, zda se nám před očima znovu odehrával od počátku příběh člověka – tvora společenského – jeho potřeby bezpečí, učení, motivace i adaptace, byť poněkud v jiné podobě a v jiném, protože virtuálním světě.

Kyberprostor, resp. jeho bezpečnost z technického, ale především z právního hlediska, je i tématem této práce. Toto téma jsem si vybral proto, že mě zajímá a svým způsobem fascinuje propojení práva jako disciplíny humanitní, jejímž východiskem i cílem je kvalitnější život jedince i celku, s prostředím internetu, které bytostně stojí na přírodních zákonitostech a technických standardech. Mým druhým důvodem je moje osobní zaujetí hledáním nových, originálních cest a možností v různých oblastech lidské činnosti spíše než jen popis toho, co již přede mnou objevili povolanější.

Mým cílem je nejprve obecně popsat problematiku kybernetické bezpečnosti – zejména s ohledem na Českou republiku, její zájmy a hrozby, kterým musí jako stát i jako záštita svých občanů, resp. obyvatel v kyberprostoru čelit. V obecné části práce tedy uvádím jednak vymezení pojmu kybernetické bezpečnosti, aktuální technologie útoků v kyberprostoru, dále cíle těchto útoků, resp. hodnoty a statky, které je nutno v zájmu státu i jednotlivců chránit a poté dvě právní témata. Prvním z nich je přehled účinné právní úpravy (tj. práva *de lege lata*) v České republice, v rámci Evropské unie, relevantních mezinárodních dokumentů a též stručný nástin aktuálního právního vývoje ze Spojených států amerických. Druhé téma pak otevírá věcný záměr českého zákona o kybernetické bezpečnosti.

Ve zvláštní části se věnuji celkem třem otázkám, jejichž společným atributem je nejednotný přístup vědecké obce k jejich řešení, event. nedostatek odborné diskuse obecně. Jde konkrétně o otázky dosahu jurisdikce orgánů ČR na úseku kybernetické ochrany, potažmo českých soudů a také o dosud nepříliš zkoumanou, avšak do budoucna stále naléhavější problematiku mezinárodního kybernetického konfliktu („kyberválky“) včetně nejen právně, ale i politicky citlivého tématu odpovědnosti státu za kybernetický útok vedený z jeho území. Jako třetí téma jsem zvolil problematiku ústavní konformity zákona o kybernetické bezpečnosti v podobě, v níž je předvídán svým věcným záměrem, též řešeným v této práci.

Práce se obecně hlásí k pragmatické právní metodě. Pokud jde o obecně logické metody, použité při jejím zpracování, pak v části obecné převládá zejména analýza a dedukce, v části zvláštní je stěžejní použití metody induktivně-deduktivní a analyticko-syntetické.

I když se práce zabývá i otázkami technickými, její těžiště leží v rovině právní. Proto její text nenabízí optimální šíři informací o technologiích a technologických trendech, ale pojímá tyto spíše jako východisko pro diskusi otázek právní teorie i praxe.

Jelikož jde o diplomovou práci, nemám přehnaná očekávání, pokud jde o její popularitu či přínos vědecké obci. Přál bych si ale aspoň, aby se z ní nestal jen další zaprášený ozdobný svazek ve fakultní knihovně, resp. netknutý soubor v Informačním systému Masarykovy univerzity.

2. KYBERNETICKÁ BEZPEČNOST

2.1. Pojem kybernetické bezpečnosti

Pojem kybernetické bezpečnosti nebo bezpečnosti kyberprostoru je nutné definovat na podkladě obou uvedených slov. Kyberprostorem rozumíme v této práci soubor zařízení, dat, resp. informací, komunikačních rozhraní a protokolů, které umožňují sociální interakci. Nejtypičtějším příkladem kyberprostoru je síť internet, nicméně příkladů existuje mnohem více (vnitropodnikové sítě a informační systémy, sítě mobilních telefonů, platební systémy apod.). O kyberprostoru se někdy mluví i jako o virtuální nebo paralelní realitě. *Bezpečností* je pak stav ochrany před vznikem škody (angl. security), resp. stav zamezující hrozbě pro lidský život, zdraví, majetek nebo prostředí (angl. safety).[5] Bezpečnost je možné definovat i jinak, např. jako takovou vlastnost sociálních struktur, které zajišťují ekonomickou a politickou moc vládnoucí skupiny nebo přežití sociálního systému za současné přiměřené úrovně veřejné bezpečnosti.[6] Podle jiné definice je bezpečnost absencí války spolu s pravděpodobným předpokladem, že případná válka by nevedla k porážce daného státu,[7] popř. obecně jako schopnost státu (systému hodnot, entity) odolat vnější (dodávám, že i vnitřní) agresi.[8] Wolfers pak hovoří v objektivní rovině o absenci hrozeb sdíleným hodnotám a v rovině subjektivní o absenci strachu z útoku na tyto hodnoty.[9] Bezpečnost nicméně není hodnotou absolutní[10] a je nutno ji vážit – zvláště v prostředí moderního demokratického státu – se svobodou a s minimalizací zásahu do lidských práv. Bezpečnost je veřejným statkem (či, chceme-li veřejným dobrem[11]), z jehož užívání nelze zcela jednoduše vydělit konkrétní osobu nebo skupinu osob. Bezpečnost každopádně nelze zužovat pouze na oblast bezpečnosti vojenské, resp. zajišťované ozbrojenými sbory – a to i u vědomí, že mimo oblast armádní bezpečnosti zdaleka nepanuje všeobecná shoda, jak široké má vymezení tohoto pojmu, potažmo vymezení zásahu státu a jeho orgánů do sféry jednotlivců a soukromých entit být.[12]

Na průsečíku obou významů pak leží výraz kybernetická bezpečnost nebo též zkráceně kyberbezpečnost. Význam tohoto pojmu lze chápat buď staticky, tj. jako cíl, jehož má být dosaženo, ale též jako proces návrhu, realizace a zpětné kontroly bezpečnostních mechanismů. Cílem je jednak prevence bezpečnostních hrozeb, dále adekvátní ochrana před jejich výskytem,

---

5 MATYÁŠ, V. et al. *Ochrana dat a informačního soukromí [online].* Cyklus přednášek v rámci stejnojmenného kurzu na Katedře počítačových systémů a komunikací Fakulty informatiky Masarykovy univerzity v podzimním semestru akademického roku 2012/2013. Brno: Masarykova univerzita, 2012.

6 Tuto definici razí József Balázs a uvádí ji BUZAN, B. *The National Security Problem in International Relations.* In: HUGHES, C. W., MENG, L. W. (eds.) *Security Studies. A Reader.* 1st ed. Abingdon (UK), New York: Routledge, 2011. ISBN 9780415326001 (hardback), 9780415326018 (paperback), str. 20.

7 Tuto definici uvádí Ian Bellany tamtéž.

8 Tamtéž definice Giacoma Lucianiho, str. 21 et al.

9 Tamtéž, str. 21.

10 ULLMAN, R. *Redefining Security.* In: HUGHES, C. W., MENG, L. W. (eds.) op. cit. sub 6, str. 12.

11 Srov. tamtéž, str. 14.

12 Srov. tamtéž, str. 16.

resp. řešení bezpečnostních událostí (incidentů) a též případně postih (represe) jejich původce. Prevence a řešení bezpečnostních incidentů je přitom zcela nezbytnou součástí bezpečnostní strategie každého subjektu s realizovaným přístupem do kyberprostoru.[13] Kybernetickou bezpečnost můžeme také chápat buď jako soubor organizačních, technických a jiných nástrojů k ochraně prostředí před útoky a hrozbami, anebo jako ucelený systém mechanismů umožňujících v případě útoku identifikovat osobu jeho původce a působit tak potenciálně odstrašujícím účinkem.

Kyberbezpečnost je podmnožinou informační bezpečnosti a ve své nejobecnější podobě zahrnuje tři velké oblasti informací, u nichž je dán zájem na jejich ochraně, a to z důvodů ekonomických (obchodní tajemství, smluvní dokumentace), právních (jejichž ochranu technickými prostředky pozitivně předepisuje objektivní právo, např. osobní údaje) nebo jiných. Tři zmíněné velké oblasti kyberbezpečnosti můžeme popsat jako ochranu identity, ochranu vlastního obsahu (dat, informací) a ochranu infrastruktury. Tyto tři oblasti jsou přitom provázány, takže narušení bezpečnosti jedné z nich může, a nezřídka má negativní dopad i na další dvě.

Narušení kybernetické bezpečnosti můžeme označit jako útok *(attack)*. Jeho primárním původcem je vždy člověk – fyzická osoba, bez ohledu na to, zda se provádění útoku v daném okamžiku osobně účastní, nebo zda např. pouze uvolní do kyberprostoru škodlivý kód, který vykonává určité akce již bez aktivního lidského zásahu. Právě tak je fyzická osoba *de facto* primárním původcem, ať je její jednání z právního hlediska přičitatelné komukoli (právnické osobě, státu apod.). Fyzická osoba – ať jako útočník, napadený či jakákoli třetí – tvoří společně s infrastrukturou, potažmo daty v její faktické dispozici tzv. socio-technický systém, který vykazuje určité zvláštnosti oproti klasické manipulaci s objektivní realitou.[14] Technologie útoků na informační infrastrukturu, potažmo kyberprostor, se s postupem doby vyvíjí jak co do početnosti (kvantity), tak do druhů útoků (kvality).[15]

---

13 Zde jedna právní odbočka. Minimálně z hlediska obecné teorie práva je zajímavý poznatek, že aktivně vstupovat do kyberprostoru dokáže z podstaty věci pouze fyzická osoba, živý člověk (pokusy s primáty nebo inteligentními roboty ponecháváme stranou). Kybernetickou bezpečnost jako stav, cíl (a do určité míry i jako proces) můžeme vysledovat jak u fyzických osob a jejich skupin bez právní subjektivity, tak u právnických osob. Zde by zřejmě rozhodujícím faktem pro určení byl nositel subjektivního práva ke statku (infrastruktuře, datům, *know-how*), který je nebo může být dotčen bezpečnostním incidentem.

14 Informační infrastruktura totiž prostřednictvím předem definovaných instrukcí má schopnost reagovat na lidskou akci, a tím také ovlivňovat akci bezprostředně následující. Oproti jiným lidským vynálezům a nástrojům má IT rovněž řádově mnohem větší variabilitu využívaných typů hardwaru i dat, k nimž uživatel přistupuje dle svých vzorců chování z „reálného“ světa, což ne vždy přináší žádoucí výsledky.

15 O předmětech útoků pojednává kapitola 2.2.

Technologie útoků[16]

Podle statistik z roku 2011 byly třemi nejčastějšími cíli útoků infiltrace (tj. neoprávněný, zpravidla vzdálený přístup k informační síti), dále agregace (tj. shromažďování) dat, ke kterým jinak útočník nemá mít přístup a konečně odstraňování dat z prostředí, na něž útok cílí.[17] V roce 2011 nabral na síle tzv. hacktivismus, tedy činnost, při níž kybernetický útočník cílí (často, byť ne vždy) na infrastrukturu a data životně důležitá pro zájmy státu. Nejedná se jako dříve o činnost výlučně za účelem nelegálního získání peněz nebo majetku, ale o formu politického protestu.[18] Klasický hacking, tj. prolomení ochranných mechanismů na úrovni softwaru, resp. dat, ovšem zůstává na scéně jako jedna z forem kyberkriminality.[19]

V obou případech se může jednat o přetížení infrastruktury (*Distributed Denial of Service,* DDoS)[20], zejména formou botnetového[21] útoku; spam[22]), krádež citlivých, potažmo přístupových dat nebo umožnění jednorázového, popř. trvalého neoprávněného vzdáleného přístupu k těmto datům (trojské koně, *keyloggery*; sociální inženýrství, často *phishing* nebo *pharming*[23],

---

16 Tato podkapitola byla zpracována s využitím materiálů *Sophos Security Threat Report 2012 [online].* K dispozici na www: http://www.sophos.com/en-us/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf (dále též *„Sophos"*) a

BROWN, S.B. (ed.) *Trustwave 2012 Global Security Report [online].* K dispozici na www: http://www.iseprograms.com/lib/Trustwave_2012GlobalSecurityReport.pdf (dále též *„Trustwave"*).

17 *Trustwave*, str. 7-9.

18 *Sophos*, op. cit. sub 16, str. 2. Proslulými se staly např. aktivity hackerské skupiny *Anonymous*, která v průběhu roku 2011 zaútočila na protest proti mezinárodní smlouvě ACTA *(Anti-Counterfeiting Trade Agreement)* mj. i na internetové stránky Vlády ČR.

19 Kyberkriminalita zahrnuje páchání trestných činů prostřednictvím kyberprostoru. Zahrnuje jak klasické skutkové podstaty (krádež, podvod, činy proti duševnímu vlastnictví), tak i skutkové podstaty nové, jedinečné (např. neoprávněný přístup k počítačové síti).

20 Česky distribuované odepření služby. Spočívá v současně zaslaném velkém počtu požadavků na přístup k určité stránce, službě, serveru. V důsledku překročení výpočetních možností se daná stránka (služba server) zhroutí a zůstane po určitý čas (do dostatečného snížení síťového provozu, restartu apod.) nedostupná.

21 Botnet je síť počítačů (zpravidla rozesetých po různých koutech kontinentu nebo i světa) ovládaných na dálku přes internet prostřednictvím škodlivého softwaru (*malwaru*).

22 Spam je souhrnné označení pro nevyžádané zprávy elektronické pošty a další sdělení. Jejich objem tvoří pravidelně 70-90% veškeré e-mailové komunikace. Prostřednictvím spamu je možné e-mailovou schránku kapacitně přehltit a tím zabránit dalšímu přijímání korespondence.

23 *Phishing* (jako slovní hříčka se slovem *„fishing"* přeložen českou internetovou komunitou vtipně jako „rhybaření") znamená zasílání podvodných e-mailových a jiných zpráv, zdánlivě odeslaných důvěryhodným subjektem (banka, softwarová společnost apod.). Ve falešném e-mailu je uživatel vyzván k vyplnění citlivých údajů (číslo účtu, PIN platební karty, heslo apod.) ze smyšleného důvodu (např. pro účely „obnovení databáze klientů"). *Pharming* je založen na podobném principu s tím, že jde o podvrženou internetovou stránku, která se tváří jako pocházející z důvěryhodného zdroje.

kompromitované standardní internetové stránky). V krajním případě může dojít až k (nejčastěji vzdálenému) převzetí kontroly nad infrastrukturou (*rootkity*).

Škodlivé programy (tj. *malware* obecně) se šíří jak po různých platformách (*PC, Apple*, chytré mobilní telefony), tak i v různých operačních systémech (*Windows, Linux, Apple iOS* u stolních zařízení a tabletů; *Android, Windows Phone*, méně pak *Bada* a *Symbian* pro chytré mobilní telefony), a to i prostřednictvím přenosných médií (*USB* a *SSD* disků, *DVD/Blu-ray* disků apod.).[24] Pro jeho šíření se kromě shora uvedených technologií sociálního inženýrství (včetně tzv. *fake antivirus* software[25], tedy falešných antivirových programů, které jsou ve skutečnosti *malwarem*), využívá i tzv. černých děr (*blackholes*).[26]

Rizikovým elementem kyberprostoru, resp. lokální sítě mohou být i vlivy zevnitř konkrétní entity nebo státu. Jeden z nich spočívá již v samotné účasti lidského faktoru a jeho psychologických charakteristik (tendence k mechanickému opakování činností, k pohodlnosti, ale i k odplatě).[27] Mnozí pracovníci nejen v soukromém sektoru nevěnují dostatečnou pozornost bezpečnému výkonu své práce v kyberprostoru (to se týká zejména úrovně odesílaných a přijímaných dat a aktualizovaných obranných nástrojů – viz následující podkapitola). S tím souvisí i druhý rizikový trend, tzv. BYOD[28] (angl. *Bring Your Own Device*, tedy dosl. „přines si své vlastní zařízení"), který je pohodlnější pro zaměstnance, ale rizikovější pro zaměstnavatele vč. státu, neboť různá zařízení mají – při neexistenci vynucovaných minimálních společných standardů ochrany – různou úroveň zabezpečení; mimo pracovní dobu se pak mohou pohybovat v různě rizikovém prostředí.

S tím, jak se zvyšuje závislost veřejné správy na informačních a komunikačních technologiích, roste i pravděpodobnost, že některé služby (disková úložiště, platformy, software, výpočetní

Někteří pachatelé trestné činnosti na internetu pak mezi léty 2011-2012 posunuli hranice sociálního inženýrství ještě o krůček dál: vybrané „oběti" oslovují telefonem a vydávají se za pracovníky určité důvěryhodné společnosti. Využívají přitom znalostí o oběti nalezených (dosl. „vygooglovaných") na internetu a také současného rozmachu telemarketingových kampaní.

24 Srov. *Sophos,* op. cit. sub 16, str. 14-19.

25 *Sophos,* op. cit. sub 16, str. 10.

26 Černá díra je mechanismus nepozorovaného přesměrování uživatele z kompromitované internetové stránky na server, z něhož se stáhne škodlivý program.

27 Nezanedbatelné procento útoků a krádeží dat v soukromé sféře pochází od zaměstnanců nebo bývalých zaměstnanců. A že ani lidé ve službách státu nejsou – minimálně v České republice – dokonale diskrétní, o tom svědčí četné zveřejňované odposlechy rozhovorů (nejen politicky) významných osob a úniky materiálů z trestních spisů. Posledním velkým případem zveřejnění utajovaných materiálů jsou v současné době aféry *WikiLeaks* (zveřejnění tajných materiálů amerických tajných služeb a diplomacie, z jejichž předání ke zveřejnění byl obviněn voják americké armády Bradley Manning) a *VatiLeaks* (záznamy o nekalých praktikách a zákulisních bojích v rámci hierarchie Svatého stolce, které měl vynést blízký spolupracovník tehdejšího papeže Benedikta XVI. (pontifikát 2005-2013)).

