KYBERNETICKÁ BEZPEČNOST JAKO AKTUÁLNÍ FENOMÉN ČESKÉHO PRÁVA[*]

RADIM POLČÁK[**]

ABSTRAKT

Česká republika je jedním z prvních civilizovaných států, který zavedl komplexní právní úpravu národní kybernetické bezpečnosti. Z hlediska právní vědy jde o relativně nový regulatorní fenomén, kterému je třeba se věnovat za užití specifické metody a při zohlednění pro právo netradičních faktorů. Článek se vedle metodického přístupu k právním problémům národní kybernetické bezpečnosti věnuje též jednotlivým institutům tohoto nového právního odvětví. V závěru pak je provedena diskuse možného dalšího vývoje legislativy i organizačních resp. technických forem řešení bezpečnostních rizik majících původ ve službách informační společnosti.

KLÍČOVÁ SLOVA

kybernetická bezpečnost; kritická informační infrastruktura; zákon o kybernetické bezpečnosti; bezpečnostní opatření; kybernetický bezpečnostní incident

ABSTRACT

Czech Republic was among first civilised countries that implemented complex national legislation on cybersecurity. This relatively new legal regulatory phenomenon requires specific methodological approach that, quite unusually for continental Europe, acknowledges a number of extra-legal factors. The paper tackles the basic methodological issues and it also analyses particular institutes

[*] Tento článek vznikl jako součást plnění projektu OPPI 5.1 SPTP02/029 Energetická a kybernetická bezpečnost.

[**] Doc. JUDr. Radim Polčák, Ph.D. je vedoucím Ústavu práva a technologií Právnické fakulty Masarykovy univerzity. Kontaktní e-mail: radim.polcak@law.muni.cz.

of cybersecurity law. In conclusions, it tries to discuss further development on the Czech legislation as well as of organisational and technical solutions for cybersecurity risks.

KEYWORDS

cybersecurity; critical information infrastructure; Cybersecurity Act; security measures; cybersecurity indicent

1. METODOLOGIE PRÁVA KYBERNETICKÉ BEZPEČNOSTI

Obecně lze v právním instrumentariu nalézt tři typy právních metod, a to metody pozitivistické, naturalistické a realistické (či pragmatické). Pozitivistické metody vyznačují se pojmovým oddělením pravidel od faktických informací[1]. Znamená to mimo jiné, že pravidlo nemůže svým obsahem vycházet z informace o skutečnosti (z výroku), ale je vždy vytvořeno jako originální informace o povinnostech. Fakticita se zde v obsahu pravidel nijak neprojevuje a s fakty pracujeme pouze jako s faktory naplnění subsumpčních podmínek[2]. Jinak řečeno je tedy v tomto metodologickém pojetí právo systémem originálně tvořených povinnostních informací a fakta jsou pro právo důležitá pouze co do rozhodování v otázce, zda právo pro konkrétní situace formuluje nějaké konkrétní imperativy (tj. v otázce, zda jsou ad hoc naplněny znaky hypotéz příslušných právních norem).

Obecně se oddělení faktických a povinnostních informací u právního pozitivismu projevuje absencí vztahu mezi právem a morálkou[3]. Morálka jako faktická kategorie totiž nemůže v pozitivistickém pojetí práva ovlivňovat obsah právních pravidel[4]. To samozřejmě neznamená, že právní

[1] Toto oddělení je založeno na Humově základní filozofické distinkci mezi bytím (is) a mětím (ought) – viz Hume, D. A Treatise on Human Nature. *Project Gutenberg*, 2003, dostupný online na adrese www.gutenberg.org/etext/4705.

[2] Kelsen označuje toto pojetí práva za „ryzí," tj. oproštěné od všeho, co do něj nepatří – viz Kelsen, H. *Pure Theory of Law*, přel. Knight, M. Berkeley: University of California Press, 1978, str. 1.

[3] K tomu srov. např. Alexy, R. *The Argument from Injustice*, přel. Paulson, S., Litschewski Paulson, B. Oxford: Oxford University Press, 2002, str. 85 a násl.

[4] Kritika nedostatku tohoto přístupu spočívajícího obecně v pojmové nemožnosti hodnotové reflexe obsahu platného práva je možno najít např. v díle Vladimíra Čemáka – viz Baroš, J. (ed.) *Vladimír Čermák – člověk, filozof, soudce*. Brno: Masarykova univerzita, 2009, str. 248.

pravidla musí být nutně amorální – jejich konstrukci ani aplikaci však morálka v tomto pojetí přímo neovlivňuje.

V oboru práva informačních a komunikačních technologií se základní motiv pozitivistické metodologie projevuje neexistencí přímého vztahu mezi faktickou situací určité technologie (tj. jejími parametry, fungováním apod.) a obsahem právních pravidel regulujících její užití. Důsledná aplikace pozitivistické metodologie v tomto směru může vést k takovým důsledkům, kdy je právně formulován právně perfektní (bezvadný) takový právní předpis nebo takové soudní rozhodnutí, jejichž praktická aplikace je z nějakého praktického důvodu vyloučena – k tomu může dojít tehdy, jsou-li např. stanoveny nereálné požadavky na nějakou technologii, právo požaduje řešení, které téměř nelze organizačně zvládnout nebo je vyžadováno splnění takové povinnosti, která je z ekonomického hlediska absurdní. Z právě uvedeného plyne, že užití této metody k řešení problému kybernetické bezpečnosti není vhodné[5].

Druhou možností je naturalistická právní metodologie[6] postavená ve vztahu k pozitivismu na zcela opačné tezi spojení faktických a povinnostních informací. Obecnou implikací této teze je možnost přímého dovození právních pravidel z morálky a jí odpovídající předpoklad, že objektivní právo je jen konstatováním existence přirozených pravidel (de facto přírodních zákonů) a že právotvorba není ve skutečnosti o originárním vytváření právních pravidel ale pouze o jejich nalézání.

Aplikace naturalistické metodologie v právu informačních a komunikačních technologií vede k závěru formulovaného předním americkým konstitucionalistou Lawrencem Lessigem, že totiž „kód je zákonem kyberprostoru.[7]“ Znamená to, že právo pro informační síť je resp. má být pouze dovozováno z technických pravidel definujících možnosti chování uživatele. Lessigem popsaný stav již v řadě ohledů reálně funguje. Především v případech, kdy brání uplatnění práva některý z právních nebo

[5] Nepomáhá v tomto směru ani výjimečná zásada impossibilium nulla obligatio – její aplikace je totiž podmíněna aletickou nemožností. V technologicky exponovaných situacích však je nutno z pohledu práva nezřídka šlápnout i na kluzký svah organizační resp. obchodní nemožnosti. To je pro právní pozitivismus neakceptovatelné, neboť může následná normativní eroze vést až k důsledkům shrnutelným slovy klasika do postulátu „když nemůžu, tak nemusím.“

[6] Obecně k pojmu viz Finnis, J. *Natural Law.* New York: New York University Press, 1991.

[7] Viz Lessig, L. *Code V. 2*. New York: Basic Books, 2006.

přirozených limitů (tj. např. otázka jurisdikce, absence věcné působnosti, vysoké náklady na výkon práva apod.), je kód skutečně dominantním normativním faktorem ovlivňujícím, často výlučně, chování uživatelů.

Z právě popsaného důvodu nelze s iusnaturalistickou metodologií pracovat pro potřeby řešení problému kybernetické bezpečnosti. Přijetí tohoto přístupu by totiž v prostředí informačních sítí znamenalo popření základní premisy, na níž zde v současnosti stojí legitimita práva, tj. že právo je legitimováno veřejným zájmem vyjádřeným prostřednictvím instituce státu. Iusnaturalistické pojetí totiž přisuzuje možnost definovat obsah právních pravidel subjektům majícím pod kontrolou technické parametry příslušných součástí informační sítě, z nichž většinou jde o soukromoprávní korporace.

Nikoli jen vylučovací metodou jeví se jako nejvhodnější k řešení problému kybernetické bezpečnosti metoda realistická[8]. Je postavena na podobném předpokladu jako právní pozitivismus, tj. že obsah právních pravidel je originárně vytvářen a je zajišťován autoritou státu, avšak netrvá na důsledném pojmovém oddělení právních pravidel od faktických informací. Zohlednění fakticity, ať technické, ekonomické nebo organizační, má formu omezení legislativních a aplikačních výstupů o ty, které jsou, stručně řečeno prakticky (pragmaticky) neproveditelné[9]. Pragmatický zákon tedy počítá jen s takovými povinnostmi, které je reálně možno splnit bez větší zátěže pro povinné subjekty a soudní rozhodnutí je založeno na předpokladu reálné (nikoli ideální) společenské, technické a ekonomické situace[10].

Zřejmá nevýhoda realistické metodologie spočívá především v riziku relativizace právních hodnot, neboť tam, kde se jejich důsledná aplikace odchyluje od toho, co považujeme za součást technické, společenské nebo ekonomické reality, prostě od nich ustoupíme. To může vést k Dworkinem kritizovanému postupnému úbytku ideálů[11] a nebezpečí tvorby situací, kdy

[8] Používá se též výrazu pragmatismus – k tomu viz např. James, W. *Pragmatism*. Rockville: ARC Manor, 2008 nebo Tamanaha, B. *Beyond the Formalist – Realist Divide*. Princeton: Princeton University Press, 2010, str. 67 a násl.

[9] K tomu viz např. Rorty, R. The Banality of Pragmatism and the Poetry of Justice. *Southern California Law Review*. 1990, roč. 63, str. 1811 a násl.

[10] Srov. Sharp, W.G. Sr. The Past, Present and Future of Cybersecurity, *Journal of National Security Law and Policy*, roč. 4, číslo 13, str. 19 a násl.