28 *Sophos*, op. cit. sub 16, str. 17.

výkon) bude poskytován v režimu cloud computingu (krátce cloudu).[29] Cloud je relativně nový koncept přístupu uživatele k softwaru[30] a interním datům. Obojí je uchováváno na oddělené infrastruktuře (v případě soukromých poskytovatelů cloudu většinou sdílené s jinými subjekty), ke které je možno přistupovat přes internet z jakéhokoli zařízení. Výhodou tohoto konceptu, zejména pro velké subjekty, je úspora nákladů na správu infrastruktury a neomezená místní a prakticky též časová dostupnost dat. Velkou nevýhodou je předání citlivých informací (ať již soukromé společnosti nebo veřejné správy) do rukou externího subjektu.[31]

Aktuální výzvou pro správu dat v kyberprostoru je fenomén tzv. *big data*, neboli relativně velkého množství dat (jejichž objem v globálním měřítku exponenciálně roste), s nimiž je nutno pracovat a vyhledávat v nich za velmi krátké časové úseky nebo dokonce v reálném čase.[32] [33]

Možnosti obrany

Kdykoli se objeví hrozba pro kyberprostor, je její více či méně zřetelnou prvotní příčinou člověk. Je proto potřebné při zvažování možností obrany proti naznačeným hrozbám vzít v úvahu nejen řešení technická (která budou níže dále rozvedena), ale též vhodné psychologické (na úrovni jednotlivců a organizačních struktur) a právní (na úrovni vnitrostátní i mezinárodní) aspekty. Jde např. o vhodné personalistické metody výběru a motivaci pracovníků, resp. o posílení mezinárodní spolupráce ve smyslu snazšího přístupu k nejmodernějším technologickým řešením,[34] potažmo usnadnění stíhání (vydávání osob, výkon rozsudků) nejzávažnějších forem protiprávního jednání (tj. zločinů proti mezinárodnímu právu), jichž by se mohly dopustit i osoby při narušování bezpečnosti kyberprostoru (zejména se jedná o fenomén kyberterorismu). K právním nástrojům obrany na bázi soukromoprávních vztahů patří též nepochybně sjednání pojištění pro případ určitých zvláště závažných bezpečnostních incidentů.

---

29 „Cloud“ znamená anglicky mrak. Protože data jsou dostupná odkudkoli, vyvolává to představu, že jsou kdesi „v mracích“, odevšad ze zemského povrchu dosažitelné.

30 Software poskytovaný z cloudu, tedy nikoli nainstalovaný v zařízení uživatele, je poskytován jako služba (*Software as a Service*, SaaS).

31 Řešením by snad v oblasti veřejné správy mohl být tzv. privátní cloud, tj. zřízení cloudových úložišť přímo administrovaných příslušným správním úřadem, bez vyvádění dat mimo dosah veřejné správy.

32 V závislosti na velikosti a významu entity se objem dat může pohybovat od stovek gigabytů až po petabyty (tisíce terabytů). Pro více informací srov. *Big data pro začátečníky a pokročilé.* Příloha Computerworld a CIO Business World. Praha: IDG Czech Republic, a.s., 2012.

33 V době uzávěrky této práce média informovala o masivním útoku vedeném především technologií DDoS na český kyberprostor z ruských IP adres. Kromě komerčních internetových stránek (bank, telekomunikačních operátorů) byl zasažen např. Registr vozidel nebo Burza cenných papírů Praha. Srov. http://aktualne.centrum.cz/domaci/zivot-v-cesku/clanek.phtml?id=773306 Poslední aktualizace: 07.03.2013 [cit. 07.03.2013] nebo též *Češi čelí největším kyberútokům v historii.* In: Deník Právo, rok 2013, ročník 23, č. 56, 7. března 2013, str. 4, ISSN 1211-2119. [cit. 07.03.2013].

34 Určitým příslibem do budoucna by mohly být např. jednání o liberalizaci obchodu mezi EU a USA, jejichž zahájení je plánováno v průběhu roku 2013.

Úvod k technickým řešením. Pro kritickou infrastrukturu[35] je nezbytné vymezit přísná pravidla omezení (fyzického, faktického) přístupu, přičemž jako metody identifikace je vhodné použití kombinace více na sobě nezávislých prvků (jak biotechnologické identifikátory, např. otisk prstu, obraz oční sítnice nebo techniky rozpoznání hlasu, tak např. *tokeny*, tj. generátory jedinečných kódů, jejichž zadání je nutné pro uskutečnění určité požadované operace).[36] Jelikož při kombinaci bezpečnostních řešení vzniká velké riziko nesprávného povolení, popř. odepření přístupu[37], je vhodné pracovat s určitou škálou pravděpodobnosti (nastavit větší či menší toleranci pro neúspěšná ověření identity).[38] Nákladnost kybernetické bezpečnosti by měla být v rovnováze k závažnosti zabezpečovaných dat, očekávanému výskytu hrozeb a nežádoucím důsledkům eventuálního útoku.

Pravidelná zpráva společnosti *Trustwave* o globální bezpečnosti informačních sítí[39] navrhuje tzv. Pyramidovou strategii informační bezpečnosti, podle níž vždy opatření na nižší úrovni má nějakým způsobem zvýšit účinnost opatření stojícího výše. Jedná se konkrétně o šest stěžejních kroků (od základny pyramidy po její vrchol): vzdělávání zaměstnanců, identifikaci uživatelů informační sítě, homogenizaci hardwaru a softwaru, evidenci užívaného hardwaru (zařízení), sjednocení nástrojů pro vyhodnocování aktivity uživatelů v síti, resp. bezpečnostních incidentů a rizik v síťovém provozu a názorného modelování eventuálních incidentů s využitím dat, získaných mj. i pomocí postupů na nižších úrovních pyramidy. Jakmile se bezpečnostní expert dostal při implementaci na vrchol pyramidy, celý proces začíná znovu od jejího úpatí.[40]

Ochrana proti hacktivismu/hackingu. Jelikož žádné úložiště dat není možno před neoprávněným přístupem ochránit ve všech případech, nabízí se jako vhodné řešení šifrování dat.[41] Z hlediska ochrany vysoce citlivých dat je vhodnější šifrování asymetrické[42] s užitím soukromých klíčů k dešifrování jako certifikátů *sui generis* se zahrnutím mechanismu ověření identity konkrétního jednotlivce.

Ochrana přístupu k vymezené síti. V případě, kdy se jedná o přístup k určité komunikačními kanály provázané fyzické nebo logické infrastruktuře vč. datových úložišť, je vhodné používat komplexní hardwarová řešení. Jedná se mj. o UTM (*Unified Threat*

---

35 Srov. vymezení pojmu podle *Věcný záměr zákona o kybernetické bezpečnosti [online].* op. cit. sub 115.

36 MATYÁŠ, V. et al. op. cit. sub 5.

37 Tj. situace, kdy osobě je umožněn přístup, ač dle použitého algoritmu jí být umožněn nemá (angl. *false acceptance*), popř. odepření přístupu, ač dotyčné osobě dle algoritmu přístup umožněn být má (*false denial*). Cit. tamtéž.

38 Tamtéž.

39 BROWN, S.B. (ed.) *Trustwave 2012 Global Security Report [online].* K dispozici na www: http://www.iseprograms.com/lib/Trustwave_2012GlobalSecurityReport.pdf (dále též „*Trustwave*"), op. cit. sub 16.

40 Srov. *Trustwave*, op. cit. sub 16, str. 51-54.

41 *Sophos*, op. cit. sub 16, str. 4. K problematice šifrování srov. též MATYÁŠ, V. et al., op. cit. sub 5.

42 Principem asymetrického šifrování je užití dvou sad šifrovacích klíčů (tj. algoritmů k převodu nešifrovaných informací do šifrované podoby): veřejného klíče k šifrování a soukromého klíče (přiřazeného ke konkrétní osobě nebo entitě) k dešifrování.

Management) zahrnující mj. firewall, detekci a prevenci činnosti v rozporu s nastavenými mechanismy (IDS/IPS – *Intrusion Detection/Prevention Systems*)[43] a také zabezpečené brány (tzv. *secure gateways*), regulující síťový provoz mezi dotyčnou sítí a „vnějším" kyberprostorem.[44]

Hrozby uvnitř entity. V daném případě přichází v úvahu kontrola zaměstnanců, která se zaměří na monitorování jejich aktivit, které budou vyznačeny samostatně nebo v souběhu za rizikové.[45] V souladu s nutností vyvážit ochranu soukromí a sledování zaměstnaneckého chování v kyberprostoru je vhodné detailně sledovat pouze výchylky (zejména v delším časovém období) od obvyklých hodnot, určené s jistou mírou citlivosti.

2.2. Předmět ochrany

Předmětem (objektem) v nejobecnějším slova smyslu je objektivně či alespoň subjektivně existující realita nebo entita, zpravidla odlišná od člověka.[46] Realitou rozumím vše, co je způsobilé přinášet užitek (hmotné substance a jejich struktury, energie, práva a jiné majetkové hodnoty).[47] Entitou je naproti tomu pro účely této vymezení jednak právnická osoba (obchodní společnost, nezisková organizace), jednak útvar v rámci širší organizační struktury nebo hierarchie, který má dostatečně specifické požadavky na zabezpečení (organizační složka státu, konkrétní lokální síť apod.).

Takto vymezený předmět ochrany by nicméně stačilo podrobit vnitřním bezpečnostním opatřením, popř. v rámci všeobecné (event. *de lege ferenda* zvláštní) prevenční povinnosti.[48] Jestliže však stát hodlá vrchnostensky regulovat kyberprostor, čímž zasahuje do práv a svobod fyzických a právnických osob, je nutno takový zásah (a každý takový zásah) dostatečně legitimizovat, a to ochranou jiných práv, která v testu proporcionality[49] převáží. Zejména jde o práva uznávaná v evropském kontinentálním právu za základní, resp. zastoupená v katalozích základních práv nejvyšší právní síly (život, bezpečnost, soukromí, informace, projev,

---

43 VELECKÝ, P. *Důležité uzly firemní bezpečnosti.* In: ICT Revue, příloha deníku Hospodářské noviny, vydání 9.10.2012. [cit. 20.02.2013].

44 *Sophos*, op. cit. sub 8, str. 13.

45 Uvádí se např. časté návštěvy internetových portálů s nabídkou volných pracovních míst spolu s neobvykle velkými objemy dat stahovaných na vlastní zařízení nebo přenosná média. Srov. DOLEJŠ, R. *Bezpečnost 2.0 z Brna.* In: Computerworld, ročník 22, č. 17 Praha: IDG Czech Republic, a.s., 2011. ISSN 1210-9924.

46 Minimálně z právního pohledu je nemožné, aby člověk – fyzická osoba byl objektem jakéhokoli vztahu. Řekneme-li, že živý člověk je „objektem ochrany", vyjadřujeme tím nepřesně skutečnost, že se ochrana zaměřuje na hodnoty jeho osobnosti nebo na statky, které má jako osoba pod kontrolou.

47 Srov. ust. §118/1 občanského zákoníku, event. §979 nového občanského zákoníku.

48 Srov. ust. §415 občanského zákoníku, event. §2900 nového občanského zákoníku.

49 Filozofie základních práv v kontinentální právní kultuře stojí na axiomu, podle něhož v případě jejich konfliktu (kolize; typicky právo na soukromí a právo na informace) je nutno vážit práva v konkrétním případě na základě tří kritérií: potřebnost zásahu do jednoho z nich, vhodnost použitého (právního) nástroje a konečně minimalizace zásahu do jednoho z práv v kolizi, která ještě umožňuje náležité uplatnění práva druhého.

shromažďování a sdružování, informace, živ. prostředí, sociální jistoty).[50] Zajištění kybernetické bezpečnosti (a koneckonců bezpečnosti obecně) má tedy v demokratickém právním státu sloužit k uchování, ochraně základních práv a svobod.

V návaznosti na tři elementární průřezové kategorie (identita, obsah, infrastruktura – viz kap. 2.1.) můžeme objekt ochrany rozdělit ještě z dalších relevantních hledisek. Předně rozlišujeme objekt ochrany na hmotný (infrastruktura, budovy, nosiče dat) a nehmotný (software a data, vč. např. přístupových údajů). Obdobné dělení hovoří o makro úrovni (hardware, software) a mikro úrovni (obchodní tajemství, *business intelligence*[51] apod.).[52] Podle jiného dělení lze hovořit o čtyřech zásadních úrovních (levelech) ochrany podle závažnosti dotčených statků. První a nejvyšší úroveň obsazují bytostné, vitální zájmy státu (vojenská a civilní bezpečnost, veřejný pořádek, utajované informace apod.). Druhá úroveň zahrnuje tzv. kritickou infrastrukturu (tj. např. systémy odpovědné za chod vojenských a zdravotnických zařízení, elektráren apod.). Tyto dvě úrovně jsou zásadní z hlediska státem spravované kybernetické bezpečnosti. Na třetí úrovni stojí soukromá a veřejná infrastruktura zajišťující veřejné statky. Na čtvrté (nejnižší) úrovni důležitosti se pak nachází infrastruktura fyzických a právnických osob – spotřebitelů a podnikatelů.[53] [54] [55]

---

50 V posledních několika letech se, částečně v souvislosti s rozmachem „pirátského hnutí" (tj. hnutí, usilujícího o zrušení restrikcí, pokud jde o přístup k internetovému obsahu a jeho šíření), objevily diskuze o právu na internet jako o dalším základním lidském právu. Dle mého názoru lze právo na internet (hypoteticky) průřezově poskládat z práv občanských a politických (právo na informace, svobodu projevu, svobodu shromažďování aj.). Dostupnost vysokorychlostního internetu (řádově desítky až stovky Mb/s) za dostupné ceny (řádově stovky až tisíce Kč měsíčně) je již na takové úrovni, že toto právo, chceme-li jej uvažovat, je fakticky realizováno – a to i se zohledněním principu proporcionality (platba poskytovateli připojení, kapacita sítě). Problémovější jsou spíše otázky jeho omezení veřejnou mocí, jak je u jiných práv pravidelně předvídá LZPS (z důvodu ochrany veřejného pořádku, mravnosti, práv jiných apod.).

51 Business Intelligence je možno definovat jako „široké spektrum aplikací a technologií pro sběr, uchovávání, analýzu a zpřístupňování dat s cílem umožnit firemním uživatelům činit odpovídající obchodní rozhodnutí (překlad autora). Srov. ROUSE, M., ROSSETTI, L. *What is Business Intelligence? [online].* K dispozici na www: http://searchdatamanagement.techtarget.com/definition/business-intelligence Poslední aktualizace 11/2006 [cit. 29.01.2013].

52 POŽÁR, J. *Informační bezpečnost.* Plzeň: Aleš Čeněk, 2005. 311 str. ISBN 8086898385.

53 V současné době je vysoce aktuálním problémem na úrovni prvního „levelu" otázka zabezpečení tzv. základních registrů coby elektronických databází vysoce citlivých údajů o osobách, společnostech, právech apod., které byly jako unikát ve světovém měřítku spuštěny v ČR od 1.7.2012. Jejich úpravu obsahuje zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

54 Lze si nicméně představit narušení kybernetické bezpečnosti i přes soukromou infrastrukturu (např. botnetový útok aj., srov. technologie útoků v kap. 2.1.).

55 Srov. TRACHTMAN, J.P. *Global Cyberterrorism, Jurisdiction and International Organization [online].* Tufts University – The Fletcher School of Law and Diplomacy, 2004. Available via www: http://ssrn.com/abstract=56636, str. 5.

V prostředí informačních sítí nalézáme též dvě komplementární, avšak do určité míry nezávislé úrovně (vrstvy), které se odlišují podmínkami přístupu.[56] Nižší úroveň je charakteristická praktickou absencí nutnosti prokazovat identitu, obsah v ní zahrnutý je v zásadě volně přístupný.[57] Na vyšší úrovni je pak již vyžadováno ověření identity uživatele, který chce přístup získat; můžeme ji označit jako vrstvu „kvalifikovanou“ či „s kvalifikovaným přístupem“.

2.3. Přehled účinné právní úpravy

V přehledu účinné právní úpravy máme na mysli právní řády a normy České republiky, Evropské unie (které jsou různým způsobem účinné i v ČR), dále normy práva mezinárodního veřejného, zejména mezinárodní dohody, a konečně normy USA. Uvedeny jsou pouze nejdůležitější předpisy – formální prameny práva, které souvisí s předmětem práce, spolu s obdobně stručnou charakteristikou svého obsahu.

Právo ČR vnitrostátního původu

Základní právní rámec tuzemského práva tvoří ústavní pořádek, kam náleží především Ústava ČR (úst. zák. č. 1/1993 Sb.), Listina základních práv a svobod (úst. zák. 23/1991 Sb.) a ústavní zákon o bezpečnosti ČR (úst. zák. č. 110/1998 Sb.). Ústava provádí v nejobecnější rovině dělbu moci (a tedy i pravomoci vůči kyberprostoru) a upravuje postavení ratifikovaných mezinárodních smluv v právním řádu (čl. 10, 10a). Listina základních práv a svobod zajišťuje práva soukromých osob, do kterých veřejná moc nesmí zasahovat, event. kterých se proti ní mohou tyto osoby dovolat. V kontextu kyberprostoru jde především o práva osobnostní (soukromí, tajemství dopravovaných zpráv) a politická (svoboda projevu, právo na informace, svoboda shromažďování a sdružování). Pro řešení správních (méně již civilních a trestních) věcí na úseku kybernetické bezpečnosti má význam též právo na spravedlivý proces[58]

V oblasti práva náhrady škody dominuje občanský zákoník jako obecný předpis pro fyzické a právnické osoby. Všeobecná prevenční povinnost je přitom stanovena §415 občanského zákoníku[59] (nový občanský zákoník[60] ji přebírá v ustanovení §2900). Zákon o elektronických komunikacích[61] stanoví osobám podnikajícím v oblasti elektronických komunikací náležité

56 srov. LESSIG, op. cit. sub 2.

57 Následná dispozice s takovým obsahem nicméně může podléhat jistým omezením (typicky z důvodu autorských práv, nekalé soutěže apod.).

58 Zaručené čl. 36 a násl. Listiny a též čl. 6 Evropské úmluvy o ochraně lidských práv.

59 Zákon č. 40/1964 Sb., Občanský zákoník, ve znění pozdějších předpisů.

60 Zákon č. 89/2012 Sb., Občanský zákoník, účinný od 1.1.2014.

61 Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

zajištění bezpečnosti komunikační sítě (srov. např. §88 cit. zákona). Obecným procesním předpisem pro vymáhání eventuálních škodních nároků je občanský soudní řád (99/1963 Sb.).[62]

Prameny veřejného práva prostupují průřezově několik pododvětví. V oblasti práva informací[63] jako takového jde především o zákon o svobodném přístupu k informacím[64], který mj. ukládá zveřejňování vyžadovaných údajů způsobem umožňujícím dálkový přístup (v drtivé většině případů na internetu), zákon o utajovaných informacích[65], který kategorizuje určité informace jako vyhrazené osobám splňujícím bezpečnostní kritéria[66] a konečně zákon o archivnictví[67], který se zabývá uchováváním významných dokumentů (archiválií), mj. i v digitální, resp. digitalizované podobě. Jako základní nástroj pro práci s informacemi, uchovávaných veřejnou správou, slouží základní registry na podkladě stejnojmenného právního předpisu.[68] Na pomezí práva informací a následující kategorie, práva komunikačního pak stojí úprava autentizace a certifikace obsahu, ztělesněná zejména zákonem o elektronickém podpisu[69] a zákon o elektronických úkonech.[70]

Pod pojem „komunikační právo" podřadíme zejména obecnou úpravu elektronických komunikací (již zmíněný zákon o elektronických komunikacích[71], jehož věcná působnost jde nicméně nad rámec úpravy komunikace v kyberprostoru) a zákon o některých službách

62 Lze si hypoteticky představit i *ex post* dohodu škůdce a poškozeného o řešení v rozhodčím řízení. Pak by byl coby procesní předpis relevantní též Zákon č. 216/1994 Sb., o rozhodčím řízení a o výkonu rozhodčích nálezů (zákon o rozhodčím řízení), ve znění pozdějších předpisů. Pro potřeby této práce se jedná nicméně o otázku zcela marginální.

63 Není totožné s právem na informace, mám na mysli průřezové právní odvětví upravující zpřístupňování, šíření a utajování informací.

64 Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

65 Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Tento zákon prakticky (s výjimkou novelizujících ustanovení části třetí) nahradil od 1.1.2006 starší Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, ve znění pozdějších předpisů.

66 Blíže k problematice utajovaných informací srov. např. POKORNÝ, L. *Základy právní úpravy činnosti zpravodajských služeb.* 1. vyd. Praha: Vydavatelství PA ČR, 2007, 73 s. ISBN 9788072512423.

67 Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů (zákon o archivnictví), ve znění pozdějších předpisů.

68 Zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů. Tento zákon téměř zcela derogoval úpravu provedenou Zákonem č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých zákonů (zákon o informačních systémech veřejné správy), ve znění pozdějších předpisů.

69 Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů.

70 Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů.

71 Cit. sub 61.

informační společnosti[72], stanovící především limitaci odpovědnosti poskytovatelů služeb informační společnosti.[73]

V oblasti kybernetické bezpečnosti a nakládání s citlivými, resp. utajovanými daty, působí instituce, jejichž existence je též zakotvena na základě zákona. Konkrétně se jedná o Bezpečnostní informační službu[74], dále Úřad pro zahraniční styky a informace a Vojenské zpravodajství[75] a do budoucna *de lege ferenda* bude mít stěžejní postavení na tomto úseku veřejné moci, resp. veřejné správy Národní bezpečnostní úřad[76].

Stranou těchto skupin stojí samostatné předpisy se specifickým, avšak souvisejícím předmětem úpravy, konkrétně krizový zákon[77], zákon o platebním styku,[78] který řeší problematiku platebních služeb, bezhotovostních finančních operací a elektronických peněz, a zákon o mezinárodním provádění sankcí (69/2006 Sb.).

Základním hmotněprávním předpisem v oblasti přestupků a správních deliktů je Zákon č. 200/1990 Sb., o přestupcích, ve znění pozdějších předpisů. Úprava skutkových podstat je však rozeseta také po velkém počtu hmotněprávních předpisů správního práva. Na řízení podle shora uvedených veřejnoprávních předpisů se v různé míře vztahuje podpůrně správní řád[79], v případě přezkumu ve správním soudnictví pak též soudní řád správní.[80]

Obecným předpisem hmotného práva pro oblast trestních sankcí je trestní zákoník[81], účinný od roku 2010, resp. zákon o trestní odpovědnosti právnických osob.[82] Do oblasti trestních předpisů

---

72 Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů.

73 K jejich vymezení srov. kap. 3.1., podkapitolu „Problémy k řešení".

74 Bezpečnostní informační služba (BIS) byla zřízena Zákonem č. 154/1994 Sb., o Bezpečnostní informační službě, ve znění pozdějších předpisů. Bezpečnostní informační služba je jednou ze zpravodajských služeb České republiky, na něž dopadá i zákon o zpravodajských službách (cit. sub 75).

75 Všechny tři uvedené zpravodajské služby (BIS, Úřad pro zahraniční styky a informace a Vojenské zpravodajství) jsou regulovány Zákonem č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů. Jde o *lex generalis* práva zpravodajských služeb.

76 Národní bezpečnostní úřad byl zřízen Zákonem č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění pozdějších předpisů. Někdy je neformálně nazýván též kompetenčním zákonem.

77 Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů.

78 Zákon č. 284/2009 Sb., o platebním styku, ve znění pozdějších předpisů.

79 Zákon č. 500/2004 Sb., Správní řád, ve znění pozdějších předpisů.

80 Zákon č. 150/2002 Sb., Soudní řád správní, ve znění pozdějších předpisů.

81 Zákon č. 40/2009 Sb., Trestní zákoník, ve znění pozdějších předpisů. Kromě obecných skutkových podstat srov. např. ust. §§230 – 232.

82 Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, ve znění pozdějších předpisů.

spadá také Zákon o soudnictví ve věcech mládeže.[83] Obecným trestním procesním kodexem je trestní řád.[84]

Právo Evropské unie

Pravomoc k normotvorbě evropských orgánů v oblasti informačních a komunikačních technologií je založena ustanoveními Smlouvy o fungování Evropské unie (SFEU)[85] o spolupráci v trestních věcech (čl. 82 a násl.), správní spolupráci v rámci kapitoly „Prostor svobody, bezpečnosti a práva" (čl. 67 a násl.) a o transevropských sítích (č. 170 a násl.). Přímo použitelná nařízení a členským státům určené směrnice jsou v zásadě až na výjimky přijímány řádným legislativním postupem, tj. společně Radou EU a Evropským parlamentem na návrh Komise podle ust. čl. 293 a násl. SFEU. Unie v daných věcech uplatňuje pravomoc sdílenou se členskými státy (čl. 4/ 2h, 2j SFEU). Jen ve zcela obecné rovině, která bude vyžadovat konkretizaci soudními rozhodnutími unijních soudů, se problematiky kybernetické bezpečnosti týká Listina základních práv Evropské unie, a to ve svých článcích 6 (právo na svobodu a osobní bezpečnost), čl. 8 (ochrana osobních údajů), čl. 42 (právo na přístup k dokumentům) a čl. 47 a násl. týkající se právních záruk soudního a mj. též trestního procesu.

Ze sekundárních předpisů mají význam zejména Nařízení (ES) 460/2004 o zřízení Evropské agentury pro bezpečnost sítí a informací[86], Směrnice 95/46/ES[87], pokud jde o zpracování a volný pohyb osobních údajů; dále Směrnice 2002/58/ES[88] o ochraně soukromí v souvislosti se zpracováním osobních údajů a Směrnice 2008/114/ES[89] týkající se určování a označování evropské kritické infrastruktury; s problematikou škodních událostí souvisí též nařízení pro

83 Zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže), ve znění pozdějších předpisů.

84 Zákon č. 141/1961 Sb., Trestní řád, ve znění pozdějších předpisů. Zákon o trestní odpovědnosti právnických osob a zákon o soudnictví ve věcech mládeže obsahují speciální procesní ustanovení.

85 Smlouva o založení Evropského společenství ve znění Lisabonské smlouvy.

86 Nařízení Evropského parlamentu a Rady (ES) č. 460/2004 ze dne 10. března 2004 o zřízení Evropské agentury pro bezpečnost sítí a informací. Agentura má na starost mj. metodickou, poradenskou, informační, koordinační a osvětovou činnost. Je nápomocna Evropské komisi a podle potřeby i dalším orgánům EU. K únoru 2013 probíhala v Evropském parlamentu a v Radě diskuse o možnostech novelizace tohoto nařízení.

87 Směrnice Evropského parlamentu a Rady č. 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. V současné době se připravuje návrh nového nařízení s totožným předmětem úpravy. Srov. *COM 2012 (11) final [online]*. K dispozici na www: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:CS:PDF

88 Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací.

89 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).

určování mezinárodní příslušnosti soudu, rozhodného práva a uznávání rozhodnutí v jiných členských státech.[90]

Zvláštním instrumentem v evropském právu je uzavírání komunitárních mezinárodních smluv.[91] V této souvislosti je relevantní Smlouva mezi členskými státy Evropského společenství o výkonu rozhodnutí v trestních věcech z r. 1991 a Protokol k ní.

V únoru 2013 představila Evropská komise Návrh směrnice o kybernetické bezpečnosti[92], proklamující nutnost sjednocení úprav zabezpečení informačních sítí na minimálním standardu ve všech členských státech. Tato směrnice má podle důvodové zprávy napomoci snazšímu fungování vnitřního trhu, např. v oblasti snazšího přeshraničního sdílení informací, rozšířit dosud nedostatečnou, neboť převážně na telekomunikace orientovanou, regulaci.[93] Směrnice je navržena v souladu s ustanovení čl. 26 a čl. 114 SFEU (týkajících se zajištění fungování jednotného trhu, resp. opatření ke sblížení právních předpisů členských států).[94] V návrhu se dále konstatuje, že navržená úprava je v souladu s principem subsidiarity, když jednak reguluje problematiku přeshraniční povahy, jednak dosavadní ponechání problematiky *praeter legem* vyústilo ve spolupráci pouze menšiny členských států.[95]

Směrnicí nemají být podle čl. 1 odst. 4, 5 dotčeny vybrané předchozí předpisy (jmenovitě Směrnice 95/46/ES, 2002/58/ES a 2008/114/ES). Podle čl. 4 a násl. má vzniknout síť národních orgánů zodpovědných za adekvátní zabezpečení kyberprostoru v jejich dosahu, vč. CERTů[96]; směrnice dále upravuje kritéria a jejich spolupráci mezi sebou, dále s Evropskou komisí a s Evropskou agenturou bezpečností sítí a informací (ENISA)[97], potažmo s Europolem (srov. čl. 8, písm. f)). Spolupráce se týká zejména výměny informací, vyhodnocování aktuální bezpečnostní připravenosti národních systémů, popř. zajištění koordinované reakce na incident v souladu s navrženým čl. 11. Směrnice též předvídá zpracování národních plánů zabezpečení sítí a informací (čl. 5). Podle článku 13 je Unie zmocněna uzavírat mezinárodní smlouvy se třetími zeměmi v oblasti přenosu dat a bezpečnosti informačních sítí.

---

90 Nařízení Rady (ES) č. 44/2001 ze dne 22. prosince 2000 o pravomoci a uznávání a výkonu rozhodnutí v občanských a obchodních věcech („Brusel I“) a dále Nařízení Evropského parlamentu a Rady (ES) 864/2007 ze dne 11. července 2007 o právu rozhodném pro mimosmluvní závazkové vztahy („Řím II“)

91 Jedná se o praxi používanou pro případ, že členské státy EU projevily vůli upravit společný postup nebo zakotvit spolupráci v určité oblasti, v níž dosud nemělo Společenství, později Unie pravomoci.

92 *Návrh Směrnice Evropského parlamentu a Rady o opatřeních k zabezpečení vysoké jednotné bezpečnosti informací a sítí v Evropské unii. COM(2013) 48 final [online].* K dispozici na www: http://ict-law.blogspot.cz/2013/02/smernice-o-informacni-bezpecnosti.html Poslední aktualizace: 13.02.2013 [cit. 26.02.2012].

93 Tamtéž, str. 2-4.

94 Tamtéž, str. 8.

95 Srov. tamtéž, str. 8-9.

96 CERT je angl. zkratka pro *Computer Emergency Response Team.*

97 ENISA je angl. zkratka pro *European Network and Information Security Agency.*

Mezinárodní právo (veřejné)

Dokumenty OSN. Charta OSN byla podepsána v červnu 1945 v San Francisku zástupci zemí protihitlerovské koalice a neutrálních zemí[98] a položila základy Organizace spojených národů jako univerzální mezinárodní organizace s globálním dosahem, která nahradila meziválečnou Společnost národů a postupně značně svým významem přesáhla úlohu pouhého garanta míru a mezinárodní bezpečnosti.

V kapitolách VI a VII upravuje otázky války a míru, zákazu použití síly a základní právo na sebeobranu při napadení (čl. 51), jakož i prostředky mírového urovnávání sporů mezi státy mj. prostřednictvím Rady bezpečnosti OSN a Mezinárodního soudního dvora (čl. 92 a násl.; jeho Statut je nedílnou součástí Charty). To má význam zejména při právním hodnocení kybernetických konfliktů mezi státy jako konfliktů válečných (srov. kap. 3.2.). Charta OSN rovněž vytváří obecný právní rámec pro mezinárodní odpovědnost státu za jednání jeho orgánů nebo i jiných entit, jejichž jednání je podle mezinárodního práva státu přičitatelné.

Součástí mezinárodního zvykového práva a také mezinárodního *iuris cogentis*[99] je pak původně formálně nezávazná, avšak bezpochyby autoritativní Všeobecná deklarace lidských práv, schválená Valným shromážděním OSN v prosinci 1948.

Rada Evropy. Jde o regionální mezinárodní organizaci, jejímž cílem je mj. posilovat účelnou a mírovou spolupráci mezi evropskými zeměmi, a to i prostřednictvím mezinárodních smluv. Jejím ustavujícím dokumentem je Statut Rady Evropy, přijatý v květnu 1949. Po pádu železné opony se k členům Rady Evropy přiřadily i země bývalého východního bloku, včetně ČR.

Nejvýznamnější relevantní mezinárodní úmluvou v rámci Rady Evropy je Evropská úmluva o ochraně lidských práv a základních svobod z r. 1950. Česká republika se stala jejím smluvním státem již v r. 1993 a podle jejího Protokolu č. 9 přijala pravomoc Evropského soudu pro lidská práva (ECHR) rozhodovat o žalobách jednotlivců proti ČR (srov. čl. 34 Úmluvy).

I v rámci Rady Evropy pak existuje Úmluva o výkonu rozsudků v trestních věcech z r. 1970[100]; Česká republika však není její stranou.

Ostatní mezinárodní dokumenty. Smlouva o NATO (Washingtonská smlouva) byla uzavřena roku 1949 mezi USA a evropskými státy západního bloku. Založila Organizaci Severoatlantické smlouvy (*North Atlantic Treaty Organization*) jako specifickou regionální mezinárodní organizaci kolektivní bezpečnosti.[101] Její relevance vzhledem ke kyberprostoru spočívá mj. v možnosti použití kolektivní sebeobrany podle čl. 5 Smlouvy („Napadení jednoho smluvního státu je napadením všech.“) i v kybernetických konfliktech a při potírání

98 Tradičně neutrální Švýcarsko se členem OSN stalo nicméně až v roce 2002.

99 *Ius cogens* je souhrnem mezinárodních norem v jakékoli podobě (psané, obyčejové), od nichž se žádný člen mezinárodního společenství nesmí odchýlit za žádných okolností. Někdy se označují také jako normy „nederogovatelné“. Patří mezi ně např. zákaz genocidy, již zmíněný zákaz použití síly, resp. ozbrojené agrese, terorismu apod.

100 Originální název úmluvy v angličtině zní *Convention on the International Validity of Criminal Judgments* (ETS No. 70).

101 Tehdejší SRN byla přijata v r. 1955; v reakci na to vznikla Varšavská smlouva jako obdobná organizace zemí východního bloku (zanikla r. 1991).

kyberterorismu (viz níže). Ve druhé polovině roku 2011 schválili ministři obrany členských zemí NATO novou politiku v oblasti kybernetické bezpečnosti a zároveň tímto směrem zaměřený Akční plán.[102] Pilíře popsaných dokumentů by se daly popsat jako prevence (účinné mechanismy předcházení kybernetickým útokům), integrace (problematiky kyberbezpečnosti do obranného plánování) a spolupráce (s partnerskými nečlenskými státy, mezinárodními organizacemi, soukromou a akademickou sférou). Od července 2012 je jako sjednocující orgán NATO pro problematiku kyberprostoru vytvořena Agentura NATO pro komunikace a informace (NCIA).[103] Koncem roku 2012 se plánovalo uvedení do provozu tzv. NCIRC[104] jako specializovaného týmu pověřeného monitorováním bezpečnostní situace v kyberprostoru a prováděním vhodných opatření v případě ohrožení. Česká republika je členem NATO od r. 1999.

S problematikou mezinárodních kybernetických konfliktů jako konfliktů válečných souvisí též celkem čtyři Ženevské konvence jako mezinárodní dohody o právu válečných konfliktů.[105] První tři konvence (o zlepšení osudu raněných příslušníků ozbrojených sil, o zacházení s válečnými zajatci a o adaptaci principů první Ženevské konvence z r. 1864 pro potřeby námořní války) jsou výsledkem přepracovaných starších dohod o péči o raněné a o právu válečném, uzavřených též v Ženevě v letech 1864 a 1929 a v Haagu v r. 1899. Novodobé pilíře „ženevského práva“ se datují od r. 1949. Čtvrtá úmluva, přidaná k předchozím třem, se týká ochrany civilních osob za války. V roce 1977 byly přijaty dva Dodatkové protokoly týkající se válečných konfliktů mezinárodních, resp. vnitrostátních.[106] [107] [108]

Právo USA

Právo Spojených států jako právo anglosaského typu dosud neobsahuje komplexní legislativu, která by se zabývala regulací kyberprostoru.[109] Regulaci související problematiky obsahuje mj. *Patriot Act*, 2001[110], vydaný po teroristických útocích na budovy Světového obchodního centra

---

102 *NATO and Cyberdefence [online].* K dispozici na www: http://www.nato.int/cps/en/SID-F324DC04-0E8A51CF/natolive/topics_78170.htm? Poslední aktualizace: neuvedeno [cit. 25.02.2012].

103 Srov. tamtéž. NCIA je angl. zkratka *NATO Communications and Information Agency.*

104 Jde o angl. zkratku pro *NATO Computer Incident Response Capability.*

105 Právo válečné je věcně součástí širšího celku práva humanitárního.

106 Třetí Dodatkový protokol z r. 2005 pak upravuje problematiku rozeznávacích znaků bojujících stran.

107 Pro podrobnější výklad srov. ONDŘEJ, J., ŠTURMA, P., BÍLKOVÁ, V. et al. *Mezinárodní humanitární právo.* 1. vyd. Praha: C.H.Beck, 2010. ISBN 9788074001857, str. 141 a násl.

108 V oblasti práva válečného platí za velmi významné též normy obyčejového práva. Srov. ONDŘEJ, op. cit. sub 107, str. 127-135 nebo HENCKAERTS, J.-M., DOSWALD-BECK, L. *Customary International Humanitarian Law. Volume I: Rules.* 3rd ed. repr. with corr. Cambridge: Cambridge University Press, 2009. 628 str. ISBN 9780521005289 (chyb.).

109 *Věcný záměr zákona o kybernetické bezpečnosti [online].* op. cit. sub 115 [cit. 13.02.2013].