[11] Viz Dworkin, R. *Justice in Robes*. London: Belknap Press, 2006, str. 38.

právo jen kopíruje požadavky ekonomické, technické nebo obecně společenské reality resp. toho, co je za realitu aktuálně považováno politickou mocí. Na druhou stranu však realistická metodologie poskytuje jako jediná z uvedených alternativ prakticky použitelná řešení pro situace vyznačující se značnou mírou technické, ekonomické či společenské složitosti a právě takovou situací je současný stav informační společnosti[12]. Udržení úrovně hodnot a principů, jakož i idealistického charakteru právních pravidel je v tomto případě řešeno nikoli metodologicky ale institucionálně prostřednictvím legitimity orgánů veřejné moci zajišťujících tvorbu příslušných právních pravidel a jejich následnou implementaci[13].

2. LEGISLATIVNÍ ŘEŠENÍ KYBERNETICKÉ BEZPEČNOSTI

Legislativní řešení kybernetické bezpečnosti nemá v platném právu žádnou prakticky srovnatelnou paralelu. Lze sice pro partikulární otázky používat nejrůznější analogie s bezpečnostními řešeními v oborech s dominantní technologickou komponentou (typicky např. v oborech stavebnictví, protipožární ochrany, dopravy, apod.), právní fenomén kybernetické bezpečnosti se však jako takový ničemu ve své podstatě nepodobá[14].

Prvním důvodem originality kybernetické bezpečnosti je skutečnost, že hodnocení bezpečnostních aktiv má až na výjimky obvykle akcesorickou povahu. Systémy a sítě, jejichž zabezpečení je předmětem právní úpravy, totiž zpravidla nemají hodnotu per se, ale závisí na tom, čemu v konečném důsledku slouží[15]. S trochou nadsázky tedy lze prohlásit, že tentýž router může sloužit jako součást informační infrastruktury internetové kavárny

[12] Viz Polčák, R. *Internet a proměny práva*, Praha: AUDITORIUM, 2012, str. 85.

[13] K tomu srov. např. Polčák, R. Internet Legal Culture, Lex Informatica and (un)Desired Sovereignty of Lawyers. In Lindskoug, P., Manusbach, U. Millqvist, G., Samuelsson, P., Vogel, H. H. *Essays in Honour of Michael Bogdan*. 1. vyd. Lund: Författarna och Juristförlaget i Lund, 2013, str. 477 a násl.

[14] Srov. např. Fredland, J. S. Building a Better Cybersecurity Act: Empowering the Executive Branch Against Cybersecurity Emergencies, *Military Law Review*, číslo 206, str. 26 a násl., nebo Brenner, S. Cyber-threats and the Limits of Bureaucratic Control, *Minnesota Journal of Law, Science and Technology*, roč. 14, číslo 1, str. 151 nebo též Grant, J. Will There Be Cybersecurity Legislation? *Journal of National Security Law and Policy*, roč. 4, str. 104. Další důvody zvláštního charakteru kybernetické bezpečnosti přidává Paul Rosenzweig v textu Rosenzweig, P. Making Good Cybersecurity Law and Policy: How Can We Get Tasty Sausage?, *Journal of Law and Policy for the Information Society*, roč. 8, číslo 2, str. 390.

[15] Srov. např. systematiku hrozeb dle Kesan, J. P., Hayes, C. M. Mitigative Counterstriking: Self-Defence and Deterrence in Cyberspace, *Harvard Journal of Law and Technology*, roč. 25, číslo 2, str. 445.

i atomové elektrárny, přičemž jeho bezpečnostní hodnota není dána jeho cenou, ale způsobem jeho užití[16].

Výjimkou ze shora uvedeného jsou systémy a sítě, jejichž smyslem a účelem je působit jako součást národní informační a komunikační infrastruktury. Typicky např. tzv. páteřní sítě neodvozují svoji důležitost od hodnoty funkcionalit, k nimž byly pořízeny, neboť jejich funkcí je udržovat v chodu informační síť jako takovou – v jejich případě tedy není nutno hodnotit, jakému primárnímu účelu slouží, neboť jejich důležitost je zpravidla dána faktory, jako jsou kapacita, zastupitelnost apod[17].

Druhým významným faktorem odlišujícím legislativní řešení kybernetické bezpečnosti od ostatních oborů platného práva je její procesní orientace. Zatímco právní úprava krizového řízení resp. úprava bezpečnosti kritických funkcionalit státu je tradičně postavena na objektovém principu, je kybernetickou bezpečnost nutno primárně vnímat jako ochranu informačních procesů[18]. Tomu pak musí odpovídat celá regulatorní logika i fungování příslušných orgánů veřejné moci, neboť primárním smyslem a účelem není ochrana existence nebo funkčnosti konkrétně definovaného objektu, ale zajištění bezproblémové existence informačních transakcí. Výsledné řešení přitom samozřejmě nemůže být vzhledem k objektům dohromady tvořícím naši informační a komunikační infrastrukturu absolutně indiferentní – objekt však má být předmětem regulatorního zájmu až v důsledku jeho konkrétní důležitosti pro kritický informační proces[19].

---

[16] Srov. např. Shane, P. M. Cybersecurity Policy as if "OrdinaryCitizens" Mattered: The Case for Public Participation in Cyber Policy Making, *Journal of Law and Policy for the Information Society*, roč. 8, číslo 2, str. 435.

[17] V českém právu je tato skutečnost zohledněna subsidiárním kritériem pro určení prvku kritické informační a komunikační infrastruktury ve smyslu ust. části VI.G.d. přílohy k nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění pozdějších předpisů.

[18] Srov. Hathaway, M. E., Klimburg, K. Preliminary Considerations: On National Cybersecurity, in Klimburg, A. *National Cybersecurity – Framework Manual*, Talinn: CCDCOE, 2012, str. 8.

[19] Viz např. Srov. např. Lin, H. Thoughts on Threat Assessment in Cyberspace, *Journal of Law and Policy for the Information Society*, roč. 8, číslo 2, str. 338. Současná česká právní úprava je naproti tomu vzhledem ke kritické informační a komunikační infrastruktuře orientována objektově. Je to dáno skutečností, že definiční kritéria pro kvalifikaci informačního systému nebo sítě obsažená v části VI.G.a., VI.G.b. a VI.G.d. přílohy k nařízení vlády č. 432/2010 Sb. jsou svázána s objektovými definicemi ostatních prvků národní kritické infrastruktury.

Třetím specifickým rysem právní úpravy kybernetické bezpečnosti je právní jev, který je doktrínou popisován jako fenomén definičních autorit. Veškeré lidské jednání totiž v prostředí informačních sítí neprobíhá bezprostředně, ale je zprostředkováváno službami informační společnosti. Člověk ani právnická osoba tedy nemůže v prostředí informačních sítí činit nic bez toho, aby se na jeho jednání fakticky nepodílela hned celá řada poskytovatelů služeb informační společnosti[20].

Označení definiční autority si tyto subjekty vysloužily z toho důvodu, že mají faktickou možnost definovat formou kódu (tzv. definiční normy) technické parametry jednání svých uživatelů. Nejedná se přitom o normu právní, neboť poskytovatelé služeb informační společnosti nedisponují právotvornou kompetencí (jde povětšinou o soukromé subjekty)[21] – přesto jde nepochybně o pravidlo, které má na jednání uživatelů zásadní vliv.

Definiční charakter těchto technických resp. faktických pravidel je od právních norem odlišuje i co do jejich fungování. Byť jde o pravidla vytvořená člověkem a zaměřená k regulaci lidského chování, nemají charakter povinnostní, ale jde o kauzální normy přímo determinující na technické úrovni výsledek lidského jednání[22]. Jsou to v podstatě člověkem vytvořené normy zaměřené k regulaci lidského chování, ale jejich technický charakter jim dává povahu kauzálního přírodního zákona.

Z právního hlediska jde o extrémně zajímavý jev mající zásadní dopady především do problematiky odpovědnosti za protiprávní jednání[23]. Především z toho důvodu, že poskytovatelé služeb informační společnosti jsou v problematických případech jedinými subjekty, které lze reálně

[20] Základem teorie definičních autorit je práce amerického konstitucionalisty Lawrence Lessiga op. cit. v pozn. 7. Z českých pramenů viz např. Polčák, R. *Internet a proměny práva*, Praha: Auditorium, 2012, str. 137 a násl.

[21] K institucionálním požadavkům na právotvůrce viz např. Kelsen H. *Pure Theory of Law*, přel. Paulson, B. L., Paulson S., Oxford: Oxford University Press, str. 91 a násl.

[22] Namísto povinnosti v tomto případě hovoříme o nutnosti člověka jednat určitým způsobem. Definiční norma nepůsobí nutnost jednat pouze v situaci, pokud ji její adresát dokáže technicky eliminovat. Definiční normou tedy není vázán pouze hacker (v pravém smyslu toho slova) – viz Polčák, R. *Internet a proměny práva*, Praha: Auditorium, 2012, str. 193.

[23] Ve státech Evropské unie vznikla za tímto účelem specifická legislativa omezující odpovědnost poskytovatelů služeb informační společnosti za protiprávnost jednání jejich uživatelů. Harmonizačním předpisem je směrnice 2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu), přičemž do českého práva byla omezení implementována zákonem č. Zákon o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů.

nalézt, proti nimž lze uplatnit právní postih a které jsou technicky schopny problematickou situaci efektivně řešit, vznikla celá relativně samostatná teorie spoluodpovědnosti těchto poskytovatelů za protiprávní jednání jejich uživatelů[24]. Dokonce lze konstatovat i dříve nevídaný obecný trend přesouvat vymáhání subjektivních práv od jejich skutečných rušitelů (tj. od individuálních uživatelů) právě k poskytovatelům služeb, jejichž prostřednictvím k porušování těchto práv dochází, respektive která protiprávní jednání technicky zprostředkovávají[25].