110 Plným názvem *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001 [online].* Srov. na www:

v New Yorku a ve svých deseti hlavách[111] umožňující rozsáhlejší sledování kybernetických i offline aktivit osob vč. odposlouchávání přenášených dat a zpráv, rozšíření oprávnění vyšetřovacích orgánů (FBI) a tajných služeb (CIA), ochranu hranic nebo zpřísnění předpisů trestního práva hmotného v oblasti terorismu. V průběhu roku 2012 byl předložen návrh zákona o kybernetické bezpečnosti (*Cybersecurity Bill*), ale k jeho schválení (ani ke schválení alternativních návrhů legislativní úpravy) zatím nedošlo. *Cybersecurity Bill* se dělí do devíti hlav[112], upravujících mj. ochranu kritické infrastruktury vč. ochrany informací, ochranu sítí provozovaných vládou USA, vzdělávání federálních zaměstnanců, výzkum a vývoj bezpečnostních řešení, sdílení informací a mezinárodní spolupráci, kde se výslovně v čl. 903 hlásí ke spolupráci s ostatními státy.[113] V únoru 2013 pak prezident USA Barack Obama vydal výnos za účelem koordinace postupu federálních orgánů v oblasti zvýšení zabezpečení kritické infrastruktury.[114]

2.4. Věcný záměr zákona ČR o kybernetické bezpečnosti[115]

Věcný záměr zákona o kybernetické bezpečnosti (dále též „věcný záměr“) byl představen v průběhu roku 2012. Vychází z potřeby sjednocení bezpečnostních mechanismů při ochraně kritické a další infrastruktury před individuálními útoky, kyberterorismem, průmyslovou a jinou špionáží, systému prevence a včasného varování[116] v českém kyberprostoru, při vědomí zvyšující se závislosti (informační) společnosti na informačních technologiích.[117] Cíli navrhované úpravy jsou zákonné stanovení práv a povinností orgánů veřejné správy a osob soukromého práva na úseku ochrany kyberprostoru, nastavení mechanismu přenosu informací pro prevenci, rozpoznání a následnou analýzu kybernetických útoků, standardizace bezpečnostních politik, potažmo opatření pro kritickou infrastrukturu státu a stanovení pravidel pro koordinaci v případě útoku nebo hrozícího útoku na ni.

---

http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf Poslední aktualizace: neuvedeno [cit. 07.03.2013].

111 Označení příslušné systematické jednotky jako „hlava“ (v orig. *title*) bylo zvoleno vzhledem k jejímu rozsahu, který přibližně odpovídá hlavám v českých právních předpisech.

112 Srov. pozn. 111.

113 *Cybersecurity Act of 2012 [online].* K dispozici na www: http://www.govtrack.us/congress/bills/112/s2105/text Poslední aktualizace: neuvedeno [cit. 26.02.2013].

114 *Executive Order – Improving Critical Infrastructure Cybersecurity [online].* K dispozici na www: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity Poslední aktualizace: neuvedeno [cit. 26.02.2013].

115 Tato kapitola byla zpracována s využitím materiálu *Věcný záměr zákona o kybernetické bezpečnosti [online].* K dispozici na www: http://www.nbu.cz/cs/aktuality/808-vecny-zamer-zakona-o-kyberneticke-bezpecnosti---verze-schvalena-vladou-/ Poslední aktualizace: neuvedeno. Citováno: viz následující odkazy k této kapitole.

116 Tamtéž, str. 5-6 [cit. 07.02.2013].

117 Tamtéž, str. 4 [cit. 07.02.2013].

Věcný záměr navazuje na Strategii pro oblast kybernetické bezpečnosti České republiky na období 2011 – 2015, přijatou vládou v červenci 2011.[118] V říjnu téhož roku pak následovalo ustavení Národního bezpečnostního úřadu (NBÚ) gestorem problematiky kybernetické bezpečnosti.[119] Věcný záměr počítá jednak se zřízením Národního centra kybernetické bezpečnosti jako jednoho z pracovišť NBÚ, odpovědného za monitorování českého kyberprostoru, podílení se na přípravě legislativy, metodiku, osvětu a výzkum.[120] Do budoucna se má NBÚ stát ústředním orgánem státní správy na úseku kybernetické bezpečnosti; do jeho pravomoci budou spadat všechny případy, vyjma těch, u nichž bude zřejmé, že mohl být spáchán trestný čin.[121]

Pro budoucí podobu předpisu byly po konzultacích s akademickou sférou navrženy tři základní zásady a tři regulatorní pilíře. K vytyčeným zásadám náleží: minimální, resp. minimalizovaný zásah do práv soukromoprávních subjektů, individuální odpovědnost za bezpečnost vlastní sítě a respektování a posílení práva na informační sebeurčení.[122] Pilíři navrhované regulace jsou ohlašovací povinnost kontaktních údajů a kybernetických bezpečnostních událostí, nutnost aplikace bezpečnostních opatření pro subjekty kritické infrastruktury a systém protiopatření pro řešení kybernetické ochrany.[123]

Zákon o kybernetické bezpečnosti má vymezit mj. kyberprostor jako takový, potažmo český kyberprostor (digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními a komunikačními technologiemi, zahrnujícími připojení k veřejné síti, resp. takové digitální prostředí vč. připojení k veřejné síti, které je regulováno právem ČR), kybernetickou bezpečnost (souhrn právních i mimoprávních opatření k zajištění bezproblémového fungování kyberprostoru), kritickou infrastrukturu (která má *ex lege* zahrnovat služby a sítě elektronických komunikací a informačních systémů a ve vztahu k soukromým osobám být určována prováděcími předpisy NBÚ), národní a vládní pracoviště CERT/CSIRT[124] a stav kybernetického nebezpečí (situace podstatného ohrožení bezpečnosti, kterou nelze odvrátit běžnou činností Národního centra kybernetické bezpečnosti).[125]

---

118 Tamtéž, str. 14 [cit. 07.02.2013].

119 Tamtéž, str. 15 [cit. 07.02.2013].

120 *Národní centrum kybernetické bezpečnosti.* Materiál prezentovaný na veletrhu pracovních příležitostí Job Challenge 2012, konaném v Brně dne 7.11.2012 [cit. 07.02.2013]. 2 str.

121 *Věcný záměr zákona o kybernetické bezpečnosti [online].* op. cit. sub 115, str. 47 [cit. 13.02.2013].

122 Právo na informační sebeurčení znamená mj. oprávnění osoby svobodně rozhodovat o tom, jaké informace o sobě bude šířit a komu, za jakých podmínek a k jakému účelu je dovolí zpracovávat.

123 *Věcný záměr zákona o kybernetické bezpečnosti [online].* op. cit. sub 115, str. 50 [cit. 13.02.2013].

124 Jde o angl. zkratky *Cyberspace Emergency Response Team/Cyberspace Security Incident Response Team*. Národním CERT/CSIRT přitom má být každé soukromé pracoviště, které na základě veřejnoprávní smlouvy s NBÚ zajišťuje a zprostředkovává sdílení informací v národním i mezinárodním kontextu. Vládní CSIRT je pak plánován jako součást Národního centra kybernetické bezpečnosti. Srov. op. cit. sub 115, str. 56 [cit. 15.02.2013].

125 Pro kompletní přehled definic srov. op. cit. sub 115, str. 55-57 [cit. 15.02.2013].

Navržený předpis předpokládá spolupráci orgánů veřejné správy a soukromých osob.[126] Zákon se má vztahovat mj. na definiční autority, správce informačních a komunikačních systémů v rámci kritické infrastruktury a správce informačních systémů veřejné správy. Charakter konkrétní entity (veřejnoprávní/soukromoprávní) bude určen podle typu infrastruktury, kterou bude daný subjekt spravovat a podle toho budou stanoveny i jejich povinnosti (ohlašovací povinnost, povinnost provádět protiopatření uložená NBÚ, předávání informací).[127]

V oblasti osobních údajů není předpokládáno pravidelné shromažďování a zpracovávání těchto údajů u fyzických osob; NBÚ bude monitorovat pouze sítě a systémy, v nichž došlo k bezpečnostním incidentům. Jinak se podpůrně uplatní zvláštní předpisy (pravděpodobně tedy mj. ZOOÚ).[128]

Věcný záměr počítá s předpokládaným zákonem o kybernetické bezpečnosti jako o *lex specialis* k zákonu o utajovaných informacích[129], když nejzávažnější informace týkající se kyberbezpečnosti ČR budou chráněny právě podle tohoto zákona.[130]

V případě vzniku škody v důsledku vyhlášení stavu kybernetického nebezpečí je výslovně předvídána odpovědnost státu podle zákona o odpovědnosti státu za škodu.[131] [132]

126 op. cit. sub 115, str. 21-22 [cit. 15.02.2013].

127 Tamtéž, str. 48-49, 57-61 [cit. 15.02.2013].

128 Tamtéž, str. 68 [cit. 15.02.2013].

129 Tamtéž, str. 47 [cit. 15.02.2013].

130 Pro méně závažné informace o kybernetických incidentech navrhuje Věcný záměr institut mlčenlivosti, což se minimálně na první pohled jeví jako nedostatečné. Srov. op. cit. sub 115, str. 68 [cit. 15.02.2013].

131 Zákon č. 82/1998 Sb., o odpovědnosti státu za škodu způsobenou při výkonu veřejné moci nezákonným rozhodnutím nebo nesprávným úředním postupem a o změně Zákona ČNR č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád), ve znění pozdějších předpisů.

132 op. cit. sub 115, str. 75 [cit. 15.02.2013].

3. AKTUÁLNÍ PROBLÉMY KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY

3.1. Narušení kybernetické bezpečnosti: Rozsah a dosah jurisdikce orgánů České republiky

Jurisdikce

Mezinárodní pravomoc a rozhodné právo. Zásadní problematika jurisdikce v sobě zahrnuje tři podstatné právní otázky: mezinárodní pravomoc, resp. mezinárodní příslušnost (tj. soudy nebo správní orgány které země budou spor rozhodovat), rozhodné hmotné právo (otázka, podle jakého právního řádu, se bude spor, resp. jeho dílčí otázky řídit) a konečně vykonatelnost, resp. vymahatelnost rozhodnutí soudu v jiné zemi. V centru naší pozornosti přitom stojí jednak delikty správní (přestupky, jiné správní delikty), jednak delikty trestní. V obou případech se jedná o jednání *contra legem* veřejnoprávní (resp. zasahující z pohledu českého, potažmo evropského právního řádu veřejný zájem do té míry, že otázka postihu není ponechána na vůli event. dotčených osob, ale řeší ji státní orgány *ex offo*).[133]

Rozsahem, event. dosahem jurisdikce přitom máme na mysli působnost právních norem České republiky a oprávnění příslušných orgánů z hlediska osobního, časového, věcného, event. (instančního). Než se budeme věnovat klíčovým kategoriím osobní a věcné působnosti, je vhodné alespoň stručně uvést, že z hlediska časového se z hlediska demokratického právního státu předpokládá zákaz pravé retroaktivity s tím, že protiprávnost jednání se posuzuje podle zákona účinného v době spáchání (ukončení páchání) činu; podle pozdějšího pak jen tehdy, je-li to pro pachatele příznivější (*reformatio in bonam partem*). Z hlediska instančního je provedeno vymezení vždy v konkrétním předpise: správní delikty bude dle navrhované úpravy projednávat NBÚ, proti jehož rozhodnutím budou přípustné opravné prostředky ve smyslu soudního řádu správního. Z hlediska osobního patrně nutno uplatnit *per analogiam* zásady trestního práva hmotného, jak je v §§4 a násl. vypočítává Trestní zákoník, tj. zejména zásadu aktivní a pasivní personality, zásadu teritoriality, univerzality a subsidiarity.

Aktivní personalita zakotvuje možnost trestního (analogicky správního) postihu pro fyzické osoby (analogicky, event. dle zákona o trestní odpovědnosti právnických osob též právnické osoby) s občanstvím, trvalým pobytem (event. sídlem) na českém území.

Pasivní personalita dovozuje aplikovatelnost českých předpisů na osobu, která se dopustí příslušného protiprávního jednání proti osobě, věci nebo jinému statku právem chráněného, pokud tato osoba odpovídá kritériím aktivní personality (občanství, trvalý pobyt, sídlo), resp. pokud statek je součástí infrastruktury obhospodařované státem nebo osobou splňující kritéria aktivní personality. Zvláště v případech, že bude aplikovatelnost českých předpisů založena

133 Lessig jde ještě dále a v otázce jurisdikce hovoří o současném bytí jedince ve dvou paralelních realitách (objektivní a virtuální), z čehož plyne též střet dvou vynutitelných systémů norem (právních a norem kyberprostoru, ať již zvykových, podmínek užívání jednotlivých služeb, hranic možného stanovených samotným kódem apod.); přitom k řešení jejich konfliktu může mít rozhodující orgán různý vztah. Z pohledu strukturního přístupu k právu (a k normám obecně) se mi objektivní právo účinné „offline“ v zemi přístupu do kyberprostoru jeví jako *lex generalis* a *lex prior* – a to proto, že reguluje podmínky již samotného přístupu do kyberprostoru (např. regulací trhu se službami ISP, právem ochrany osobních údajů, spotřebitelským právem apod.). Normy v kyberprostoru, resp. ty z nich, které budou sankcionovány státem (ať ve formě normativního či individuálního právního aktu) pak tvoří *lex posterior*, resp. *lex specialis*. Srov. LESSIG, op. cit. sub 2, str. 298.

z titulu pasivní personality, není vyloučeno, že půjde o protiprávní jednání, jež nemělo osoby a statky na českém území za *ab initio* předvídaný cíl. Pak je pravděpodobné, že bude založena jurisdikce více států; zvláště v případě třetích zemí (zemí mimo EU) by bylo vhodné zvážit zákonnou nebo mezinárodněprávní smluvní úpravu uznávání rozhodnutí cizích orgánů, jde-li o tentýž protiprávní akt.

Zásada teritoriality znamená možnost postihu činů, které se buď udály, popř. jejichž škodlivé účinky nastaly na území České republiky. Je pravděpodobně namístě využít pro podřazení činů teritoriální svrchovanosti České republiky aktuálních poznatků nauky mezinárodního práva soukromého a hraničních určovatelů *lex loci delicti commissi* a *lex loci damni infecti*.[134]

Lex loci delicti commissi se vztahuje na území celé České republiky, včetně plavidel a letadel pod vlajkou České republiky, exteritoriálních prostor českých zastupitelských úřadů apod.[135] Vzhledem k problematice kybernetické bezpečnosti jako ochrany vitálních zájmů státu je však nutno klást důraz na *lex loci damni infecti*, který je možno zobecnit jako každý prvek (nejen kritické) infrastruktury, na němž jsou uložena data vitální pro zájmy státu. Již přítomnost takových dat, která z hlediska ústavně konformního zákona nebo mezinárodní smlouvy jsou podřízena některému ze stupňů utajení nebo které jsou vyňaty ze zákona o svobodném přístupu k informacím z důvodu ochrany soukromí nebo ochrany jiného veřejného zájmu (veřejný pořádek, veřejná bezpečnost apod.) zakládají mezinárodní jurisdikci českých orgánů – výlučnou nebo paralelní s jinými státy. Deliktu podle českého práva se nicméně dopustí i ten, kdo k takto vymezenému *loco delicti* alespoň z nedbalosti neoprávněně přistoupí (resp. naplní alespoň stádium pokusu tohoto přístupu), *a minori ad maius* pokud přitom překoná legálně či nelegálně drženými nástroji (typicky softwarovými) zabezpečení infrastruktury nebo dat. O naplnění kritérií mezinárodní jurisdikce je dále možné uvažovat i tehdy, pokud osoba jinak nespojená s Českou republikou využije falešné identity získané na základě digitálního certifikátu nebo jiného způsobu prokázání identity vydaného českou autoritou. Zde by však patrně převážila jurisdikce toho státu, jehož infrastrukturu takto identifikovaný útočník napadl nebo k níž přistoupil, a to podle zásady nejužšího spojení (*closest connection*), používané rovněž v mezinárodním právu soukromém.

Zásada univerzality vyjadřuje povinnost státu podle pravidel mezinárodního *iuris cogentis* stíhat určité nejzávažnější trestné činy bez ohledu na místo jejich spáchání a charakteristiky jejího pachatele. Pro účely této práce má zvláštní význam stíhání teroristických činů, k nimž dochází jak online, tak i v reálném světě.

Zásada subsidiarity je pak zásadou vlastní především trestnímu právu (soudnímu). Plným názvem subsidiarita trestní represe vyjadřuje skutečnost, že k sankcím trestního práva má být saháno jen tehdy, neexistuje-li mírnější prostředek postihu, v tomto případě cestou správního práva (procesního, trestního).

V právu veřejném, jak ho chápe kontinentální právní kultura, zároveň takřka automaticky platí, že mezinárodní pravomoc určitého státu znamená zároveň i aplikovatelnost jeho hmotného

134 V daném případě se jedná o argumentaci podobným (*argumentum a simili*), nikoli o analogii.

135 V případě poskytnutí diplomatické ochrany podle práva Evropské unie jiným členským státem by pravděpodobně i tak došlo na základě *legis loci damni infecti* k založení jurisdikce českých orgánů, i když *lex loci delicti commissi* by zakládal mezinárodní pravomoc státu zastupitelského úřadu.

práva.[136] Procesní postup orgánů veřejné moci se pak zásadně řídí principem *legis fori*, tj. procesním právem rozhodným je vždy právo státu, jehož orgán rozhoduje.

Souběh jurisdikce. V praxi může dojít k případům, kdy mezinárodní jurisdikci uplatňuje více států. V případě, že není možné řešit pozitivní konflikt pravomoci diplomatickou cestou, popř. vhodným výkladem práva (vč. možnosti položení předběžné otázky Soudnímu dvoru EU v případě dvou nebo více členských států), pak je namístě vzít v úvahu několik kritérií. Jedná se konkrétně o preferenci *legis loci damni infecti* před *lege loci delicti commissi*, neboť minimálně dokonané protiprávní jednání je stíháno především pro způsobené ohrožení nebo škodu; jednání ve stádiu pokusu je z tohoto pohledu problematičtější, avšak v zájmu jednoty pravidel se rovněž přikláním k preferenci jurisdikce podle místa cíle útoku (je-li z nedokonaného jednání zřejmý). V případě více států splňujících kritérium místa vzniku škody lze uvažovat buď o soustředění řízení do státu, v němž vznikla škoda podstatně přesahující škody v ostatních státech (s tím, že tyto ostatní státy by měly coby poškození postavení intervenienta-vedlejšího účastníka), popř. je možno využít mezinárodní pravomoci podle *legis domicilii* (a to vždy, pokud je jedním z dotčených států stát trvalého pobytu, resp. domicilu podezřelého). Pokud nebude použitelné ani jedno z těchto pravidel, nabízí se podpůrně doktrína překážky věci projednávané (*litis pendentis*), tj. mezinárodní pravomoc by měl ten stát, jenž by zahájil trestní řízení jako první.

Uznání a výkon rozsudků. Výkon cizích správních a trestních (soudních) aktů je podle českého práva přípustný pouze na základě zvláštního ustanovení zákona[137] nebo mezinárodní smlouvy. Kontinentální právní kultura obecně při respektování aktů cizí státní moci (ale i např. v otázkách extradice podezřelých či právní pomoci) vychází kromě mezinárodní smluvní, potažmo zákonné úpravy též z faktické nebo presumované reciprocity ze strany požadujícího státu.

U extradice v zásadě platí, že Česká republika nevydává své státní příslušníky (popř. osoby, jimž byl udělen azyl) k trestnímu stíhání do jiného státu, a to s výjimkou evropského zatýkacího rozkazu, kdy ale musí být mj. splněna podmínka oboustranné trestnosti (tj. čin, pro který je extradice žádána, musí být trestný jak v ČR, tak i ve státu vyžadujícím vydání domnělého pachatele).[138] Vyloučeno je vydání osob, které podle českého práva nejsou trestně odpovědné (tj. osob mladších 15 let), vydání do států, kde by osobě hrozil trest smrti, mučení nebo jiné nehumánní zacházení (zásada *non-refoulement*) a vydání výlučně pro činy označené ve vyžadujícím státě jako trestné, pokud jsou politické povahy, resp. vydání pro uplatňování základních práv a svobod.

V ustanovení §377 trestního řádu je obsažena výhrada veřejného pořádku, která umožňuje odmítnutí žádosti cizího státu o právní pomoc nebo ve věcech extradice, jestliže by se takové

---

136 Závažnější a i v praxi veřejnoprávní alespoň občas se objevující nesnází může být kvalifikační problém v podobě nutnosti vyjasnit právní otázku, pro niž neexistuje z důvodů politických, kulturních aj. v domácím právu ekvivalent. Pro řešení kvalifikačního problému *per argumentum a simili* srov. KUČERA, Z. *Mezinárodní právo soukromé.* 7. opr. a dopl. vyd. Brno: Doplněk, 2009. ISBN 9788072392315 (Doplněk Brno), 9788073801717 (Aleš Čeněk Plzeň), str. 141 a násl.

137 Srov. např. §450 trestního řádu.

138 Srov. §10/2 trestního zákoníku a §§403-422 trestního řádu.

rozhodnutí příčilo Ústavě České republiky nebo jejímu právnímu řádu, popř. jestliže by takovým postupem byl dotčen jiný významný chráněný zájem České republiky. Příkladem mohou být i výše uvedené právní záruky lidských práv vč. spravedlivého procesu a ochrana svých občanů.

Denegatio iustitiae a jurisdikce. Obecným principem jakéhokoli soudního řízení, resp. spravedlivého procesu je zákaz odepření spravedlnosti (lat. *denegatio iustitiae,* angl. *denial of justice*). V úzkém smyslu lze odepření spravedlnosti definovat tak, že soud (rozhodující orgán) odmítne jakkoli – kladně nebo záporně – posoudit otázku, kterou mu strany předložily bez ohledu na důvody, které k tomuto stavu vedly. Širší pojetí, s výslovným důrazem na spory s mezinárodním prvkem, zastává Paulsson, když *denegatio iustitiae* vymezuje jako zásadní porušení spravedlivého procesu (*fundamental procedural fairness*) s nutností *ad hoc* posuzování splnění určitých minimálních procesních záruk vč. přístupu k opravným prostředkům, od nichž lze rozumně očekávat meritorní posouzení a nápravu vytýkaných pochybení.[139] Odepření spravedlnosti je tak v naprosté většině případů procesní povahy, byť není vyloučeno ani v podobě hmotněprávní coby extrémně zmatečné, z hlediska skutkových závěrů a právní kvalifikace a subsumpce vadné rozhodnutí.[140]

V moderním mezinárodním právu nejsou jako faktory zakládající dovolání se odepření spravedlnosti před mezinárodními institucemi např. odepření *přístupu* ke spravedlnosti (tj. vůbec k orgánům pro řešení sporů), cílenou národní legislativu, uplatnění imunity jednoho státu před soudy státu druhého, přímý zásah vlády státu, podnícení nepřiměřeného tlaku veřejného mínění. Zde se jedná o *denegatio* způsobené vnějším zásahem do procesu (rozuměj vnějším z pohledu soudní moci). Na úrovni soudu, resp. rozhodujícího orgánu pak lze za odepření spravedlnosti dle Paulssona považovat např. nepřiměřené průtahy, zjevnou svévoli při rozhodování, nedostatek znalostí o problematice, ale i legislativu s atributem pravé retroaktivity.[141]

V mezinárodním styku může dojít i k situaci, kdy vznikne negativní spor o pravomoc, tj. kdy více soudů odepře zabývat se meritorní otázkou z důvodu tvrzeného nedostatku mezinárodní pravomoci. Na rozdíl od čistě vnitrostátních řízení zde není vždy soud, který by tento negativní spor o pravomoc mohl rozhodnout.[142] Je proto otázka, zda by za určitých podmínek neměla mít kterákoli strana možnost obrátit se na některý ze soudů států, které by se mezinárodní dohodou nebo podle svého vlastního vnitrostátního práva zavázaly, že rozsoudí spor o právo těch stran,

---

139 PAULSSON, J. *Denial of Justice in International Law.* 1st paperback ed. Cambridge: Cambridge University Press, 2010, ISBN 9780521172912. str. 130.

140 Srov. tamtéž, str. 98.

141 Tamtéž. Podrobný výklad srov. část 6. a 7. publikace.

142 V případě určení mezinárodní pravomoci v rámci EU by pravděpodobně rozhodoval SDEU na základě předběžné otázky položené národním soudem členského státu. K nejednoznačnému oprávnění, resp. problematickému postavení Mezinárodního soudního dvora v rozhodování sporů mezi státy srov. GOLDSMITH, J., POSNER, E. A. *The New International Law Scholarship [online].* Chicago: The Law School of the University of Chicago. Public Law and Legal Theory Working Paper No. 126, May 2006. 27 str. K dispozici na www: http://ssrn.com/abstract_id=901991

jimž byla odmítnuta spravedlnost soudy, k nimž měl spor rozumný vztah.[143] Jde samozřejmě o prostředek *ultimae rationis.*[144]

Související problémy

Tato podkapitola má za cíl stručně popsat a právními nástroji mezinárodního práva soukromého a trestního navrhnout *de lege ferenda* mechanismy řešení žádoucích, či nežádoucích, leč každopádně dosud obtížně právně uchopitelných jevů. Konkrétně jde o kyberterorismus, a odpovědnost poskytovatelů služeb informační společnosti (ISP, *Information Service Providers*) v mezinárodním měřítku.

Kyberterorismus.[145] Terorismus obecně je možné definovat jako „použití násilí a hrozeb za účelem zastrašení nebo donucení, zvláště pro politické účely."[146] a ve větším měřítku jsme svědky jeho projevů teprve přibližně od druhé poloviny 20. století, a to díky rozšiřujícím se možnostem dopravy a komunikace mezi státy a celými kontinenty, což způsobuje větší pravděpodobnost konfliktu zájmů mezi politickými, hospodářskými, náboženskými a jinými mocnostmi nebo skupinami. Svoji roli nepochybně hraje též povážlivě přetrvávající chudoba značné části obyvatel planety[147] a překážky přístupu ke vzdělání, které vždy vytvářely podmínky pro černobílé vidění světa, extremismus a radikální prostředky boje proti skutečnému, ale častěji domnělému „nepříteli".

Kyberterorismus je ve své podstatě virtualizovaným terorismem; neliší se od něj svými cíli, znaky (nejistota ohledně osoby útočníka, neudržitelnost až následného postihu, ale potřeba preventivních opatření[148]), ale způsobem provedení, k němuž využívá přímo[149] prostředí

143 Bylo by otázkou politické shody vyjmenovat taxativní případy, kdy je toto kritérium splněno; event. k dobru stran subsidiárně stanovit obecnou klauzuli nebo princip *in dubio pro iuris dictione.*

144 Konečně by v takovém případě mohlo najít využití ust. §9/5 OSŘ stanovící věcnou příslušnost Nejvyššího soudu v prvním stupni.

145 Tato podkapitola byla zpracována s využitím textu TRACHTMAN, J.P. *Global Cyberterrorism, Jurisdiction and International Organization [online].* Tufts University – The Fletcher School of Law and Diplomacy, 2004. 36 str. K dispozici na www: http://ssrn.com/abstract=56636

146 Tato i další definice viz ROUSE, M., ROSSETTI, L. *Terrorism | Define Terrorism at Dictionary.com [online].* K dispozici na www: http://dictionary.reference.com/browse/terrorism Poslední aktualizace: 2013 [cit. 28.02.2013].

147 Pro představu: průměrný občan ČR pobírající průměrnou mzdu, mající menší úspory a bydlící v nájemním bytě, který je schopen uspokojit své každodenní základní potřeby (potrava, voda, teplo, elektřina, doprava) patří mezi cca 10% nejbohatších obyvatel planety.

148 TRACHTMAN, op. cit. sub 145, str. 4.

149 Máme na mysli činy, které jsou z podstatné části provedeny s použitím ICT technologií; nikoli ty, jejichž příprava je pouze s využitím ICT služeb a funkcionalit koordinována (typicky přes e-mailovou komunikaci nebo sociální sítě jako např. Facebook nebo Twitter) nebo ty, jejichž jediným spojením s prostředím ICT je uskutečňování finančních operací online s cílem získat prostředky pro teroristickou činnost.

informačních sítí. Jak kyberprostor, tak i terorismus se vyvinuly ze státem podporovaného fenoménu v jev nikoli zcela, ale přesto výrazně decentralizovaný.[150]

Terorismus často doprovází jiná, „méně závažná“ trestná činnost (vydírání, rozsáhlé krádeže dat nebo zboží a služeb, praní špinavých peněz apod.)[151] Ochrana před kyberterorismem a obecně před kybernetickou kriminalitou je přitom veřejným statkem a veřejným dobrem.[152]

Řešení kybernetického terorismu v jeho možných podobách naznačuje Trachtman čtyři: omezení přístupu k zabezpečeným sítím (mj. biometrickými technikami), popř. filtrování obsahu, preventivní sledování a detekci obsahu dat v kyberprostoru, identifikaci útočníka a vhodnou odpověď vč. odpovědi právní, popř. zavádění robustnějších sítí.[153] Soukromý sektor ve svém úsilí o ochranu před kybernetickým terorismem není omezen hranicemi států ani limity mezinárodní spolupráce. Zatímco poskytovatelé připojení k internetu (jedna z kategorií ISP, viz níže) právě tak jako podnikatelé mají vhodnou motivaci k trvalému udržování vysokého standardu bezpečnosti (v obou případech se jedná o komerční, byť kvalitativně odlišné důvody)[154], uživatelé – spotřebitelé většinou sledují „jen“ zájem ochrany svých soukromých dat, a to zdaleka ne vždy. Přesto „díra“ v zabezpečení na kterékoli úrovni může mít v případě teroristického útoku v kyberprostoru fatální následky.[155]

Odpovědnost poskytovatelů služeb informační společnosti.[156] Pod množinu „poskytovatelů služeb informační společnosti (dále jen „ISP“) můžeme podřadit zejména poskytovatele internetového připojení[157], provozovatele internetových stránek vč. sociálních sítí a sítí *peer-to-peer* (sdílení obsahu mezi uživateli), resp. poskytovatele dat v digitální podobě na dálku a/nebo na vyžádání, provozovatele platebních systémů[158] apod. Neřadíme sem tedy především soukromé uživatele, ať fyzické nebo právnické osoby.

---

150 TRACHTMAN, op. cit. sub 145, str. 1, 11.

151 Tamtéž, str. 3.

152 Tamtéž, str. 12.

153 Tamtéž, str. 6-9.

154 Tamtéž, str. 12.

155 Je otázkou, kde vést hranici mezi kybernetickým terorismem a kybernetickou kriminalitou. Jako dvě kritéria se nabízí počet osob zasažených konkrétním činem a míra jejich účasti ve správě věcí veřejných. Spolu s kritériem snahy donutit k určitému jednání by této definici vyhovovaly i hackerské útoky skupiny *Anonymous* z roku 2011. Je na druhé straně otázka, zdali např. „pouhé“ napadení (veřejně přístupného) webu vlády a umístění vlastního textu je možné považovat za terorismus; zde už se totiž blížíme k hranicím občanské angažovanosti, resp. občanské neposlušnosti, která je – byť za podmínky ochromení ústavních institucí – chráněna i podle čl. 23 Ústavy ČR.

156 Tato podkapitola byla zpracována s využitím textu LICHTMAN, D., POSNER, E. A. *Holding Internet Service Providers Accountable.* In: GRADY, M. F., PARISI, F. (eds.). *The Law and Economics of Cybersecurity* 1st ed. New York: Cambridge University Press, 2006, ISBN 0521855276. str. 221-258.

157 Pro označení poskytovatelů internetového připojení se anglická zkratka ISP používá také, a to v podobě *Internet Service Providers.*

158 Nemusí se týkat jen systémů elektronických peněz, ale i nakládání s virtuálními směnnými jednotkami, např. pro účely některých online počítačových her.

Právní odpovědnost těchto subjektů může být buď přímá (za vlastní nebo jim přičitatelné protiprávní jednání v jejich zájmu), což je pravidelný případ, nebo také nepřímá – obdobná např. odpovědnosti zaměstnavatele za škodu způsobenou třetí osobě zaměstnancem nebo provozovatele vozidla za škodu způsobenou tím, kdo jeho vozidlo s jeho vědomím užíval. Zákonná nepřímá odpovědnost zvláště v zaměstnaneckých, potažmo třeba i spotřebitelských vztazích vyvažuje odlišnou vyjednávací sílu smluvních stran a směřuje k ochraně slabší strany, tj. zaměstnance nebo spotřebitele.[159]

Důvody užití institutu nepřímé odpovědnosti jsou jednak často více či méně obtížný dosah objektivního práva a jeho sankčních mechanismů na škůdce (vč. někdy omezených možností škůdce uhradit škodu v plné výši), jednak prakticky neprůchodné smluvní mechanismy (právě ve vztazích s nerovnou vyjednávací silou) o rozdělení povinnosti, popř. limitace výše nahrazované škody smluvními stranami. Dalším důvodem je pak zákonitý vznik negativních externalit při činnosti osoby nebo entity, jíž vzniká sekundární závazek z nepřímé odpovědnosti nebo potenciál ISP mít v každé chvíli alespoň v omezeném rozsahu kontrolu nad všemi informacemi, které přes jejich zařízení nebo software prochází.[160]

V případě zmíněných externalit u ISP jde především o nežádoucí důsledky provozování jejich služeb, ať již připojení nezabezpečeného nebo dokonce vědomě závadný obsah rozšiřujícího uživatele, pomluvy a neověřené informace, vkládané uživateli na různé weby, zvláště diskusní fóra a sociální sítě, podvodné platby na internetu apod. Tím dochází i k přizpůsobení ceny služeb těmto rizikům; cena pak více odpovídá všem pozitivním i negativním důsledkům poskytnutí služby.[161]

Případné námitky o přecitlivělosti ISP na potenciální rizika představovaná uživateli a omezení motivace uživatelů k vlastní snaze o zabezpečení Lichtman a Posner odmítají s poukazem na ekonomickou teorii mezního užitku[162] a na možnost strukturovat ceny ISP za služby i podle toho, do jaké míry přistupující uživatel udržuje své zařízení v bezpečí.[163]

Jak nicméně Lichtman s Posnerem správně poznamenávají, nepřímá odpovědnost ISP je v příkrém kontrastu s nejednotnou regulací ochrany kybernetické bezpečnosti ve světě. Nehledě na skutečnost, že nepřímá odpovědnost může při jediném a témž útoku vzniknout u více než jednoho ISP (pak si lze jen těžko představit odpovědnost společnou a nerozdílnou, která by pravděpodobně byla finančně neúnosná a následný postih značně obtížně vymahatelný), pak

159 srov. LICHTMAN, D. POSNER, E. A. *Holding Internet Service Providers Accountable.* In: GRADY, M. F., PARISI, F. (eds.), op. cit. sub 156, str. 227 a násl.

160 Nemám samozřejmě na mysli, že i giganti jako je Google, Facebook nebo různé bankovní domy jsou schopni v každé vteřině filtrovat 100% dat nebo mají povinnost je znát. Takový výklad by bylo nutno odmítnout *per argumentum ad absurdum.*

161 Pro podrobnější výklad posledních dvou odstavců srov. LICHTMAN, D. POSNER, E. A., op. cit. sub 156, str. 232-239.

162 Teorie mezního užitku spočívá, zjednodušeně řečeno, v nutnosti zkoumat, zda při zvýšení produkce, poskytnutí nebo spotřeby statku o jednotkové množství převáží přínosy (zisk, efektivnější využití výrobních kapacit, uspokojení) nebo náklady producenta/poskytovatele/spotřebitele. Kolegům ekonomům se za fušování do řemesla omlouvám.

163 Srov. LICHTMAN, D. POSNER, E. A., op. cit. sub 156, str. 239-244.

vzniká otázka, zda ISP ve státech s volnější regulací, event. zcela zproštěni deliktní odpovědnosti nejsou neadekvátně zvýhodněni.[164] Na to lze odpovědět pouze zavedením subjektivní odpovědnosti ISP – byť i s důkazním břemenem na straně delikventa – neboť nepřímá odpovědnost jako objektivní nebo dokonce absolutní (tj. bez možnosti zproštění) skutečně není přiměřená aktuálním možnostem ISP. ISP by v takovém případě musel prokázat, že provedl všechna rozumná a ekonomicky efektivní opatření, jaká na něm lze spravedlivě požadovat; nelze samozřejmě vyloučit ani případ, kdy část škody ponese poškozený sám, pokud k jejímu vzniku zaviněným jednáním přispěl.

3.2. Mezinárodní kybernetický konflikt

Úvod. Mezinárodní kybernetický konflikt je speciálním případem ozbrojeného válečného konfliktu. Je tomu tak proto, že se jako i u klasických „offline" válečných konfliktů jedná o použití síly – ať již v rámci sebeobrany anebo v rozporu s normami mezinárodního práva jako akt agrese – přes hranice národního kyberprostoru[165] (resp. přes hranice suverénně spravovaných území). Od jiných mezinárodních konfliktů se konflikt kybernetický neliší zcela svými subjekty, svým účelem ani cíli útoku a ani prostředky případného urovnání, avšak liší se podstatným způsobem co do použitých zbraní. Použití síly vůči kyberprostoru státního suveréna přitom může být agresí, která vyvolá akt sebeobrany v „offline" světě, anebo naopak, může se jednat o sebeobranu proti útoku vedenému mimo kyberprostor.