V oblasti kybernetické bezpečnosti se fenomén definičních autorit rovněž projevuje zásadním způsobem, a to osobní působností příslušných právních předpisů. Povinnosti plynoucí z potřeby chránit kritické informační funkcionality státu resp. národní informační a komunikační infrastrukturu nejsou v tomto případě vůbec ukládány koncovým uživatelům, ale směřují ve velké míře na poskytovatele služeb resp. na správce zájmových systémů a sítí[26].

V tomto směru je možno vidět i další podstatný rozdíl mezi právní úpravou krizového řízení a kybernetickou bezpečností, neboť v případě krizového řízení může právní úprava bezprostředně dopadat na libovolné fyzické či právnické osoby. Rozsah osobní působnosti právní úpravy kybernetické bezpečnosti naproti tomu nepočítá s dopadem na nikoho jiného, než jsou právě poskytovatelé služeb - v případě české právní úpravy jde konkrétně o poskytovatele služeb elektronických komunikací[27].

Posledním základním rysem právní úpravy kybernetické bezpečnosti, který z ní činí specifický regulatorní fenomén, je značná míra konvergence soukromého a veřejného zájmu. Obecně bývá obvyklé, že v případě zájmu

[24] Obsáhlé zmapování aktuální české, slovenské i zahraniční rozhodovací praxe přináší publikace Husovec, M. *Zodpovednosť na internete podľa českého a slovenského práva*, Praha: CZ.NIC, 2014, ke stažení on-line na adrese http://knihy.nic.cz/files/nic/edice/Zodpovednost_web_FINAL.pdf.

[25] Důsledkem tohoto trendu jsou naneštěstí i některé extrémní právní konstrukce, jako např „třikrát a dost“ v zákoně HADOPI – srov. např. working paper Dejean, S., Pénard, T., Suire, R. *Une première évaluation des effets de la loi Hadopi sur les pratiques des Internautes français*, Rennes: CREM, ke stažení on-line na adrese http://www.01net.com/genere/article/fichiersAttaches/300415066.pdf.

[26] Správcem je pro potřeby zákona č. 181/2014 Sb. analogicky s definicí obsaženou v zákoně č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, subjekt, který určuje účel provozu příslušného informačního systému nebo sítě – povinnosti pak zákon stanoví právě jemu. K tomuto přístupu viz např. Berejka, M. A Case for Government Promoted Multi-Stakeholderism, *Journal on Telecommunications and High-Tech Law*, roč. 10, str. 9.

na ochraně tzv. nedistributivních[28] práv je výsledná právní úprava konfliktní se soukromým zájmem resp. s distributivními právy osob[29]. Vzájemné vyvážení soukromého a veřejného zájmu je v takových případech nezřídka otázkou právní a politické alchymie[30]. Pokud však má právní úprava nedistributivního práva jako v případě českého zákona o kybernetické bezpečnosti pouze základní rozsah, je hodnotově konzistentní s tím, co lze označit za tvrdé jádro ústavy[31], a navíc má na distributivní práva jen minimální dopad, dochází k výjimečně nekonfliktní situaci[32].

Jestliže tedy můžeme konstatovat, že naše právní úprava kybernetické bezpečnosti není zásadně konfliktní ve vztahu k distributivním právům, je to dáno především skutečností, že omezení, která reálně přináší, jsou v porovnání s důležitostí chráněných zájmů jen nepatrná. Nejzávažnějším bezprostředním zásahem do distributivních práv je v tomto případě zásah do práva vlastnického, neboť povinným subjektům může vzniknout

---

[27] Takto široký rozsah působnosti zákona uplatní se navíc pouze ve výjimečném případě vyhlášení stavu kybernetického nebezpečí. Za standardní situace běžného fungování systému národní kybernetické bezpečnosti mají konkrétní zákonné povinnosti pouze správci zvlášť určených systémů a sítí (poskytovatelé služeb elektronických komunikací mají pouze povinnost hlásit své kontaktní údaje). K tomu viz § 3 zákona č. 181/2014 Sb., přičemž zákonné povinnosti nad rámec hlášení kontaktních údajů jsou dalšími ust. ukládány pouze subjektům vypočteným v § 3 písm. c) až e) zákona č. 181/2014 Sb. – srov. zejm. § 4 odst. 1 a 2 zákona č. 181/2014 Sb.

[28] Pojem distributivnosti práv je výtečně vyložen v odlišném stanovisku Pavla Holländera k nálezu pléna Ústavního soudu ze dne 3.4.1996, č.j. Pl.ÚS 32/95, 112/1996 Sb., N 26/5 SbNU 215, dostupné z: www.nalus.usoud.cz, následovně: „Ústavní úprava postavení jedince ve společnosti obsahuje ochranu individuálních práv a svobod, jakož i ochranu veřejných statků (public goods, kolektive Gütter). Rozdíl mezi nimi spočívá v jejich distributivnosti. Pro veřejné statky je typické, že prospěch z nich je nedělitelný a lidé nemohou být vyloučeni z jeho požívání. Příklady veřejných statků jsou národní bezpečnost, veřejný pořádek, zdravé životní prostředí. Veřejným statkem se tudíž určitý aspekt lidské existence stává za podmínky, kdy není možno jej pojmově, věcně i právně rozložit na části a tyto přiřadit jednotlivcům jako podíly. (-) Pro základní práva a svobody je, na rozdíl veřejných statků, typická jejich distributivnost. Aspekty lidské existence, jakými jsou např. osobní svoboda, svoboda projevu, účast v politickém dění a s tím spjaté volební právo, právo zastávat veřejné funkce, právo sdružovat se v politických stranách atd., lze pojmově, věcně i právně členit na části a tyto přiřadit jednotlivcům."

[29] V obecné rovině se tomuto fundamentálnímu konfliktu věnuje např. Ronald Dworkin v práci Dworkin, R. *Justice for Hedgehogs*, London: Belknap Press, 2011.

[30] Z institucionálního hlediska se tomuto problému věnuje např. text Kelly, T. K., Hunker, J. Cyber Policy: Institutional Struggle in a Transformed World, *I/S: Journal of Law and Policy*, roč. 8, číslo 2, str. 210 a násl.

[31] K pojmu viz např. Höllander, P. Materiální ohnisko ústavy a diskrece ústavodárce, *Právník*, roč. 2005, č. 4, str. 318.

[32] Viz Powell, B. Is Cybersecurity a Public Good? Evidence From the Financial Services Industry, *Journal of Law, Economics and Policy*, roč. 1, číslo 2, str. 497.

povinnost investovat své prostředky do zabezpečení vlastní informační a komunikační infrastruktury.

Jak vyplynulo z jednání vedoucích k přijetí zákona o kybernetické bezpečnosti, jsou tyto investice již standardně povinnými subjekty realizovány – nikoli sice z důvodu jejich zájmu na zajištění národní kybernetické bezpečnosti, ale z čistě zištného zájmu na ochraně vlastních systémů před kybernetickými bezpečnostními incidenty. Ve většině případů tedy bude nutno ze strany povinných subjektů investovat pouze do komponent zajišťujících komunikaci s národním nebo vládním CERT resp. dokumentaci odpovídající zákonnému standardu[33].

3. PRINCIPY ČESKÉ A EVROPSKÉ PRÁVNÍ ÚPRAVY KYBERNETICKÉ BEZPEČNOSTI

V právu EU je specifická právní úprava kybernetické bezpečnosti v současné době ve stadiu návrhů základních normativních právních aktů[34], zatímco v České republice již je komplex zákona a podzákonných normativních právních aktů již účinný. Přestože vznikala nezávisle na sobě, sdílejí obě legislativní řešení stejnou regulatorní strategii a z jejich struktury lze rovněž vyčíst prakticky obdobný systémový základ. Důvodová zpráva k zákonu o kybernetické bezpečnosti shrnuje tyto principy následovně[35]:

1. Princip technologické neutrality[36] – na základě toho principu, jehož jedním z rozměrů je i tzv. síťová neutralita, dochází ke striktnímu

[33] Není v tomto směru žádným tajemstvím, že naše podzákonná úprava konkrétních náležitostí bezpečnostních opatření a jejich dokumentace vychází ze široce akceptovaného standardu organizačních norem v oblasti informační bezpečnosti z rodiny ISO 27k. Kritickou analýzu těchto standardů viz např. v příspěvku Vorobiev, V. I., Fedorchenko, L. N., Zabolotsky, V. P., Lyubimov, A. V. Ontology-based analysis of information security standards and capabilities for their harmonization, in *Proceedings of the 3rd international conference on Security of information and networks*, New York: ACM, 2010, str. 137 a násl.

[34] Viz zejm. dokumentaci k návrhu směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii - COM(2013)0048 – C7-0035/2013 – 2013/0027(COD).

[35] Ze srovnání např. se strategií legislativy ke kybernetické bezpečnosti USA plynou základní rozdíly právě ve volbě jejích určujících principů – relativně větší úspěch českého resp. evropského legislativního přístupu ukazuje, že tento zřejmé více odpovídá aktuálnímu stavu politického a společenského diskursu. K tomu srov. např. Grant, J. Will there Be Cybersecurity Legislation? *Journal of National Security Law & Policy*, roč. 4, str. 103 a násl.

[36] K původnímu významu tohoto pojmu viz např. Balabanian, N. Presumed Neutrality of Technology, *Society*, roč. 17, číslo 3, str. 7.

oddělení obsahu komunikace od technologií používaných pro jeho ukládání nebo přenos. Informační a komunikační technologie jsou tedy neutrální vzhledem ke způsobu, kterým jsou používány. Důležitým aspektem technologické neutrality je rovněž nezávislost právního regulačního rámce na konkrétní technologii – právní regulace je tedy důsledně neutrální vůči produktům různých dodavatelů (žádný z nich nepreferuje ani nevylučuje).

2. Princip ochrany informačního sebeurčení člověka[37] – informační sebeurčení člověka zahrnuje nejrůznější základní informační práva, z nichž pro kybernetickou bezpečnost jsou důležité především právo na ochranu soukromí, právo na ochranu osobních údajů, právo na svobodný přístup k informacím a právo na přístup ke službám informační společnosti (to vychází ze skutečnosti, že v dnešní době nelze žít plnohodnotný soukromý život bez toho, aby měl člověk možnost tyto služby využívat)[38].
3. Princip ochrany nedistributivních práv[39] – v tomto případě jde především o ochranu národní bezpečnosti a specificky pak o ochranu bezpečnosti prostředí, v němž dochází k realizaci informačních transakcí (k tomu podrobněji viz dole).
4. Princip minimalizace státního donucení – v případě návrhu právní úpravy jde především o implementaci výstupního kritéria třetího prvku testu proporcionality[40], v němž je nutno hodnotit, zda je zásah do lidské svobody proveden jen v nezbytně nutné míře. Konkrétně jde o svobodu povinných subjektů volně užívat předmět

[37] Dokonce i v odborné literatuře převažuje přesvědčení, že kybernetická bezpečnost je v kontrapozici k základním informačním právům – srov. např. Nojeim, G. T. Cybersecurity and Freedom on the Internet, *Journal of National Security Law & Policy*, roč. 4, str. 118 a násl. Ve skutečnosti je však ochrana základních práv jediným skutečným a legitimním smyslem a účelem kybernetické bezpečnosti. To mimo jiné reflektuje i aktuální praxe a agendě ochrany základních práv Valného Shromáždění OSN – srov. např. zprávu Zvláštního zpravodaje Valného shromáždění OSN č. A/HRC/17/27 – stejný názor ve vztahu k právu na soukromí viz např. v článku Bambauer, D. Privacy versus Security, *The Journal of Criminal Law & Criminology*, roč. 103, číslo 3, str. 667.

[38] Podrobněji viz Polčák, R. *Internet a proměny práva*, Praha: AUDITORIUM, 2012, str. 326.

[39] Srov. Powell, B. J. Is Cybersecurity a Public Good? Evidence from the Financial Services Industry, *Journal of Law, Economics and Policy*, roč. 1, číslo 2, str. 497 a násl.

[40] Do našeho právního řádu byl tento test zaveden kontinuální řadou rozhodnutí Ústavního soudu, z nichž můžeme vybrat rozhodnutí ze dne 12. 10. 1994, sp.zn. Pl. ÚS 4/94 nebo ze dne 21. 3. 2002, sp.zn. III. ÚS 256/01. K pojmu a metodě viz též např. viz Alexy, R. On the Structure of Legal Principles. *Ratio Iuris.* 2000, roč. 13, č. 3, str. 1 a násl. nebo Holländer, P. *Filosofie práva*. Plzeň: Aleš Čeněk, 2006, str. 158 a násl.

jejich vlastnického práva (tj. jejich informační a komunikační infrastrukturu). Ve vztahu k člověku se návrh v tomto směru omezuje prakticky dokonale, neboť uživatelům služeb informační společnosti vůbec nezasahuje do jejich práv (zákon se netýká informačních práv uživatelů, nezasahuje do jejich soukromí ani jim neukládá žádná jiná omezení či povinnosti).

5. Princip autonomie vůle regulovaných subjektů – tento princip se týká metody právní regulace a projevuje se stanovením cílových parametrů bez toho, aby právotvůrce nutil regulované subjekty k nějakému specifickému konkrétnímu řešení (subjekty si tedy volí způsob, jak cílového stavu dosáhnout v podmínkách, v nichž samy působí).
6. Princip bdělosti ve vztahu k ostatním státům a k mezinárodnímu společenství – tento princip označovaný v mezinárodním právu veřejném jako due dilligence[41] týká se odpovědnosti státu za mezinárodně škodlivé následky jednání, k němuž dojde pod jeho suverénní jurisdikcí (viz dále).

Za zvláštní pozornost stojí především princip ochrany nedistributivních práv směřující především k ochraně infrastruktury tvořené službami informační společnosti. Nedistributivní charakter bezpečnosti je v tomto případě dán skutečností, že tuto hodnotu nelze distribuovat, tj. nelze konstatovat, že z její existenci přímo plynou konkrétní práva jednotlivým subjektům. Namísto toho má bezpečnost celostní charakter (jde o ochranu prostředí jako celku) a práva k jeho ochraně vykonává výlučně stát podobně, jako je tomu např. v případě národní bezpečnosti nebo ochrany životního prostředí.

Je v tomto směru nutno zdůraznit, že bezpečnost obecně (tj. vč. kybernetické bezpečnosti) nepředstavuje hodnotu či relevantní zdroj legitimity právních norem sama o sobě. Jedná se jako u ostatních nedistributivních principů o akcesorický institut, jehož legitimita není dána přímo ale prostřednictvím primárních principů, k jejichž ochraně směřuje. Nelze tedy hovořit pouze o bezpečnosti bez dalšího resp. nelze jí per se odůvodňovat vznik nových právních povinností nebo obecně jakékoli

[41] Srov. Hessbruegge, J. A. *The Historical Development of the Doctrines of Attribution and Due Dilligence in International Law*.

zásahy do svobody subjektů. Bezpečnost jako taková pak nemůže být ani ve struktuře proporcionality přímo poměřována s ostatními (distributivními) právními principy jako např. s právem na vlastnictví, právem na svobodu projevu nebo právem na práci. Namísto toho je třeba vždy řešit otázku, co je bezpečností chráněno, tj. jaká primární hodnota resp. jaký primární princip je příslušnými konkrétními bezpečnostními instituty zajištěn[42].

Dominantním motivem české právní úpravy je tedy v tomto směru právo na informační sebeurčení[43]. To vychází genericky z práva na soukromý život, tj. práva člověka na hodnotnou osobní existenci, a to jak vzhledem k vlastní integritě (důstojnosti), tak i vzhledem k možnostem zapojení do společnosti. Komponentou informačního sebeurčení, která s rostoucí penetrací běžného života službami informační společnosti nabyla na zásadní důležitosti, je ochrana soukromí, z níž se ještě v poslední době specificky vydělila ochrana osobních údajů[44]. Bezpečnost této pasivní komponenty informačního sebeurčení má především charakter jistoty člověka ohledně rozumné míry zabezpečení soukromé informační sféry před násilnými vnějším vlivy.

Aktivní komponentou informačního sebeurčení, která má vzhledem ke kybernetické bezpečnosti přinejmenším srovnatelný význam jako ochrana soukromí a osobních údajů, je právo na komunikaci. Jeho podstatou je předpoklad, že člověk nemůže vést plnohodnotný soukromý život bez toho, aby měl možnost běžným způsobem interagovat s okolním světem, tj. především komunikovat formou, která je v příslušných sociokulturních reáliích obvyklá[45]. V aktuálních podmínkách je tak tuto komponentu

---

[42] Ke smyslu kybernetické bezpečnosti jako ochrany informačních práv člověka viz např. Polčák, R. Vygum v kyberprostoru: Právní problémy české a evropské kybernetické bezpečnosti. In Haňka, R., Kaplan, Z., Matyáš, V. Mikulecký, J. Říha, Z. *Information Security Summit 2011*. 1. vyd. Praha: Data Security Management, 2011, str. 159-165.

[43] Pojem informačního sebeurčení byl do právní praxe zaveden rozhodnutím Ústavního soudu Spolkové republiky, které se týkalo připravovaného sčítání lidu a jehož předmětem bylo primárně proporcionální vymezení informačního soukromí člověka. Viz nález Spolkového ústavního soudu ze dne 15. 12. 1983, č.j. BVerfGE 65, 1 [on-line]. Dostupné z: <www.thm.de/datenschutz/images/stories/volkszaehlungsurteil_bverfger_1983.pdf>.

[44] Srov. např. Mates, P. *Ochrana soukromí ve správním právu*. Praha : Linde Praha, 2006, str. 14. Pojmu soukromí se v českém právu věnuje jen minimum kvalitní doktrinální literatury – světlými výjimkami jsou např. sborník Šimíček, V. (ed.) *Právo na soukromí*. Brno : Mezinárodní politologický ústav, 2011 nebo monografie Matejka, J. *Internet jako objekt práva – hledání rovnováhy autonomie a soukromí*, Praha: CZ.NIC, 2013, k dispozici též on-line ke stažení na adrese https://knihy.nic.cz/files/nic/edice/jan_matejka_ijop.pdf.

informačního sebeurčení možno přeložit jako právo na přístup k (fungujícím) službám informační společnosti[46].

Právě uvedené samozřejmě neznamená, že by stát měl povinnost zajistit všem subjektům dodávky služeb informační společnosti nebo že by uvedené služby měly být s garancí státu poskytovány bezplatně. Stát má však v situaci, kdy jsou tyto služby běžnou součástí soukromého lidského života, povinnost garantovat jejich dostupnost a na nejvyšší úrovni též jejich funkčnost. To v tomto případě mimo jiné znamená též povinnost státu zabezpečit tyto služby tak, aby mohly být poskytovány a konzumovány bez obav o jejich bezpečnost. Z právě uvedeného tedy plyne, že jen bezpečné služby informační společnosti mohou dát člověku prostor k nerušené realizaci jeho práva na informační sebeurčení.