Kybernetický konflikt probíhá mezi státy nebo dalšími zvláštními subjekty mezinárodního práva[166] a subjekty kyberprostoru[167], v zásadě s výjimkou jednotlivců.[168] Cílem útoku jsou statky (budovy, věci, infrastruktura) více či méně nezbytné pro hospodářskou stabilitu, bojeschopnost a kontrolu dosavadního území napadeného státu. Účelem útoku je získání převahy nad napadeným státem v určité oblasti (hospodářské, technické, vojenské, územní, informační) a dočasné nebo trvalé udržení této převahy.

Útok v daném případě není veden (buď vůbec, anebo výlučně) klasickými prostředky ozbrojeného boje (pozemními, námořními, leteckými jednotkami), ale pomocí řízeného toku informací s cílem kompromitovat (narušit) kritickou infrastrukturu a citlivá data státu. Na tento

---

164 Tamtéž, str. 244-247.

165 Národní kyberprostor je možné definovat jako část kyberprostoru pod jurisdikcí konkrétního státu, event. jiného subjektu mezinárodního práva. Srov. kap. 2.4.

166 Nejčastějším zúčastněným subjektem odlišným od státu bude zřejmě povstalecké hnutí, event. přechodná vláda. Srov. DAVID, V., BUREŠ, P., FAIX, M. et al. *Mezinárodní právo veřejné s kazuistikou.* 2. akt. a přeprac. vyd. Praha: Leges, 2011, ISBN 9788087212868, str. 132 a násl.

167 V daném případě máme na mysli typicky poskytovatele služeb informační společnosti (ISP), resp. definiční autority (k nim viz pozn. sub 4).

168 Vyloučení jednotlivců z dosahu kybernetického konfliktu není absolutní: v duchu „nejlepších" tradic studené války si lze představit např. cílený státem podporovaný nebo trpěný kybernetický útok proti představiteli jiného státu. Obecně je však útok jednotlivce nebo soukromé entity proti kritické infrastruktuře státu nebo jeho utajeným datům spíše otázkou mezinárodního práva trestního, nikoli vztahů mezi státy.

specifický prvek – provedení útoku – pak navazují některá specifika další: jednak jde o ne zcela předvídatelný řetězec možných důsledků takového útoku (např. při dalším lavinovitém šíření škodlivého kódu), jednak nutnost prokazování původce útoku – o kybernetický konflikt mezi státy se totiž jedná pouze tehdy, je-li útok nějakým způsobem úmyslně státem iniciován a podporován. V opačném případě půjde „jen" o odpovědnostní delikt proti mezinárodnímu právu (více srov. níže v této kapitole).

Je-li stát shledán původcem kybernetického útoku, tj. vlastně agresorem, dopouští se jednání proti kogentním normám mezinárodního práva (*peremptory norms, ius cogens*), resp. mezinárodního zločinu[169], neboť porušuje základní zásadu mezinárodního společenství, totiž zákaz ozbrojeného útoku, resp. zákaz použití síly.

Z právního hlediska každopádně připadá v úvahu aplikace (buď *per analogiam* nebo *per argumentum a simili*) válečného a humanitárního práva ve všech jeho podobách (*ius cogens*, mezinárodní úmluvy, obyčeje apod.). Nejvýznamnějšími smluvními prameny budou z povahy věci ustanovení čtvrté Ženevské úmluvy o ochraně civilistů a první Ženevské úmluvy, zabývající se raněnými. Ustanovení těchto úmluv nutí státy promýšlet předvídatelné následky svých ozbrojených akcí v kyberprostoru, které často nastanou bez fyzického střetu a setkání s bojovníky a civilisty druhého státu. Status kombatanta (příslušníka ozbrojených sil) podle ženevského práva pak lze *a simili et e ratione legis* přiznat především osobám, jejichž zodpovědností je kybernetická bezpečnost daného státu.

Takový konflikt je možné urovnat, ať již v zárodku nebo při plné realizaci válečných operací, diplomatickou cestou (např. setkání na neutrální půdě často doprovázené zprostředkováním kontaktu znepřátelených stran prostřednictvím významných státníků), za použití smírčího řízení nebo arbitráže[170] nebo posléze cestou smluvní (mírové smlouvy stanovící zároveň omezující podmínky *dare, facere, ommittere, pati*[171] poražené straně).

Mezinárodní odpovědnost státu za kybernetický útok z jeho území

Problematika mezinárodní odpovědnosti je aktuální již od vzniku prvních státních útvarů. Její charakter se někdy dovozuje jako analogie deliktní odpovědnosti vnitrostátní. Problematičnost této koncepce spočívá ve dvou odlišných *modis operandi* mezinárodní odpovědnosti: *inter partes* (při porušení dispozitivních norem mezinárodního práva; je z větší části relevantní pro naši analýzu) nebo *erga omnes* (mezinárodní zločiny, porušení norem kogentních), která je aktuální nejpozději od skončení 2. světové války.[172] Jiná teorie předpokládá suverénní státy jako nositele

169 Mezinárodní zločin jako závažné protiprávní jednání státu je oproti porušení kogentních norem užším pojmem. srov. DAVID, V., BUREŠ, P., FAIX, M. op. cit. sub 166, str. 343.

170 Podrobnější výklad o diplomatickém, smírčím a arbitrážním řešení konfliktů s ohledem na mezinárodněprávní odpovědnost státu srov. CRAWFORD, J., PELLET, A., OLLESON, S. (eds.) *The Law of International Responsibility. Oxford Commentaries on International Law.* 1st ed. New York: Oxford University Press, 2010. lxv, 1296 str. ISBN 9780199296972.

171 Což je důsledkem toho, že dějiny a podmínky mírových smluv píší vítězové.

172 KOSKENNIEMI, M. *Doctrines of State Responsibility*. In: CRAWFORD, J., PELLET, A., OLLESON, S. (eds.) op. cit. sub 170, str. 47 – 48.

subjektivních práv (v nejobecnějším slova smyslu odpovídajícím komplementární povinnosti ostatních států vyjádřenou imperativem *Neminem laedere*[173]). Koncepce *due diligence* ponechává stranou povahu odpovědnosti, avšak staví se k ní jako k odpovědnosti objektivní, postavené pouze na možnostech státu kontrolovat určité jednání osoby (*control*) a přičitatelnosti (*attributability*; též *blameworthiness*).[174] Odpovědnost státu je v tomto případě dovozována jako odpovědnost objektivní a nadto nepřímá: sankce vůči státu tedy nejsou založeny na tom, že stát sám prostřednictvím fyzických osob něco spáchal, ale že je mu určité jednání přičitatelné. Kromě přičitatelnosti je nutným předpokladem vzniku odpovědnosti též vznik škody, resp. újmy; tato újma může mít povahu jak materiální, tak nemateriální (a samozřejmě kauzální nexus mezi jednáním a vznikem škody).

Vznik škody je nutno posoudit zásadně podle práva místa, kde se projevil následek útoku. Přičitatelnost útoku je následně stanovena na základě tří kumulativních kritérií, totiž osoby (*ratione personae*), místa (*ratione loci*), času (r*atione temporis*) a cíle útoku (*ratione materiae*).

Pojem osoba vlastně není zcela přesný: v daném případě má totiž zahrnovat jednak organizační složky státu, jednak osoby fyzické a právnické s pravomocí a působností v oblasti veřejné správy, jednak i fyzické a právnické osoby bez tohoto mocenského atributu. Ve všech třech případech musí jít o jednání (buď komisivní – aktivní útok nebo omisivní – pochybení při zabezpečení, umožnění kybernetického útoku „přes" vlastní kyberprostor), které je vykonáváno buď v rámci svěřené pravomoci (u prvních dvou jmenovaných), s výslovnou nebo konkludentní podporou nebo schválením státu (u všech tří) nebo je vykonáno jménem státu. Výkon veřejné moci předpokládá úzkou vazbu ke státu formou občanství nebo sídla; u osob soukromého práva však není závazný občanský nebo obdobný poměr ke státu relevantní; rozhoduje pouze vztah státu k protiprávnímu jednání této osoby. Naproti tomu, státu není přičitatelné jednání ryze soukromého, potažmo komerčního charakteru, a to opět u všech tří vyjmenovaných kategorií osob.[175]

Přičitatelnost z pohledu místa útoku zahrnuje rozhodně případy spuštění útoku z území, potažmo z infrastruktury odpovědného státu. Pokud jde o útok, který započal ve třetí zemi a přes (potenciálně odpovědný) stát pouze „prochází", pak je patrně nutné se ptát, zda odpovědný stát učinil vše, co je po něm možno rozumně požadovat (zejména s ohledem na ekonomickou výkonnost státu, rozsah jeho sítě apod.), aby zneužití své infrastruktury zabránil.

Z pohledu *ratione temporis* je nutno zvážit dvě zásadní otázky. Zaprvé, zda povinnost, která měla být jednáním porušena, existovala v době tohoto jednání – ať již jako součást *iuris cogentis* (tam zpravidla ano), ve zvykové podobě, ve smlouvách, kterými je stát vázán. A zadruhé, zda v době

173 Jde o latinský originál právního principu „Nikomu neškodit".

174 op. cit. sub 172, str. 48.

175 Soukromý kybernetický útok na státní kybernetickou infrastrukturu a data je zpravidla trestným činem – buď v zemi, odkud je útok prováděn nebo v zemi, která je terčem útoku; popř. v obou těchto zemích. Z poslední doby srov. britský případ *McKinnon*, kde britský občan bez jakékoli vazby na stát zaútočil na infrastrukturu USA. V daném případě byla též klíčovou otázka extradice obviněného – britského občana do USA, která byla nakonec po několika letech řízení zamítnuta ze zdravotních důvodů.

jednání stát disponoval potřebnou mírou suverenity nad osobami a územími, ze kterých/kterými byl útok veden. Nesplnění alespoň jedné z těchto podmínek by znamenalo, že odpovědnost nevznikne, neboť buď není co přičítat (neexistuje povinnost) nebo není komu přičítat (není zde relevantní subjekt).

Aktuální koncepce mezinárodní odpovědnosti, jak ji zmiňuje Sternová, přichází také s pouhými dvěma podmínkami, jejichž naplnění znamená vznik mezinárodní odpovědnosti státu, a to přičitatelnost určitého jednání konkrétnímu státu a skutečnost, že toto jednání zakládá porušení mezinárodního práva. Zde tedy nehraje roli ani to, zda vůbec nějaká škoda vznikla.[176]

V každém případě by nemělo jít o odpovědnost absolutní. Stěžejní dokument aktuálních snah o kodifikaci práva mezinárodní odpovědnosti (*Articles on State Responsibility*), připravený Komisí pro mezinárodní právo OSN v roce 2001[177], předvídá několik právně relevantních skutečností, které jsou překážkou vzniku odpovědnosti. Jde jednak o předchozí svolení poškozeného státu (podle zásady *„Volenti non fit iniuria."*[178]), porušení povinnosti jen za účelem souladu jednání s *iure cogenti*, sebeobranu, odvetná opatření, vyšší moc (*force majeure*), tíseň a krajní nouze.[179] [180] Důvodem možnosti liberace je též fakt, že se objevují stále nové a nové kybernetické útoky, na něž při vší snaze není stát ani objektivně schopen reagovat (jinými slovy, bylo by po něm žádáno něco nemožného a *impossibile nulla est obligatio*). Svoji roli by zde ale měl sehrát též princip subsidiarity, tj. stát by neměl být činěn odpovědným, pokud zde existuje jasná cesta k pachateli, na němž je navíc ještě možno s úspěchem škodu vymoci.

Pokud jde o odpovědnost jiné entity než státu (např. povstaleckého nebo národně-osvobozeneckého hnutí), je dána a postavena na analogickém užití postavení suveréna (vykonávajícího veřejnou moc) na určitém území. Je každopádně více pravděpodobné, že bude dán některý důvod vylučující vznik odpovědnosti – zejména sebeobrana, plnění *iuris cogentis*, případy tísně nebo krajní nouze. Odpovědnost mezinárodních organizací je pak diskutována v návrhu Článků o odpovědnosti mezinárodních organizací (*Articles on Responsibility of*

---

176 STERN, B. *The Elements of an Internationally Wrongful Act.* In: CRAWFORD, J., PELLET, A., OLLESON, S. (eds.) op. cit. sub 170, str. 200.

177 text dokumentu v angličtině viz: CRAWFORD, J., PELLET, A., OLLESON, S. (eds.), op. cit. sub 170, str. 1229 a násl.

178 Latinský originál právní zásady „Tomu, kdo chce, se neděje bezpráví".

179 Srov. výklad in: CRAWFORD, J., PELLET, A., OLLESON, S. (eds.), op. cit. sub 170, Part III, Section 1 Subsection D, str. 427-501. V češtině pak DAVID, V., BUREŠ, P., FAIX, M. et al., op. cit. sub 166, str. 334-339.

180 Tíseň (*distress*) je stav, kdy osoba jednající jménem státu (nebo osoba, jejíž jednání se státu přičítá) jedná v rozporu s mezinárodním právem, aby odvrátila bezprostřední ohrožení života jí svěřených osob. Krajní nouze (*necessity*) je stav, kdy stát jedná protiprávně, aby zabránil potenciálnímu nebo aktuálnímu ohrožení svých vitálních zájmů (bezpečnost obyvatelstva. K rozdílům srov. SZUREK, S. *Circumstances Precluding Wrongfulness in the ILC Articles on State Responsibility: Distress.* In: CRAWFORD, J., PELLET, A., OLLESON, S. (eds.) op. cit. sub 170, p. 483. K problematičnosti krajní nouze v současném mezinárodním právu srov. DAVID, V., BUREŠ, P., FAIX, M. op. cit. sub 166, str. 337.

International Organizations), který byl v prvním čtení projednáván Komisí pro mezinárodní právo OSN v roce 2009.[181]

Možnosti řešení nastalé situace jsou obdobné jako u kybernetického konfliktu (viz první část této kapitoly výše). Jde tedy o řešení diplomatické, prostřednictvím smírčího nebo rozhodčího (arbitrážního) řízení, popř. cestou smluvní. Nedojde-li k urovnání žádným z těchto způsobů a zůstává-li existence, popř. rozsah odpovědnosti mezi stranami sporný, je nutno přikročit k postavení celého nároku najisto. To může na návrh poškozeného státu učinit buď mezinárodní orgán, ať již je stálý (např. Mezinárodní soudní dvůr, jiný orgán OSN, nově ustavený specializovaný orgán v oblasti ICT), anebo vytvořený *ad hoc*.

Obsahem mezinárodní odpovědnosti jako sekundárního, akcesorického právního vztahu, je pravidelně povinnost zdržet se dalšího protiprávního jednání, poskytnutí záruk, že nedojde k opakování tohoto jednání a odčinění vzniklé újmy. Toto odčinění má běžně podobu restituce (tj. uvedení v předešlý stav) nebo kompenzace (adekvátní náhrada, odčinění způsobené újmy); při dovoditelném (jakkoli jinak irelevantním) zavinění státu v podobě úmyslu nebo nedbalosti přichází v úvahu využití institutu zadostiučinění (*satisfaction*), které je svou podstatou sankcí[182], protože jeho poskytnutí není závislé na existenci újmy. Ne vždy však musí mít charakter poskytnutí statků; může jít i např. o vyslovení politování a omluvu, potrestání osob zodpovědných za protiprávní jednání, popř. oficiální konstatování protiprávnosti jednání, a to buď státem samým anebo mezinárodním soudním orgánem, který spor rozhoduje.[183] V praxi spíše těžko představitelný, ale teoreticky možný je i model, podle něhož státu odpovědnému za útok vzniká kromě shora uvedených povinností též povinnost uznat a vykonat, s výhradou veřejného pořádku, rozsudky státu (států) vzniku škody nebo v něm usazených osob, kterým vznikla škoda, proti útočníkům, jsou-li známi, a to alespoň v oblasti civilní, resp. všech sankcí, které postrádají charakter trestního práva (tj. retribuční spravedlnosti).

Pokud by kybernetickým útokem přičitatelným státu byly porušeny normy *iuris cogentis*, přidávají se k povinnosti zdržení se jednání a nahrazení újmy též povinnosti třetích států mj. neuznat protiprávní stav a odepřít pomoc a podporu státu, jemuž se jednání přičítá.[184] Odpovědnost v tomto případě se rozšiřuje na celé mezinárodní společenství; pouhé obnovení *statu quo ante inter partes* je v tomto případě nedostačující.[185]

3.3. Ústavní konformita navrhované regulace kybernetické bezpečnosti v ČR

Věcný záměr zákona o kybernetické bezpečnosti, jak byl představen v kapitole 2.4., musí být samozřejmě jako každá česká zákonná úprava v souladu s českým ústavním pořádkem (zejména

181 Text dokumentu v angličtině viz: CRAWFORD, J., PELLET, A., OLLESON, S. (eds.) op. cit. sub 170, str. 1241 a násl.

182 WYLER, E., PAPAUX, A. *The Different Forms of Reparation: Satisfaction.* In: CRAWFORD, J., PELLET, A., OLLESON, S. (eds.) op. cit. sub 170, str. 623-624.

183 Tamtéž, str. 630-632.

184 Srov. výklad in CRAWFORD, J., PELLET, A., OLLESON, S. (eds.) op. cit. sub 170, str. 677-701.

185 Srov. DAVID, V., BUREŠ, P., FAIX, M. op. cit. sub 166, str. 334.

s Ústavou ČR a Listinou základních práv a svobod). Otázky ústavní konformity je přitom nutné hodnotit ve světle *ústavních principů dělby moci a proporcionality.* Prizmatem druhé uvedené maximy českého ústavního pořádku, tedy proporcionality, pak zvažujeme dva zásadní problémy. Prvním je *dotčení lidských práv*, garantovaných Listinou a mezinárodními dokumenty (např. Evropská úmluva o ochraně práv a základních svobod, Mezinárodní pakt o občanských a politických právech, Listina základních práv Evropské unie). Druhým je pak *potřeba odchylné bezpečnostní úpravy* v případě kybernetického útoku, resp. stavu kybernetického nebezpečí.