S právě uvedeným též souvisí jiný princip, který český návrh nijak zvlášť nezdůrazňuje, ale který má ve vztahu ke kybernetické bezpečnosti rovněž zásadní význam, tj. princip svobody projevu. Na rozdíl od informačního sebeurčení se v tomto případě jedná namísto aktivní soukromé komunikace o zabezpečení možnosti veřejně vyjádřit svůj názor a případně se účastnit obecného společenského nebo politického diskursu. Stejně jako v případě informačního sebeurčení je přitom možno konstatovat, že pouze bezpečně

[45] Skutečnost, že soukromí člověka tvoří i možnost komunikovat s okolím, zdůraznil náš Ústavní soud, přičemž původně poukázal především na nutnost ochrany informačních vztahů v rámci rodiny. Doslova k tomu uvedl: „Právo na ochranu osobního soukromí je právem fyzické osoby rozhodnout podle vlastního uvážení zda, popř. v jakém rozsahu a jakým způsobem mají být skutečnosti jejího osobního soukromí zpřístupněny jiným subjektům a zároveň se bránit (vzepřít) proti neoprávněným zásahům do této sféry ze strany jiných osob. Přílišná akcentace pozitivní složky práva na ochranu soukromého života vede k neadekvátnímu zúžení ochrany pouze na to, aby skutečnosti soukromého života fyzické osoby nebyly bez jejího souhlasu či bez důvodu uznávaného zákonem a tak nebyla narušována integrita vnitřní sféry, která je pro příznivý rozvoj osobnosti nezbytná. Ústavní soud nesdílí toto zúžené pojetí, neboť respektování soukromého života musí zahrnovat do určité míry právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi.“ – viz nález Ústavního soudu ze dne 1. 3. 2000, č.j. II. ÚS 517/99, N 32/17 SbNU 229.

[46] Ústavní soud se k této otázce vyjádřil v nálezu ze dne 07.04.2010, č.j. I.ÚS 22/10 následovně: „Lze dovodit, že člověk tak bývá netoliko objektem společenských ‚poměrů‘, ale stává se i objektem práva, je-li nucen podrobovat se mu zcela při jeho interpretaci a aplikaci, tj. bez zohlednění jeho individuálních zájmů, resp. základních práv. Vedle subjektivních faktorů na straně jednotlivce je při posuzování ‚obvyklosti, resp. oprávněnosti‘ výdaje třeba vzít v úvahu i faktory objektivní, mezi ty mimo jiné patří technologický vývoj (např. mobilní telefony, internet) a s ním související změny ve způsobech komunikace, získávaní informací, styku s úřady, sdružování apod., resp. vývoj technologií, skrze niž je realizováno právo jednotlivce na osobní rozvoj, vztahy s ostatními lidmi a vnějším světem, tedy právo na soukromý život.“

fungující služby informační společnosti mohou k takové účasti poskytnout adekvátní prostor[47].

Ostatní shora uvedené principy mají ve struktuře navrhované právní úpravy spíše implementační charakter. Princip technologické neutrality zdůrazněný hned na prvním místě týká se především skutečnosti, že česká právní úprava směřuje k zajištění funkčnosti informační a komunikační infrastruktury bez toho, aby se týkala komunikovaného obsahu[48]. Právní povinnosti subjektů ani pravomoci založené zákonem Národnímu bezpečnostnímu úřadu se tedy z podstaty nemohou týkat informací tvořících obsah komunikace prostřednictvím služeb informační společnosti. Dalším aspektem technologické neutrality je v tomto případě skutečnost, že povinné technické standardy ani technická řešení přímo implementovaná na národní úrovni nebudou zvýhodňovat nebo upřednostňovat žádnou konkrétní proprietální technologii[49].

Princip autonomie vůle regulovaných subjektů a princip minimalizace státního donucení vztahují se především k osobní působnosti, rozsahu a míře obecnosti konkrétních právních povinností definovaných právní úpravou. Ta je minimalistická v tom směru, že se vztahuje pouze na omezený okruh subjektů, přičemž míra zátěže těchto subjektů specifickými povinnostmi odpovídá důležitosti jimi spravovaných systémů a míře jejich bezpečnostní expozice.

Zohlednění maximální autonomie vůle při formulaci povinností pro subjekty spadající do osobní působnosti zákona má aspekt liberální i pragmatický. Inkorporace tohoto principu je pro regulované subjekty přirozeně příznivá, neboť jim poskytuje maximální volnost při implementaci příslušných povinností.

---

[47] Kybernetická bezpečnost se stala i jedním z ústředních motivů zprávy Zvláštního zpravodaje Valného shromáždění OSN k zásadním problémům práva na svobodu projevu – viz kap. IV., část E, Report of the Special Rapporteur on thepromotion and protection of the right to freedom of opinion and expression, Frank La Rue, č. A/HRC/17/27, ke stažení on-line na adrese www.ohchr.org.

[48] K tomu srov. např. Yoo, C. S. Network Neutrality and the Economics of Congestion. *Georgetown Law Journal*, roč. 94, str. 1847 a násl.

[49] K důležitosti tohoto principu vzhledem k fungování síťových efektů, na nichž je prakticky založen další rozvoj naší kultury v nejširším smyslu slova, viz např. Zittrain, J. The Generative Internet. *Harvard Law Review*, roč. 119, str. 1974.

Vedle toho tento princip zohledňuje i značnou rozmanitost informačních sítí a systémů, jichž se dotýká. Pokud by byla úprava rigorózní co do specifikace konkrétních povinností, znamenalo by to buďto definovat nespočet variant dle rozsahu a funkcí příslušných sítí a systémů nebo pracovat s předpokladem, že standardní zákonné varianty budou vyhovovat co do efektivity vynaložených investic pouze některým subjektům – to by v konečném důsledku vedlo na jedné straně k tomu, že by byly některé subjekty nuceny investovat prostředky do bezpečnostních opatření, která by byla vzhledem k charakteru příslušných systémů přehnaně rozsáhlá a jiné subjekty by naopak ani při splnění zákonných požadavků neochránily svoji infrastrukturu v dostatečném rozsahu. Namísto toho volí zákon stanovení cílového stavu, tj. požadované úrovně funkčnosti bezpečnostních opatření, přičemž ponechává regulovaným subjektům relativní volnost ve volbě konkrétních nástrojů pro jeho dosažení. To ostatně odpovídá i jedné ze shora zmíněných komponent principu technologické neutrality, neboť zákonné podmínky lze splnit nespočtem typů různých bezpečnostních řešení založených na technologiích od různých vzájemně si konkurujících dodavatelů.

Druhým aspektem autonomie vůle je možnost dobrovolné spolupráce soukromoprávních subjektů stojících mimo osobní působnost zákona s národním dohledovým pracovištěm. Přestože se tato zákonná konstrukce jeví být na první pohled absurdní, lze o tuto formu spolupráce očekávat velký zájem především mezi subjekty, které jsou předmětem zvýšené bezpečnostní expozice, ať už jde o aktivistické útoky na jejich infrastrukturu, konkurenční boj, průmyslovou špionáž apod. Spoluprací s národním dohledovým pracovištěm mohou tyto subjekty získat nejen přehled o tom, jaká je v reálném čase bezpečnostní situace v české informační a komunikační infrastruktuře (a tím i schopnost reagovat na aktuální kybernetické hrozby v předstihu), ale mohou získávat i průběžnou metodickou a koordinační pomoc při řešení kybernetických bezpečnostních incidentů. Nadto bude pro subjekty nabízející služby informační společnosti představovat dobrovolná spolupráce s národním dohledovým pracovištěm přidanou hodnotu, kterou budou moci prezentovat svým klientům.

Z hlediska povinných soukromoprávních subjektů však má inkorporace principu autonomie vůle též jeden problematický aspekt. Právní úprava

totiž nepočítá s tím, že by měly povinnost nechat si ex ante schvalovat nebo nějak potvrzovat vlastní řešení kybernetické bezpečnosti vzhledem ke splnění standardních zákonných požadavků. Především u středních a velkých podniků a veřejnoprávních korporací investujících podstatné prostředky do rozvoje své informační a komunikační infrastruktury je přitom stěžejní otázkou tzv. compliance, tj. ex ante kontrolovaného plnění zákonných požadavků příslušné jurisdikce. Je totiž z ekonomického hlediska neúčelné pro tyto subjekty investovat do rozvoje vlastní infrastruktury určité prostředky a přitom nemít jistotu, že tyto investice negenerují nějaké právní riziko[50]. Skutečnost, že zákon ve své struktuře neobsahuje explicitní povinnost certifikace nebo jiného schválení příslušných technických a organizačních řešení tedy je na první pohled pro regulované subjekty příznivá, neboť jim nevznikají další náklady spojené se schvalovacími procesy. Středním a velkým povinným subjektům však může způsobit zvýšení míry rizikovosti jejich investic do informační a komunikační infrastruktury, neboť neposkytuje ex ante jistotu, že jimi implementovaná bezpečnostní řešení skutečně bezezbytku plní zákonné požadavky. Nabízí se samozřejmě řešení formou regresní odpovědnosti dodavatelů – takové řešení však již není otázkou compliance a pro střední a velké subjekty představuje jen těžko postižitelné právní a ekonomické riziko[51].

Princip bdělosti ve vztahu k mezinárodnímu společenství a ostatním suverénním státům se v navrhované právní úpravě projevuje už samotnou skutečností, že se Česká republika snaží při vynaložení podstatného úsilí dostat pod kontrolu bezpečnostní problémy vyskytující se pod její jurisdikcí. Obecně totiž tento princip zakládá odpovědnost státu za škodlivé následky způsobené ostatním státům v důsledku porušení mezinárodního práva veřejného v situacích, kdy stát mohl takovému porušení zabránit.

V situaci, kdy je infrastruktury na území státu zneužito k provedení kybernetického útoku s dopady v zahraničí, mají postižené státy a mezinárodní společenství důvod ptát se, zda škodlivým následkům nebylo možno zabránit. Existují-li popsané způsoby, jak předejít kybernetickým

[50] Srov. Weill, P., Woodham, R. Don't Just Lead, Govern: Implementing Effective IT Governance. *MIT Sloan Working Paper No. 4237-02*, 2002, dostupné on-line na adrese http://ssrn.com/abstract=317319.

[51] Podrobněji k tomuto problému viz dále.

útokům resp. zneužití informační a komunikační infrastruktury, a kdy je implementace nejrůznějších bezpečnostních opatření nejen technicky možná ale též ekonomicky a sociálně akceptovatelná, pak má stát typu České republiky nikoli pouze právo ale přímo povinnost řešit svou vlastní kybernetickou bezpečnost[52].

4. INSTITUTY ČESKÉHO PRÁVA KYBERNETICKÉ BEZPEČNOSTI

Před výkladem k jednotlivým institutům je nutno vyjádřit se ke třem populárním mýtům vztahujícím se k právu kybernetické bezpečnosti. První z nich týká se smyslu a účelu specifické legislativy a je založen na předpokladu, že právní předpis upravující práva a povinnosti k zajištění národní kybernetické bezpečnosti má ve svém textu obsahovat pro jednotlivé zainteresované subjekty komplexní návod na to, jak se správně chovat respektive důkladný popis toho, co je zakázáno. Zvláštní zákon upravující oblast národní kybernetické bezpečnosti však nemá a ani nemůže sloužit jako kuchařka – namísto toho má pouze v minimální formě upravit specifické povinnosti povinným subjektům a dále pak založit kompetence institucím, do jejichž působnosti tato oblast spadá. Je přitom třeba vycházet nikoli z předpokladu, že všem zainteresovaným je třeba zákonem detailně a nekompromisně sdělit, co mají nebo nemají dělat, ale že:

1. právo není jen zákon – konkrétní obsah zákonných povinností nebývá nutně specifikován pouze zákonem, ale může být též např. otázkou judikatury či aplikace obecných či zvláštních právních principů. Z toho mj. plyne i skutečnost, že zákon může zůstat relativně rigidní, ale obsah platného práva se může v čase výrazně měnit[53],
2. soukromým subjektům mají být zákonem stanoveny pouze konkrétní příkazy nebo zákazy – dovolené jednání není třeba

[52] Tato doktrína je ještě na počátku svého vývoje, ale lze při mírném optimismu předpokládat její brzké uplatnění v praxi – viz Glennon, M. The Dark Future of International Cybersecurity Regulation, *Journal of National Security Law and Policy*, roč. 6, str. 563.

[53] Výmluvně to ilustruje Gustav Radbruch v článku Zákonné neprávo a nadzákonné právo původně publikovaným jako Radbruch, G. Gesetzliches Unrecht und übergesetzliches Recht, *Süddeutsche Juristenzeitung*, roč. 1946, str. 105–108.

vymezovat, neboť tyto subjekty mohou činit vše, co jim zákon nezakazuje[54],

3. orgánům veřejné moci má zákon vymezit působnost, stanovit povinnosti a možnosti autoritativního jednání (orgány veřejné moci mohou totiž oproti subjektům soukromého práva dělat jen to, co jim zákon výslovně ukládá nebo umožňuje)[55],
4. není vhodné ani potřebné upravovat to, co upravují jiné právní předpisy nebo mezinárodní smlouvy resp. zakládat povinnosti, které jsou již založené jinými částmi našeho právního řádu. Z toho plyne též obecná nutnost strukturovat a formulovat zákon tak, aby do systému platného práva nevnášel redundantní nebo nekoherentní prvky[56],
5. předmětem zákona je právní povinnost a normativními modalitami jsou příkaz, zákaz a dovolení. Co z nějakého důvodu není možné nebo účelné definovat jako právní povinnost prostřednictvím některé z těchto modalit, nemá v psaném právu co pohledávat. Typickým příkladem jsou technické standardy nemající charakter právních povinností a
6. zákon nesmí odporovat Ústavnímu pořádku České republiky – žádná zákonem založená právní povinnost nesmí vybočovat z rámce proporcionality základních práv člověka a nedistributivních práv státu[57].

Z právě uvedeného mimo jiné vyplývá, že právní úprava kybernetické bezpečnosti České republiky není ani zdaleka tvořena jen zákonem o kybernetické bezpečnosti. Povinnosti při ochraně informační a komunikační infrastruktury totiž kromě něj zakládá i řada dalších součástí českého právního řádu. Následující výklad je zaměřen na instituty, které se z hlediska zajištění kybernetické bezpečnosti jeví jako

[54] Viz čl. 2 odst. 3 Listiny základních práv a svobod.

[55] Viz čl. 2 odst. 2 Listiny základních práv a svobod.

[56] V tomto případě jde o komponenty označované právní teorií jako tzv. materiální náležitosti právotvorby normativního typu. K náležitostem i technice české právotvorby viz např. Šín Z.: *Tvorba práva*. Praha: C. H. Beck, 2003.

[57] Proporcionalita je metoda poměřování právních principů, přičemž charakter právních principů mají i všechna ústavně zaručená základní práva. K používání této metody v českém právním prostředí viz učebnici Holländer, P. *Filosofie práva*, 2. Vydání, Plzeň: Aleš Čeněk, 2012.

nejdůležitější z pohledu povinných subjektů. Konkrétně se budeme věnovat otázkám

1. bezpečnostních opatření
2. protiopatření
3. odpovědnosti za nedbalost a prevenčních povinností
4. disciplinární odpovědnosti a disciplinárních povinností

4.1 BEZPEČNOSTNÍ OPATŘENÍ

Bezpečnostní opatření jsou základním kamenem zákona o kybernetické bezpečnosti a z operačního hlediska i jeho zdaleka nejdůležitější součástí[58]. Primárním účelem zákona totiž není řešení jednotlivých kybernetických bezpečnostních incidentů ale vytvoření prostředí, v němž jsou kritická informační a komunikační infrastruktura státu a další zájmové informační systémy a sítě preventivně chráněny tak, že pro ně žádná kybernetická bezpečnostní událost nepředstavuje bezpečnostní riziko.

Zákon sám zavádí povinným subjektům pouze základní povinnost mít bezpečnostní opatření v taxativně vymezených kategoriích, přičemž technické podrobnosti upravuje prováděcí předpis[59]. Zákon je postaven na dokumentačním modelu, tj. ukládá povinným subjektům povinnost především dokumentovat jednotlivé typy bezpečnostních opatření a následně pak dává právo Národnímu bezpečnostnímu úřadu kontrolovat, zda je dokumentace souladná nejen s konkrétními požadavky zákona a prováděcího předpisu, ale samozřejmě též s aktuální skutečností.

Smyslem bezpečnostních opatření je primárně vytvoření takových preventivních mechanismů, které povinným subjektům umožní vyrovnávat se autonomně k kybernetickými bezpečnostními událostmi (ať už jde o prevenci jejich samotného vzniku nebo o nástroje a mechanismy k jejich následnému pokrytí)[60]. Subsidiárně jsou pak bezpečnostní opatření formulována tak, aby jejich zavedení umožnilo efektivní fungování

[58] Zákon je v § 4 odst. 1 vymezuje jako „souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru“.

[59] Viz vyhlášku č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti).

[60] Za tímto účelem dělí zákon bezpečnostní opatření na organizační a technická a ty pak dále specifikuje v ust. § 5 odst. 2 a 3.

kybernetických bezpečnostních struktur na úrovni státu, tj. především národního a vládního dohledového pracoviště.

Systematickým problémem bezpečnostních opatření, kterému jsme se už stručně věnovali výše, je skutečnost, že jsou formulována jako technický a organizační standard, aniž by však zákon předpokládal existenci oficiálních certifikačních nebo jiných a priori procedur použitelných k verifikaci jejich kvality. Povinné subjekty tedy budou investovat do akvizic nebo úprav příslušných bezpečnostních řešení, aniž by měly možnost a priori ověřit, zda to, čím se snaží plnit zákonné požadavky skutečně je nebo není v souladu se zákonem resp. s prováděcím předpisem.

4.2 PROTIOPATŘENÍ

Protiopatřeními pro potřeby tohoto textu souhrnně nazýváme to, co zákon označuje jako „opatření“ a dělí dle typu na varování, reaktivní opatření a ochranná opatření. Všechny typy protiopatření mají povahu vrchnostenské činnosti Národního bezpečnostního úřadu, přičemž varování má charakter informativní a zbývající dvě opatření mají formu závazných individuálních právních aktů resp. opatření obecné povahy.

Institut varování může se zdát na první pohled zbytečným, neboť jeho užití nepřináší bezprostřední imperativ ani riziko přímé sankce[61]. Jeho charakter však vystihuje typický efekt zákona o kybernetické bezpečnosti v otázkách odpovědnosti za kybernetické bezpečnostní incidenty. Zákon totiž ani u imperativních institutů nepřináší žádné přímé drakonické sankce, ale zavádí přímo nebo nepřímo nové typy právních povinností, jejichž neplnění může mít za následek vznik povinnosti nahradit škodu. Povinný subjekt tedy nemůže kalkulovat právní riziko plynoucí z nově založených zákonných povinností pouze ve vztahu k možné pokutě (ta je co do své výše spíše symbolická) ale též vzhledem k velmi neurčitému potenciálu škod, k nimž může dojít v důsledku zaviněného[62] i nezaviněného[63] kybernetického bezpečnostního incidentu.

[61] Viz § 12 ve spojení s § 25 zákona č. 181/2014 Sb.