Dělba moci zahrnuje respektování odděleného výkonu zákonodárství, praktického výkonu právních předpisů a jeho výkladu v konkrétních sporech o právo. Základy kontinentálního pojetí dělby moci se objevují v díle francouzského osvícence 18. století Charlese Louise de Montesquieu O duchu zákonů (*De l'esprit des lois*). Ekvivalentem dělby moci v doktríně *common law* je systém brzd a rovnovah (*checks and balances*), jak ho známe např. z Velké Británie.[186] Pro moderní, demokratický a právní stát (*Rechtsstaat, Rule of Law*) je v případě dělby moci kladen důraz na stěžejní roli orgánu voleného – zákonodárného shromáždění, které pravidelně vyslovuje důvěru vládě a jehož akty, ať již ústavní nebo zákonné právní síly, teprve zmocňují exekutivní státní moc k její činnosti vrchnostenské, podzákonné a nařizovací. Moc soudní je pak jako součást veřejné moci nezávislá (v ideálním případě fakticky i prostřednictvím právních záruk) na obou zbývajících složkách. Jejím úkolem je rozhodovat spory, ať již mezi soukromými osobami nebo korporacemi navzájem; stranou takových sporů může být za určitých okolností i sám stát. Soudní moc při své činnosti právo vykládá, dotváří (v kontinentálním systému psaného práva) nebo přímo vytváří nová právní pravidla, pokud neodporují účinné legislativě (precedenční doktrína zemí *common law*).

Věcný záměr předpokládá naplnění požadavků dělby moci jednak *ex definitione* řádným legislativním postupem při schvalování vlastního návrhu zákona, jednak udělením potřebného zmocnění k vydávání podzákonných předpisů (vyhlášky, opatření obecné povahy, individuální rozhodnutí) orgánům veřejné správy[187], zejména Národního bezpečnostního úřadu.[188] V souvislosti s dělbou moci upozorníme snad jen na nález Ústavního soudu Pl. ÚS 77/06 (37/2007 Sb.)[189], který se týká neústavnosti tzv. přílepků neboli legislativních jezdců, tj. věcně nesouvisejících pozměňovacích návrhů schvalovaných současně se zcela odlišnou materií.

Proporcionalita, tj. přiměřenost právní úpravy, se do české ústavní praxe dostala z německého prostředí. Její obdobou v prostředí *common law* (např. v USA) je tzv. *scrutiny test.* Filosofickým východiskem testu přiměřenosti je poznání, že základní práva a svobody se

186 V britském pojetí *checks and balances* nejsou jednotlivé složky státní moci zcela odděleny, ale mírně se prolínají a některými svými rozhodnutími na sobě závisí. Např. do konstituování britského Nejvyššího soudu v prvním desetiletí 21. století plnila funkci nejvyšší soudní instance Sněmovna lordů (*House of Lords*), tj. horní komora britského parlamentu.

187 Pro jistotu připomeňme, že vláda jako kolektiv je oprávněna vydávat podzákonné právní předpisy v mezích zákona již na základě čl. 78 Ústavy ČR; výslovné zákonné zmocnění na rozdíl od jiných orgánů veřejné správy proto není třeba.

188 Srov. *Věcný záměr zákona o kybernetické bezpečnosti [online].* op. cit. sub 115, str. 59-60, 64 [cit. 10.3.2013].

189 Nález je k dispozici na www: http://nalus.usoud.cz [cit. 10.3.2013].

nezřídka ve společenských, resp. právních vztazích dostávají do vzájemného střetu. Typickým případem je střet práva na soukromí a svobody projevu. V takových situacích přichází ke slovu poměřování kolidujících práv prizmatem proporcionality.

V české a německé podobě zahrnuje test proporcionality tři kroky. Prvním je test potřebnosti – otázka zní, zda (účinná, nebo navrhovaná) regulace je vůbec potřebná k tomu, aby bylo dosaženo zamýšleného účelu (např. ochrany určitých práv, omezení nežádoucího společenského jevu, urychlení řízení apod.). Dále následuje jako druhý krok test vhodnosti, kdy jsou vůči předpokládaným výsledkům poměřovány použité prostředky (např. předvídané individuální akty aplikace práva, zajištění osob nebo majetku apod.). Konečně, třetím prvkem kontinentální obdoby *scrutiny testu* je test minimalizace zásahu do „upozaděného" základního práva – tj. zhodnocení, zda právní norma, potažmo právní předpis i to právo, jež je v daném případě vnímáno jako relativně méně závažné, je omezeno pouze v nejnutnější míře, která ještě postačuje k naplnění účelu příslušné úpravy.[190]

Navržený Věcný záměr se k potřebě testu proporcionality výslovně hlásí.[191] Na základě konzultací byl upraven směrem k menší regulaci soukromých subjektů a národní CERT (viz kapitola 2.4.) byl vyčleněn ze struktury institucí mimo pravomoc NBÚ.[192] V rámci překotného technologického vývoje je nicméně nutno dbát na to, aby s ohledem na potřebný obecný dosah zákona byla jednotlivá ustanovení, ukládající povinnosti soukromoprávním subjektům nebo zasahující do jejich práv, formulována dostatečně konkrétně. Obecnost ustanovení do té míry, že umožňuje výkladem zasahovat do práv subjektů nad minimální míru, může být i důvodem zrušení této úpravy pro neústavnost (jako se stalo nálezem Pl. ÚS 24/10 v příp. §97/3, 4 zákona o elektronických komunikacích ve věci uchovávání provozních a lokalizačních údajů [tzv. nález *data retention*])[193] nebo nálezem Pl. ÚS 24/11, který zrušil §88a trestního řádu.[194] Na druhou stranu, Ústavní soud opakovaně judikoval v tom smyslu, že je-li možno namítanou neústavnost překlenout výkladem, má tento postup prioritu před zrušením napadeného ustanovení nebo předpisu.

Dotčení lidských práv

Základní lidská práva a svobody, jak je zakotvuje Listina základních práv a svobod a četné mezinárodní dokumenty (Evropská úmluva[195], Mezinárodní pakty o občanských a politických

190 V českém prostředí patrně poprvé byl test proporcionality použit Ústavním soudem v nálezu Pl. ÚS 4/94. Cit. in: Nález Ústavního soudu České republiky sp. zn. Pl. ÚS 24/11 ze dne 20. prosince 2011, bod 15. Oba k dispozici na www: http://nalus.usoud.cz

191 *Věcný záměr zákona o kybernetické bezpečnosti [online].*op. cit. sub 115, str. 77.

192 Srov. tamtéž, str. 51.

193 Nález Ústavního soudu České republiky sp. zn. Pl. ÚS 24/10 ze dne 22. března 2011 (94/2011 Sb.). K dispozici na www: http://nalus.usoud.cz

194 Nález Ústavního soudu České republiky sp. zn. Pl. ÚS 24/11 ze dne 20. prosince 2011 (43/2012 Sb.). K dispozici tamtéž.

195 Sdělení Federálního ministerstva zahraničních věcí č. 209/1992 Sb., o sjednání Evropské úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících.

a o hospodářských, sociálních a kulturních právech[196], Úmluva o právech dítěte[197] aj.) náleží mezi právní normy nejvyšší právní síly v českém právním řádu.[198] Kategorickým imperativem veřejné moci je jejich ochrana a výklad zákonného a podzákonného práva ve světle základních práv. Neproporcionální nebo dokonce svévolný zásah do základních práv prostřednictvím právního aktu zakládá jeho protiústavnost (u normativních právních aktů) nebo jeho nulitu (u individuálních právních aktů).[199] V obou případech je založeno oprávnění Ústavního soudu ke zrušení takového aktu (pravomoc negativního zákonodárce). Účinky normativních aktů přitom pomíjejí *ex nunc*, tj. až od účinnosti nálezu Ústavního soudu (na základě doktríny tzv. presumpce ústavní konformity), individuální akty pozbývají právní relevance *ex tunc*, tj. zpětně k okamžiku svého vydání.

Navrhovanou úpravu kybernetické bezpečnosti je třeba vážit především z pohledu práva jednotlivce na soukromí, resp. na soukromý a rodinný život, důvěrnost dopravovaných zpráv (v rámci kyberprostoru typicky e-mail, ale též VoIP volání, zprávy na sociálních sítích apod.) a též na informační sebeurčení (tj. na oprávnění jedince rozhodovat o tom, zda vůbec a potažmo které informace týkající se jeho osoby a soukromého života mohou být zpracovávány, kým a k jakému účelu). Potenciální zásah lze předpokládat též u svobody projevu a dalších tzv. informačních práv (svoboda vyhledávání a šíření informací, právo na vzdělání, svoboda vědeckého bádání). Poněkud volněji pak se specifickou regulací kyberprostoru souvisí realizace svobody svědomí, přesvědčení a vyznání. V souvislosti se stanovováním povinností soukromoprávních subjektů pak Věcný záměr předpokládá zásahy do práva vlastnictví a svobody podnikání. Jedná se konkrétně o povinnosti vlastníků infrastruktury, potažmo poskytovatele služeb informační společnosti – mimo stav kybernetického nebezpečí především povinnosti ohlašovací (kontaktní údaje, kybernetické bezpečnostní události) a povinnosti respektovat bezpečnostní standardy vydávané podzákonným předpisem NBÚ.

Informační práva. Informační práva vycházejí je možné *largo sensu* dovodit z práva na soukromí, resp. z práva na respektování soukromého a rodinného života. Na ústavní úrovni jsou informační práva zachycena v čl. 10, 13 a 15/2 Listiny, potažmo v čl. 8 Evropské úmluvy a čl. 17 Mezinárodního paktu o občanských a politických právech.[200] Při ochraně soukromí se ostře projevuje jak Jellinekův *status negativus* (veřejná moc nesmí zasahovat do soukromí člověka), tak též i *status positivus* (povinnost státu chránit jedince před narušením jeho soukromí). V judikatuře Evropského soudu pro lidská práva existují rozhodnutí, která staví na extenzivním

196 Vyhláška Ministerstva zahraničních věcí č. 120/1976 Sb., o Mezinárodním paktu o občanských a politických právech a Mezinárodním paktu o hospodářských, sociálních a kulturních právech.

197 Sdělení Federálního ministerstva zahraničních věcí č. 104/1991 Sb., o sjednání Úmluvy o právech dítěte.

198 I když mezinárodní smlouvy jsou podle čl. 10 Ústavy „pouze“ součástí právního řádu s aplikační předností před zákonem, akceptuje Ústavní soud jejich ustanovení jako standardy posuzování ústavnosti předpisů a procedur, pokud se týkají lidských práv.

199 Pro účely této práce ponecháváme stranou tzv. zdánlivé právní akty (pa-akty), u nichž většinou dochází bez ohledu na zásah do základních práv i k jiným zásadním právním vadám (nedostatek pravomoci k vydání nebo její překročení apod.).

200 Obdobné ustanovení je možné nalézt též v čl. 16 Úmluvy o právech dítěte.

výkladu výrazu „soukromý život“ – v případě dopravovaných zpráv, resp. shromažďování údajů se jedná o rozhodnutí *Niemetz proti Německu*[201], *Halfordová proti Spojenému království*[202], *Klass a další proti Německu*[203], *Malone proti Spojenému království*[204] a *Kruslin proti Francii.*[205] [206]

Jako nutnou podmínku pro autonomní existenci a adekvátní realizaci člověka v demokratickém právním státě pak český Ústavní soud postavil právo informačního sebeurčení na základě čl. 10/2 Listiny v nálezu II. ÚS 2048/09 ze dne 2.11.2009.[207] Problematiku informačního sebeurčení pak také poměrně výstižně vystihuje citace amerického rozhodnutí *Olmstead* z r. 1928, v jehož odlišném stanovisku soudce Brandeis poprvé definuje právo „být ponechán sám sobě“ (*to be let alone*).[208]

Pokud jde o svobodu projevu, Ústavní soud ve svém nálezu I. ÚS 453/03 deklaroval, že každý projev je nutné až do soudního přezkumu považovat za ústavně konformní, pokud jde o osobní úsudek, tj. nikoli fakty ověřitelný stav reality, ale vyjádření osobního postoje autora.[209]

---

201 Rozhodnutí Evropského soudu pro lidská práva ze dne 16. prosince 1992 ve věci stížnosti č. 13710/88. K dispozici na www: http://hudoc.echr.coe.int Pan Niemetz byl německým advokátem, jehož kancelář byla na soudní příkaz prohledávána v souvislosti s trestním řízením pro pomluvu. Účelem provedené prohlídky bylo pokusit se zjistit totožnost pachatele, který se měl dopustit pomluvy „jménem“ jistého místního politického subjektu, jehož byl p. Niemetz též členem; do jeho kanceláře byla dosílána i pošta pro tento subjekt. Soud konstatoval porušení čl. 8 Evropské úmluvy.

202 Rozhodnutí Evropského soudu pro lidská práva ze dne 25. června 1997 ve věci stížnosti č. 20605/92. K dispozici na www: http://hudoc.echr.coe.int Paní Halfordová pracovala v 80. letech jako policejní důstojník. V r. 1990 podala žalobu k britskému soudu, neboť se domnívala, že v otázce služebního postupu je diskriminována na základě pohlaví. Kromě jiných více či méně důvodných opatření vůči ní jí byl také odposloucháván služební telefon; tímto postupem bylo sledováno získání informací použitelných proti paní Halfordové ve zmíněném soudním sporu. Jelikož se dle rozhodnutí britských orgánů na případ nevztahoval zákon o odposleších (Interception of Communications Act 1985), konstatoval Soud nejen porušení práva na soukromý život dle čl. 8, ale též odepření účinného prostředku nápravy podle čl. 13 Úmluvy.

203 Rozhodnutí Evropského soudu pro lidská práva ze dne 6. září 1978 ve věci stížnosti č. 5029/71. K dispozici na www: http://hudoc.echr.coe.int

204 Rozhodnutí Evropského soudu pro lidská práva ze dne 2. srpna 1984 ve věci stížnosti č. 8691/79. K dispozici na www: http://hudoc.echr.coe.int

205 Rozhodnutí Evropského soudu pro lidská práva ze dne 24. dubna 1990 ve věci stížnosti č. 11801/85. K dispozici na www: http://hudoc.echr.coe.int

206 Rozhodnutí Klass, Kruslin a Malone cit. in: Nález Ústavního soudu České republiky, sp. zn. Pl. ÚS 24/11 ze dne 20.prosince 2011., bod 17. K dispozici na www: http://nalus.usoud.cz [cit. 10.3.2013].

207 Cit. in Nález Ústavního soudu České republiky, op. cit. sub 202, bod 29. [cit. 10.3.2013].

208 *Olmstead v. U. S.* 438, 478, 1928. Cit. in Nález Ústavního soudu České republiky sp. zn. Pl. ÚS 24/10 ze dne 22. března 2011 bod 27 (94/2011 Sb.) K dispozici na www: http://nalus.usoud.cz [cit. 10.3.2013].

209 K tvrzeným faktům, jež je nutno prokázat, srov. též rozhodnutí Sněmovny lordů ze dne 28. 10. 1999 ve věci *Reynolds v. Times News Papers Limited* (cit. in Nález Ústavního soudu České republiky sp. zn. I. ÚS 453/03 ze dne 11. listopadu 2005, sub IV.) [cit. 10.3.2013].

V případě informačních práv snad nejvíce závisí, s jakou péčí bude aplikován správními orgány test proporcionality. Oproti jiným odvětvím správního práva totiž na úseku kyberprostoru získává NBÚ značné pravomoci, neboť regulací virtuální reality ovlivňuje při vynaložení minimu zdrojů celou masu informačních práv. Je otázkou, zda nehrozí efekt tzv. *slippery slope*, tj. mírně, ale neustále se zvětšující míry zásahů do vyhledávání a šíření informací, jejich sledování a uchovávání. Obávám se také, že současná česká přetížená justice nebude schopna event. výtky proti činnosti NBÚ ze strany osob soukromého práva adekvátně rychle řešit.

Svoboda vlastnictví a svoboda podnikání. Tyto svobody zajišťuje český právní řád mj. v ustanoveních čl. 11, čl. 26 Listiny. Kromě obecného korektivu zákazu zneužití vlastnického práva a ustanovení, podle něhož je dovoleno vše, co není zákonem zakázáno, je svoboda vlastnictví zaručena za rovných podmínek s možnou výhradou cizinců (dnes již výhradně občanů nečlenských států EU) a svoboda podnikání s výhradou nutné profesní kvalifikace a státního povolení (koncese) v určitých případech.

Věcný záměr předpokládá, že vlastníci kritické a jiné infrastruktury, která slouží k zajišťování vitálních funkcí státu (vojenství, bezpečnost, zdravotnictví, energetika), potažmo podnikatelé v oblasti poskytování služeb informační společnosti budou (oproti jiným vlastníkům a podnikatelům v jiných oborech) zatíženi povinnostmi navíc. Jelikož se však jedná o povinnosti ohlašovací, které mají především preventivní význam, a povinnosti provádění protiopatření nařízená NBÚ, lze uzavřít, že z hlediska proporcionality takové řešení plně obstojí a zásahy do obou práv jsou ve srovnání s hodnotami, na jejichž ochranu se navrhovaná úprava zaměřuje, relativně zanedbatelné. Pouhou součinností subjektů, která při jejich předpokládaných ročních obratech (odhadem desítky milionů až miliardy korun ročně) bude představovat jen malou položku v nákladech (navíc event. daňově uznatelných), totiž bude ustaven mechanismus, bránící „zamoření“ českého kyberprostoru s hrozbou velkých ztrát citlivých dat, s tím souvisejícími ztrátami výkonnosti ekonomiky, ztráty na hmotném majetku, nebo dokonce i ztráty na životech (napadený klíčový software v jaderné elektrárně nebo zdravotnickém zařízení).

Svoboda svědomí, přesvědčení a vyznání. Tyto svobody, zaručené mj. čl. 15 Listiny a čl. 9 Evropské úmluvy, mohou být v zásadě dotčeny jednak dočasnou nepřístupností informací, které má osoba podle svého přesvědčení zájem vyhledávat, jednak povinností *dare, facere, ommittere* nebo *pati* za krizové situace, kdy na ní může být vynucováno jednání, které nebude odpovídat jejímu světonázoru nebo vyznání.[210]

Pokud jde o nepřístupnost informací, jednoznačně převažuje hledisko bezpečnosti; nehledě na to, že k nezanedbatelnému množství zdrojů bude podle všeho zachován přístup offline (knihy a další tištěné publikace v knihovnách). Mimořádné uložené povinnosti by pak za krizového stavu v kyberprostoru měly postihovat jiné subjekty než jednotlivce (viz následující oddíl v této kapitole), které ovšem nejsou ke svobodě svědomí, přesvědčení ani vyznání z povahy věci způsobilé. I tak jsou ale tyto povinnosti charakteru spolupráce se státním orgánem, což à priori

210 Už od dob evangelia nás nicméně západní kultura učí, že tvrdošíjně trvat na určitých pravidlech, dogmatech nebo rituálech i za cenu velkých škod na životech nebo majetku je v lepším případě neživotné, v horším přímo pokrytecké.

nevzbuzuje dojem dotčení práv jednotlivců, kteří budou tyto povinnosti jménem povinných subjektů vykonávat.