[62] Odpovědnost je v tomto případě založena na základě obecných ust. § 2910 a násl. zákona č. 89/2012 Sb., občanský zákoník.

[63] V úvahu zde u podnikatelských subjektů připadá povinnost nahradit škodu způsobenou provozní činností na základě § 2924 zákona č. 89/2012 Sb.

V případě varování tedy Národní bezpečnostní úřad sice provádí pouze adresnou osvětu ohledně konkrétních bezpečnostních rizik, ta ale ve svém důsledku vede k prokazatelné informovanosti povinných subjektů. Zprostředkovaně tím přináší povinným subjektům možnost založení povinnosti nahradit škodu způsobenou tím, že na základě varování nepřijmou přiměřená opatření k zabránění vzniku kybernetických bezpečnostních incidentů nebo zmírnění jejich následků[64].

V typickém případě tedy bude Národní bezpečnostní úřad formou varování informovat o konkrétním bezpečnostním riziku (např. o tzv. bezpečnostní díře) – jestliže povinné subjekty nebudou na základě této informace za vynaložení přiměřeného úsilí na takto identifikované riziko reagovat (např. instalací záplat) a v důsledku toho dojde ke škodě u třetích osob, mohou třetím osobám povinné subjekty přímo odpovídat z titulu nesplnění prevenční povinnosti. Je-li pak v této situaci způsobena škoda i samotnému povinnému subjektu, může být shora popsaný nedostatek reakce na varování též důvodem pro pojišťovnu, aby odmítla nebo výrazně snížila hodnotu pojistného plnění.

Z hlediska povinných subjektů tedy přináší i na první pohled bezzubý institut varování nový typ právního rizika, které je a priori jen velmi těžko ohodnotitelné – čím větší je přitom povinný subjekt a čím více spravuje systémů spadajících pod rozsah zákona o kybernetické bezpečnosti, tím je toto riziko závažnější, a to co do své potenciální hodnoty i do míry nepředvídatelnosti svého výskytu. Dokonce lze s trochou nadsázky konstatovat, že s rostoucí velikostí můžeme sledovat u povinných subjektů klesající míru zájmu o přímé sankce zákona o kybernetické bezpečnosti (tj. o pokuty) a naopak rostoucí zájmovost nepřímých sankcí ve formě právě popsaného potenciálu povinností k náhradě škody resp. limitace pojistného plnění[65].

Další dva typy protiopatření již disponují v porovnání s varováním též přímou možností autoritativního vynucení. Zákon definuje jejich věcný rozsah velmi široce - prakticky jde o jakákoli opatření „k řešení kybernetického bezpečnostního incidentu anebo k zabezpečení

[64] K tomu srov. § 2901 zákona č. 89/2012 Sb.

[65] K nim ještě přistupují jen těžko vyčíslitelné náklady spojené s případnou kontrolou a realizací adresně uložených opatření k nápravě ve smyslu § 24 zákona č. 181/2014 Sb.

informačních systémů nebo sítí a služeb elektronických komunikací před kybernetickým bezpečnostním incidentem“[66]. V tomto směru ale nelze na rozdíl od některých bulvárních názorů uvažovat o tom, že by takto široce definovaná věcná působnost příslušných správních rozhodnutí nebo opatření obecné povahy dávala Národnímu bezpečnostnímu úřadu do rukou nějaký totalitní nástroj ke kontrole národní informační a komunikační infrastruktury. Vedle konkrétního omezení smyslem a účelem protiopatření (resp. reaktivních nebo ochranných opatření) je v tomto případě Národní bezpečnostní úřad standardně omezen působností zákona a dále pak obecnými principy správního práva, z nichž nejdůležitějšími jsou zřejmě principy dobré správy[67] a zákaz svévole.

V rovině ústavního práva pak je Národní bezpečnostní úřad omezen především judikatorní doktrínou tzv. omezeného testu proporcionality[68]. Národní bezpečnostní úřad má tedy implicitní povinnost vybrat pro příslušné reaktivní nebo ochranné opatření takovou alternativu, která bude povinné subjekty nejméně zatěžovat.

Imperativní protiopatření zákon dělí z hlediska jejich účelu na reaktivní a ochranná. První jmenovaný typ se uplatní v případech hrozícího nebo probíhajícího konkrétního kybernetického bezpečnostního incidentu. Tomu odpovídá i procesní charakteristika reaktivních protiopatření zahrnující ve správním právu spíše výjimečné instituty okamžité vykonatelnosti a absence odkladného účinku řádného opravného prostředku (v tomto případě rozkladu)[69].

Okamžitost a bezprostřednost imperativního účinku reaktivních protiopatření odpovídá jejich charakteru jakožto bezpečnostních nástrojů výkonné moci. Přestože bylo nutno z hlediska procesní formy dostát požadavkům správního práva na dokonalý proces autoritativní aplikace, je zřejmé, že v tomto případě nejde o klasickou exekutivní aplikaci práva, ale spíše o konkrétní vrchnostenský zásah vedoucí k pokrytí okamžité

[66] Viz § 13 odst. 1 zákona č. 181/2014 Sb.

[67] K pojmu viz např. Košičiarová, S. *Princípy dobrej verejnej správy a Rada Európy,* Bratislava: Iura Edition, 2012, 556 s.

[68] Jako omezený test proporcionality označuje se výstupní část standardního testu proporcionality, která spočívá v hodnocení míry zásahu do zájmu chráněného právním principem. Platí přitom, že zásah do práv osoby nesmí být větší, než je vzhledem k okolnostem pragmaticky nutné – srov. Holländer, P. *Filosofie práva*, 2. Vydání, Plzeň: Aleš Čeněk, 2012.

[69] Srov. § 15 zákona č. 181/2014 Sb.

bezpečnostní hrozby. Připodobnit jej lze namísto jiných procesů, na jejichž konci stojí vykonatelné správní rozhodnutí (resp. opatření obecné povahy), spíše k okamžité akci bezpečnostní složky výkonné moci, tj. např. k fyzickému zásahu policie[70].

V tomto případě však z podstaty věci plyne, že Národní bezpečnostní úřad nemá možnost provést takový zásah autonomně[71]. Exekutivní reakce k zajištění národní kybernetické bezpečnosti tedy v tomto případě nemůže mít povahu přímé akce bezpečnostní složky státu, ale pouze vrchnostenského imperativu vedoucího k akci subjektu, o jehož informační systém nebo síť se jedná. Nemaje ve správním právu jiného použitelného institutu, sáhl tedy v tomto případě právotvůrce logicky po institutu správního rozhodnutí resp. opatření obecné povahy.

Ochranná opatření mají naproti tomu svou náturou blíže ke klasickému správnímu rozhodování resp. k vrchnostenské podzákonné normotvorbě, neboť jde o imperativy, jejichž implementace, lidově řečeno, až tak nehoří. Jejich podkladem jsou rovněž konkrétní kybernetické bezpečnostní incidenty, ale jejich smyslem a účelem není bezprostřední reakce, nýbrž zvýšení úrovně bezpečnosti příslušných informačních systémů a sítí[72]. Především v případech, kdy jsou ochranná opatření vydávána formou opatření obecné povahy neurčitému okruhu adresátů je lze vlastně z funkčního hlediska považovat za doplněk podzákonného předpisu konkretizujícího obsah bezpečnostních opatření.

4.3 ODPOVĚDNOST ZA NEDBALOST A PREVENČNÍ POVINNOSTI

Přestože sám zákon o kybernetické bezpečnosti se tomuto typu odpovědnosti z pochopitelných důvodů vůbec nevěnuje, představuje pro povinné subjekty možnost odpovědnosti za vědomou či nevědomou nedbalost resp. za nesplnění prevenční povinnosti zřejmě nejsilnější právní motivační faktor k faktické realizaci bezpečnostních opatření.

---

[70] Nabízí se zde například srovnání s pravomocemi policie při zajišťování bezpečnosti chráněných prostorů, objektů a osob ve smyslu ust. § 48 odst. 4 zákona č. 273/2008 Sb., o Policii české republiky, ve znění pozdějších předpisů.

[71] K tomu viz shora konstatovaný specificky rys kybernetické bezpečnosti spočívající ve zprostředkovanosti veškerých aktivit službami informační společnosti.

[72] Srov. § 14 zákona č. 181/2014 Sb.

Odpovědnost v tomto případě znamená, jak bylo uvedeno shora, nejen potencialitu povinnosti nahradit škodu způsobenou třetím osobám v důsledku nedbalosti nebo opomenutí preventivního zásahu, ale též srovnatelně důležité riziko krácení nebo ztráty nároku na pojistné plnění u škod na vlastním majetku[73] resp. na vlastní činnosti nebo i riziko subsidiární sankce za nesplnění povinnosti specificky regulovaného odvětví (např. v oblasti energetiky[74]).

K právě uvedeným typům odpovědnostních důsledků lze ještě připočíst riziko prodlení v případech, kdy kybernetický bezpečnostní incident způsobí neschopnost povinného subjektu plnit jiné právní povinnosti. Typicky může například dojít k situaci, kdy má povinný subjekt povinnost dodávat svým odběratelům zboží nebo služby a v důsledku kybernetického bezpečnostního incidentu toho není po nějakou dobu schopen. Za předpokladu, že kybernetický bezpečnostní incident vedl k takovým důsledkům kvůli neschopnosti povinného subjektu splnit si zákonnou povinnost vyplývající ze zákona o kybernetické bezpečnosti, nebude se povinný subjekt moci bránit poukazem na tento incident proti nárokům třetím osob z vadného resp. pozdního plnění.