Bezpečnostní otázky

Úvod. V případě mimořádných událostí, ať přírodních (povodně, rozsáhlé požáry, zemětřesení), mezinárodních (válka, teroristický útok) nebo jiné povahy (nedostatek potravin, paliv apod.), je přípustné za podmínek čl. 4/3 Listiny na základě zákona omezit základní práva a svobody za podmínek rovného uplatnění těchto omezení. Jistou konkretizací tohoto obecného ustanovení jsou pak taxativní, byť spíše vágní výčty důvodů (ochrana života, zdraví, veřejného pořádku apod.) pro omezení některých práv (tajemství dopravovaných zpráv, vlastnické právo, právo na podnikání, svoboda projevu) u příslušných ustanovení Listiny. Povahu *legis generalis* pro bezpečnostní problematiku má ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění pozdějších předpisů. Ten stanoví ve svém čl. 1, že *„[z]ajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot je základní povinností státu".* Na úrovni zákonné je pak hlavním formálním pramenem práva zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů.

Krizová situace vyžaduje ochranu hodnot z hlediska demokratického sekulárního právního státu nejzávažnějších, tj. především života a zdraví, potažmo osobní svobody a až pak majetku. Ani v krizové situaci tak nesmí být nikdo podroben trestu smrti (viz Protokoly 6, 13 k Evropské úmluvě) a má právo na řádný soud (čl. 36 a násl. Listiny, čl. 6 Evropské úmluvy). Naopak, v krizových situacích je možno např. určité omezení nedotknutelnosti osoby a domovní svobody (srov. §5/a krizového zákona), dočasné zabírání vlastnictví (k tomu §5/b; samozřejmě za pozdější náhradu podle čl. 11/4 Listiny), výraznější omezení práva shromažďovacího nebo práva na stávku (§5/d, f). Tato omezení základních práv však musí být účelná a přiměřená hodnotám, jejichž ochrana se sleduje. Krizový zákon výslovně předvídá jako krizovou situaci též narušení kritické infrastruktury (srov. §2/b). V mimořádných situacích vznikají též nové povinnosti fyzickým osobám, podnikajícím fyzickým osobám a právnickým osobám (§29 a násl. krizového zákona).

Stav kybernetického nebezpečí. Věcný záměr se zabývá jedinou mimořádnou situací, a tou je stav kybernetického nebezpečí. Je definován jako „stav vyhlašovaný předsedou vlády České republiky na základě návrhu ředitele NBÚ, je-li ve velkém rozsahu ohrožena bezpečnost sítí nebo služeb elektronických komunikací nebo informačních systémů, … (čímž) dojde k porušení nebo ohrožení zájmu České republiky, a ohrožení není možné odvrátit běžnou činností Národního centra kybernetické bezpečnosti."[211]

Stav kybernetického nebezpečí je oproti obecné úpravě krizových stavů specifický minimálně v okruhu adresátů, jímž se jeho vyhlášením budou zakládat povinnosti, Nepůjde totiž o jednotlivce, fyzické osoby (mohli bychom říci „uživatele"), ale výhradně o osoby právnické, konkrétně pak poskytovatele služeb elektronických komunikací a správce kritické informační infrastruktury. Otázka potřebnosti speciální úpravy spočívá pak právě v okruhu subjektů,

211 *Věcný záměr zákona o kybernetické bezpečnosti [online].* op. cit. sub 115, str. 56-57 [cit. 10.3.2013].

kterým má vzniknout povinnost provádět opatření proti kybernetickému útoku, která nařídí NBÚ. Je jistě možné se přít, zda by bylo vhodnější vtělit jak obecnou, tak zvláštní úpravu krizových stavů do jednoho velkého předpisu (jakéhosi „krizového zákoníku"). Tak jako tak však tato speciální úprava musí být provedena, neboť charakter povinností, zcela míjejících jednotlivce, je odlišné kvality než u subjektů zahrnutých pod dosavadní obecnou úpravu (pomoc při zpracování krizových plánů, poskytnutí věcných prostředků, pracovní povinnost apod.).[212]

Závěrečné poznámky

S problematikou proporcionality a ochrany základních práv souvisí též další ústavní maxima, jíž je zákaz libovůle v rozhodování. Za stavu kybernetického nebezpečí bude již z povahy věci ochromen výkon shora naznačených práv, pokud má být uskutečňován v kyberprostoru (anebo toto ochromení bude vysoce pravděpodobné). Otázkou spíše zůstává, nakolik bude možné zachovat výkon těchto práv i v offline světě, který – jak bylo dříve uvedeno – na tom virtuálním již značně závisí. V daném případě budou muset zúčastněné orgány vč. NBÚ pečlivě vážit předběžnou opatrnost, která bude velet k většímu omezení virtuální interakce a komunikace oproti maximálnímu zachování práv a svobod jednotlivců, potažmo právnických osob. Rozhodování to bude o to těžší, že na rozdíl od konfliktu válečného nepůjde o dny nebo hodiny, ale řádově o minuty nebo i vteřiny.

Věcný záměr zákona o kybernetické bezpečnosti ústavní hlediska v žádném případě nepomíjí, naopak. Z hlediska jeho ústavní konformity je možno doporučit, aby paragrafované znění obsahovalo, resp. formou odkazu obsáhlo určité principy, na nichž bude předpis vybudován. Dále bude nezbytné u většiny neurčitých pojmů připojit alespoň demonstrativní výčet znaků, za nichž bude ustanovení s tímto pojmem aplikovatelné. Tam, kde bude třeba konkretizace zákonného ustanovení s ohledem na aktuální technologie, je vhodné přenechat delegací normotvorbu v nutném rozsahu prováděcím předpisům. Klíčovým prostředkem k dosažení ústavní konformity tohoto zákona bude též nepochybně vhodně prováděný (účel a smysl zákona a ochranu subjektivních práv zohledňující) výklad jeho ustanovení.

[212] Srov. ust. §29 krizového zákona. Jedním z mála styčných bodů krizového zákona a navržené úpravy kybernetické bezpečnosti jsou ustanovení o prvku kritické infrastruktury (srov. §2/g, h, §29a – 29c krizového zákona).

4. ZÁVĚR

Tato práce se zabývala kybernetickou bezpečností, a to jednak obecně, jednak ve vazbě na aktuální právní poměry v České republice. Vymezila postupně kyberprostor-virtuální realitu, pojem bezpečnosti z hlediska soudobých bezpečnostních studií a zaměřila se na hrozby, kterým paralelní virtuální „binární" realita aktuálně (tj. v období 2011-2012) čelí. Práce přináší přehled legislativy na národní, evropské i mezinárodní úrovni, a to i se snahou reflektovat možný vývoj *de lege ferenda*, zejména pokud jde o zákon České republiky o kybernetické bezpečnosti.

Ve zvláštní části této práce jsem se nejprve zabýval relevantními kritérii pro určování všech typů jurisdikce orgánů České republiky, tj. mezinárodní pravomocí, rozhodným právem a konečně vymahatelností. Svět jurisdikce kybernetické bezpečnosti se díky dominujícím prvkům práva veřejného poměrně značně liší od jurisdikce v mezinárodním právu soukromém. V něčem je jednodušší; ďábel se ovšem skrývá ve schopnosti a ochotě k mezinárodní spolupráci a respektu jednotlivých státních suverénů.

Téma mezinárodního kybernetického konfliktu jako druhé ve zvláštní části se pokoušelo nastínit odlišnosti kybernetického útoku od ostatních forem ozbrojeného boje (ať v podobě agrese nebo sebeobrany) a alespoň se přiblížit k nezřetelné, ale přesto nutně reálně existující hranicí mezi kybernetickým konfliktem a kybernetickým (byť i trestním) deliktem, který má na svědomí soukromá osoba bez jakékoli vazby na stát a jeho zájmy.

Poslední text zvláštní části si potom kladl otázku ústavní konformity uvažovaného návrhu zákona o kybernetické bezpečnosti, ztělesněného zmiňovaným věcným záměrem. Prochází postupně otázky proporcionality, dělby moci, dotčení základních lidských práv a jen stručně naznačuje úskalí aplikace práva kyberprostoru v krizových situacích – počínaje stavem kybernetického nebezpečí a konče stavem válečným.

Je nesporné, že informační a komunikační technologie se i nadále vyvíjejí a představují výzvu – ať ve smyslu normativním nebo deskriptivním – pro právo a právní vědu, ale i pro etiku, sociologii, pedagogiku a *last but not least* i pro přírodní vědy.

Pragmatický přístup, který je posledním výdobytkem jurisprudence ve vztahu k průřezovému odvětví práva ICT, je zatím ve své ideální podobě nejblíže přístupu, který by se dal označit jako přístup zdravého rozumu. Nemají-li mít ale pravdu kritici pragmatismu (viz např. Dworkin) a nemá-li se tedy naplnit jejich teze o kontinuálním úpadku práva v zajetí ryzího pragmatismu, pak je nutno zachovat vazbu pragmatického uvažování na elementární základy demokratického právního státu, totiž dlouhodobě postulované, byť nepsané právní principy.

Tato možná již současná, možná teprve budoucí podoba pragmatismu v právu překlenuje propast mezi překotným vývojem technologie a rigiditou právního řádu nikoli snad eliminací, ale řízeným ústupem ze slávy nejrigidnějšího (jakkoli častým novelizacím podléhajícího) prvku právního řádu, kterým je podústavní psané právo, tj. klasická legislativa. Pragmatické uvažování má dva nosné pilíře: právní principy (jak jsou zakotvené v Ústavě, resp. ústavách civilizovaných národů a vykládány ústavními, resp. nejvyššími soudy) a faktický problém, resp. spor vzešlý z komunikační infrastruktury a vymezený zákonitostmi kyberprostoru, jehož řešení v duchu právních principů leží na bedrech soudu. Na tyto dva pilíře pak navazuje legislativní práce, která pokud možno určuje směr, kterým se má ubírat interpretace budoucích právních problémů,

popř. řešení problémů již právu ICT a rozhodovací praxi soudů známých, a to v perspektivě *pro futuro*. Vzhledem k chronické přetíženosti justice není od věci ani perspektiva řešení bagatelních nebo kvazibagatelních věcí soukromými autoritami (např. provozovatelem webu, na němž došlo k protiprávnímu nebo alespoň morálně pochybnému jednání, speciálními institucemi složenými z odborníků na právo a uživatelů apod.). Jako poněkud problematická se naopak jeví jakási jurisdikce *sui generis* definičních autorit – zvláště proto, že nejvyšší definiční autorita odpovědná za fungování celého internetu sídlí v USA, které mají čas od času tendenci dávat přednost svým zájmům na úkor zájmů ostatních států, resp. celé mezinárodní komunity.

S narůstajícími možnostmi výpočetní techniky se objevují nové možnosti a příležitosti, ale i nové hrozby. Méně formalit je pro zachování rychlého a pružného online spojení se zbytkem světa nutností. Na místo rigidního práva by mělo nastoupit právo nepsané, zvykové – jehož předobrazem snad může být i netiketa – a vynucované jak pomocí sociálních mechanismů akceptace a exkomunikace v rámci online komunit, tak pověřenými definičními autoritami na všech kontinentech a pod dohledem celého mezinárodního společenství. Základem však zůstává odpovědnost jednotlivce-uživatele, kterému osud sítě sítí a dění na ní nebude lhostejný.

Tato práce mi umožnila zaměřit se na různorodá témata, v nichž se stýká právo a informační technologie. Těchto témat k mé radosti stále více přibývá, a tím přibývá i zákoutí k objevování a otázek k zodpovězení. V duchu svého životního hesla *Gaudium scientiae* (Radost z poznání) oceňuji, že jsem si pod vedením doc. Polčáka rozšířil své obzory. Mrzí mě snad jen převaha popisnosti v tomto textu, neboť nové obory by si žádaly trochu více kreativity. Leč zřejmě nelze žádat po stále ještě jen poučeném právním laikovi, aby se pokoušel obsáhnout svými normativními soudy celé mezinárodní společenství a exabyty dat. „Bylo to krásné, a bylo toho dost," chtělo by se říci. Snad tedy na shledanou někdy v budoucnu – reálně nebo i virtuálně.

POUŽITÉ ZDROJE

1. CRAWFORD, J., PELLET, A., OLLESON, S. (eds.) *The Law of International Responsibility. Oxford Commentaries on International Law.* 1st ed. New York: Oxford University Press, 2010. lxv, 1296 str. ISBN 9780199296972.
2. CURRIE, D. P., KAY, H. H., KRAMER, L. et al. *Conflict of Laws. Cases – Comments – Questions.* 7th ed. St. Paul, Minnesota: Thomson/West, 2006. 921 str.
3. DAVID, V., BUREŠ, P., FAIX, M. et al. *Mezinárodní právo veřejné s kazuistikou.* 2. akt. a přeprac. vyd. Praha: Leges, 2011. 448 str. ISBN 9788087212868.
4. GOLDSMITH, J., POSNER, E. A. *The New International Law Scholarship.* Chicago: The Law School of the University of Chicago. Public Law and Legal Theory Working Paper No. 126, May 2006. 27 str.
5. GRADY, M. F., PARISI, F. (eds.). *The Law and Economics of Cybersecurity* 1st ed. New York: Cambridge University Press, 2006. 310 str. ISBN 0521855276.
6. HUGHES, C. W., MENG, L. W. (eds.) *Security Studies. A Reader.* 1st ed. Abingdon (UK), New York: Routledge, 2011. xviii, 451 str. ISBN 9780415326001 (hardback), 9780415326018 (paperback).
7. KOHL, U. *Jurisdiction and the Internet.* 1st ed. Cambridge: Cambridge University Press, 2007. 323 str.
8. KUČERA, Z. *Mezinárodní právo soukromé.* 7. opr. a dopl. vyd. Brno – Plzeň: Doplněk – Aleš Čeněk, 2009. 462 str. ISBN 9788072392315 (Doplněk Brno), 9788073801717 (Aleš Čeněk Plzeň).
9. LESSIG, L. *Code, version 2.0.* 2nd ed. New York: Basic Books, 2006. 410 str. ISBN 0465039146.
10. MATYÁŠ, V. et al. *Ochrana dat a informačního soukromí.* Cyklus přednášek v rámci stejnojmenného kurzu na Katedře počítačových systémů a komunikací Fakulty informatiky Masarykovy univerzity v podzimním semestru akademického roku 2012/2013. Brno, 2012.
11. *Národní centrum kybernetické bezpečnosti.* Materiál prezentovaný na veletrhu pracovních příležitostí Job Challenge 2012, konaném v Brně dne 7.11.2012. 2 str.
12. ONDŘEJ, J., ŠTURMA, P., BÍLKOVÁ, V. et al. *Mezinárodní humanitární právo.* 1. vyd. Praha: C.H.Beck, 2010. 559 str. ISBN 9788074001857.
13. PAULSSON, J. *Denial of Justice in International Law.* 1st paperback ed. Cambridge: Cambridge University Press, 2010. xxvi, 279 str. ISBN 9780521172912.
14. POLČÁK, R. *Internet a proměny práva.* 1.vyd. Praha: Auditorium, 2012. 388 str. ISBN 9788087284223.
15. POŽÁR, J. *Informační bezpečnost.* Plzeň: Aleš Čeněk, 2005. 311 str. ISBN 8086898385.
16. SVANTESSON, D. J. B. *Private International Law and the Internet.* 1st ed. Alphen an den Rijn: Kluwer Law International, 2007. xxi, 440 str.
17. SVANTESSON, D. J. B. *Private International Law and the Internet.* 2nd ed. Alphen an den Rijn: Kluwer Law International, 2012. xxii, 557 str.

Elektronické zdroje

18. *ASPI 2012 [právní informační systém].* K dispozici na www: http://www.wkcr.cz
19. BROWN, S.B. (ed.) *Trustwave 2012 Global Security Report [online].* K dispozici na www: http://www.iseprograms.com/lib/Trustwave_2012GlobalSecurityReport.pdf

20. *Council of Europe Webpage [online].* K dispozici na www: http://www.coe.int

21. *Dictionary.com [online].* K dispozici na www: http://dictionary.com

22. *Eur-Lex. Přístup k právu Evropské unie [online].* K dispozici na www: http://eur-lex.europa.eu

23. *Financial Crimes Enforcement Network. United States Department of Treasury [online].* K dispozici na www: http://www.fincen.gov/

24. *GovTrack.us: Tracking the U. S. Congress [online].* K dispozici na www: http://www.govtrack.us/

25. *HeinOnline [online databáze].* K dispozici na www: http://www.heinonline.org

26. *Job Challenge 2012 Newsletter [online].* K dispozici na www: http://www.jobchallenge.muni.cz/uploads/media/Newsletter_JobChallenge2012.pdf. 7 str.

27. LICHTMAN, D., POSNER, E. A. *Holding Internet Service Providers Accountable [online].* School of Law, University of Chicago, 2004. 51 str. Available via www: http://ssrn.com/abstract_id=573502

28. *Mendeley Desktop 1.6 [online software].* K dispozici na www: http://www.mendeley.com

29. *North Atlantic Treaty Organization Webpage [online].* K dispozici na www: http://www.nato.int

30. ROUSE, M., ROSSETTI, L. *What is Business Intelligence? [online].* K dispozici na www: http://searchdatamanagement.techtarget.com/definition/business-intelligence Poslední aktualizace 11/2006 [cit. 29.01.2013].

31. *Searchkindly.org [online vyhledávač].* K dispozici na www: http://www.searchkindly.org

32. *Sophos Security Threat Report 2012 [online].* K dispozici na www: http://www.sophos.com/en-us/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf

33. SYMEONIDES, S. C. *Party Autonomy and Private-Law Making in Private International Law: The Lex Mercatoria that Isn't [online].* In: Liber Amicorum Konstantinos D. Kerameus. Athens: Sakkoulas/Kluwer Press, 2006. 25 str.

34. TRACHTMAN, J. P. *Global Cyberterrorism, Jurisdiction and International Organization [online].* Tufts University - The Fletcher School of Law and Diplomacy, 2004. 36 str. K dispozici na www: http://ssrn.com/abstract=566361

35. *United Nations Webpage [online]*. K dispozici na www: http://www.un.org

36. *The White House Webpage [online].* K dispozici na www: http://www.whitehouse.gov/

37. *World Legal Information Institute [online]. K dispozici na www:* http://www.worldlii.org

38. *Zákony pro lidi [online].* K dispozici na www: http://www.zakonyprolidi.cz