To samozřejmě neznamená, že by povinné subjekty měly důvod obávat se toho, že budou odpovídat za veškeré škody způsobené třetím osobám kybernetickými bezpečnostními incidenty, na nichž se bude nějakým způsobem podílet jejich nedostatečně zabezpečená informační a komunikační infrastruktura. Ani v případě, byla-li by škoda třetím osobám skutečně způsobena v důsledku zanedbání specifických povinností plynoucích ze zákona o kybernetické bezpečnosti (resp. z jeho imperativních institutů), nejednalo by se ze strany povinného subjektu zřejmě o povinnost výlučnou – tam, kde byla např. v důsledku nedbalosti povinného subjektu zneužita jeho infrastruktura k provedení kybernetického útoku, zkoumal by soud u povinného subjektu míru jeho zavinění resp. míru toho, jak se nedbalá realizace opatření k zajištění

[73] K tomu viz zejm. ust. § 2800 odst. 2 zákona č. 89/2012 Sb.

[74] Vedle pokut či opatření k nápravě může jít též o nebezpečí odnětí licence nebo jiného povolení k výkonu specifické činnosti – tuto možnost dává národním regulátorům úprava např. v oblasti energetiky nebo elektronických komunikací – srov. zákon č. 458/2000 Sb., o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon), ve znění pozdějších předpisů) nebo zákon č. 127/2005 Sb, o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

kybernetické bezpečnosti podílela na celkovém škodním dopadu příslušného kybernetického bezpečnostního incidentu[75].

Za připomenutí stojí v této souvislosti především typologie nedbalostního zavinění sestávající vedle vědomé (tj. hrubé – culpa lata) nedbalosti též z nedbalosti nevědomé (tj. lehké – culpa levis)[76]. Za zaviněné porušení právní povinnosti se tak považují nejen situace, kdy má povinný subjekt prokazatelně k dispozici informace o hrozícím nebezpečí a vlastní liknavostí nezabrání škodlivému následku, ale také případy, kdy povinný subjekt sice těmito informacemi objektivně nedisponuje, ale opatřit si je měl a mohl. Ve vztahu ke shora zmíněnému institutu varování to mimo jiné znamená, že ze strany povinného subjektu nebude možno namítat například nefunkčnost povinně sdělované kontaktní adresy nebo interní komunikační problémy v rámci organizace, kvůli kterým se informace o varování vydaném Národním bezpečnostním úřadem nedostane na správné místo.

Nedbalost nebo nesplnění prevenční povinnosti každopádně nemusí mít, jak bylo naznačeno výše, důsledky pouze soukromoprávní. Řada povinných subjektů působí v odvětví, která mají specifickou a často i poměrně rigorózní správní regulaci – příkladem může být energetika, elektronické komunikace, tzv. jiné utility (odpadové hospodářství, distribuce vody apod.), zdravotnictví nebo potravinářství. Ve většině z těchto odvětví mají povinné subjekty nejen povinnosti vztahující se bezprostředně k příslušnému typu činnosti, ale též související povinnosti, z nichž podstatná část se může přímo nebo nepřímo týkat provozu vnitřních informačních systémů nebo komunikačních sítí. Pokud v takovém případě dojde k narušení regulované činnosti povinného subjektu v důsledku kybernetického bezpečnostního incidentu, který povinný subjekt nedokázal zvládnout v důsledku nedbalosti nebo porušení prevenční povinnosti, může to pro něj znamenal vedle shora uvedených odpovědnostních rizik též možnost postihu dle specifických pravidel příslušného regulovaného

[75] V tomto případě je specifický charakter kybernetických bezpečnostních incidentů společně s charakterem účasti způsobené nedůslednou ochranou vlastního systému možno obecně považovat za okolnosti hodné zvláštního zřetele a je tedy důvod předpokládat, že povinnost nahradit škodu bude v tomto případě specifikována dle míry zavinění resp. dle míry účasti – k tomu viz § 2915 odst. 2, první věta zákona č. 89/2012 Sb.

[76] Viz např. Knapp, V. Některé úvahy o odpovědnosti v občanském právu. *Stát a právo* I. roč. 1956, str. 66.

odvětví. Není pak v tomto směru žádným tajemstvím, že např. pro subjekty v oboru energetiky může být takový subsidiární sankční postih dle energetického zákona nepoměrně citelnější, než primární sankce plynoucí ze zákona o kybernetické bezpečnosti.

Všechna shora uvedená právní rizika jsou v porovnání s imperativními a sankčními mechanismy zákona o kybernetické bezpečnosti pro povinné subjekty nejen mnohem závažnější, ale také co do svého důsledku mnohem méně předvídatelná. Zatímco lze vcelku snadno odhadnout, jaká výše pokuty hrozí při neprovedení reaktivního protiopatření, jen těžko se dá z pohledu povinného subjektu odhadovat, jaký dopad může mít tatáž situace z pohledu soukromoprávní odpovědnosti vůči poškozeným třetím osobám, jak velká vymahatelná škoda může vzniknout zákazníkům nebo jak bude reagovat regulátor příslušného specifického odvětví (např. Energetický regulační úřad, český telekomunikační úřad apod.)

Velká míra této subsidiární právní rizikovosti ve spojení s absencí oficiálních compliance procedur vytváří na povinné subjekty tlak projevující se v důsledku jednak chvályhodnou vůlí investovat do bezpečnostních opatření, to dokonce často i vysoko nad rámec zákonných požadavků. Kromě toho však může tato nejistota vést k tomu, že se povinné subjekty budou za každou cenu snažit o únik z osobního rozsahu zákona nebo se budou pokoušet o různé ohýbání jeho pravidel. Zabránit tomuto efektu by kromě nezávislých certifikačních procedur mohla též osvětová činnost Národního bezpečnostního úřadu realizovaná ve spolupráci s odvětvovými regulátory nebo rozšíření nabídky pojistných či zajišťovacích finančních produktů. Svou nezastupitelnou roli pak budou jistě hrát i odvětvové organizace, které mohou vedle zprostředkování komunikace mezi povinnými subjekty a Národním bezpečnostním úřadem působit i v rovině vzdělávací, koordinační nebo poradenské.

4.4 DISCIPLINÁRNÍ ODPOVĚDNOST A DISCIPLINÁRNÍ POVINNOSTI

Shora diskutovaná bezpečnostní opatření mají vést k tomu, že povinné subjekty budou mít systematicky řešenu kybernetickou bezpečnost tak, aby kybernetické bezpečnostní incidenty buďto nevznikaly nebo aby jejich výskyt neznamenal bezpečnostní riziko. Nástroje, s nimiž bezpečnostní

opatření počítají, lze z pohledu platného práva rozdělit do následujících základních skupin:

1. Technické prvky (specifický software a hardware vč. detekčních systémů, reportovacích nástrojů, autentizačních či kryptografických nástrojů, technika k zajištění fyzické bezpečnosti apod.)
2. Analytické prvky a dokumentace (typicky analýza informačních aktiv, topografie sítí, analýza rizik apod.)
3. Interní předpisy (organizační opatření, školící plány, krizové plány, interní instrukce pro vybrané skupiny zaměstnanců, interní pravidla pro nákup a outsourcing ICT apod.)
4. Lidské zdroje (specificky vyčleněný personál k zajištění realizace bezpečnostních opatření nebo personál zajišťující výjimečně ad hoc určité činnosti v oblasti kybernetické bezpečnosti)

Poslední dvě uvedené kategorie týkají se vztahu povinného subjektu a jeho pracovníků, ať už jde o zaměstnance nebo obdobně působící externisty. Běžné fungování specificky vyčleněného personálu nebo pracovníků, jimž mohou být úkoly v oblasti kybernetické bezpečnosti ukládány ad hoc, jsou pro existenci a efektivitu bezpečnostních opatření kriticky důležité. Sebelépe postavený a vybavený bezpečnostní systém totiž není k ničemu, pokud není adekvátně obsluhován resp. pokud jeho fungování brání faktická bezpečnostní rizika představovaná vlastními pracovníky povinných subjektů.

Z právního hlediska jde především o otázku povinností, které pracovníkům povinných subjektů ukládá zákon resp. povinností, které na základě zákona svým pracovníkům ukládají povinné subjekty formou interních instrukcí nebo běžné řídící činnosti v rámci korporátní hierarchie[77]. V tomto směru je předně nutno rozlišovat mezi pracovníky, jejichž pracovní náplň souvisí s tvorbou nebo realizací bezpečnostních opatření a pracovníky, jimž jsou pouze na základě bezpečnostních opatření ukládány konkrétní povinnosti s tím, že jejich běžná pracovní náplň s kybernetickou bezpečností jinak nesouvisí (tj. uživatele).

[77] Rozdíl mezi interní instrukcí a aktem řízení spočívá v tom, že zatímco interní instrukce je určena neurčitému okruhu pracovníků splňujících určitou podmínku (např. pracovníkům v určité funkci), je akt řízení adresován, tj. určen konkrétnímu člověku. K povaze interní instrukce viz např. Galvas, M. a kol. *Pracovní právo*. Brno: Masarykova univerzita, 2012, str. 50 nebo Vysokajová, M. *Zákoník práce - komentář*. Praha : Wolters Kluwer, 2012, str. 623.

Bezpečnostní personál nebo pracovníky, u nichž alespoň část běžné pracovní agendy představuje kybernetická bezpečnost lze logicky zatížit nejen větším množstvím pracovních povinností oblasti kybernetické bezpečnosti, ale lze od nich požadovat i vyšší míru odborné erudice a schopnosti plnit specifické požadavky interních bezpečnostních předpisů. Bezpečnostnímu technikovi, správci sítě nebo systémovému administrátorovi tak lze nejen uložit řadu specifických pracovních povinností, jejichž předmětem může být zabezpečení příslušné informační a komunikační infrastruktury, ale tyto povinnosti lze na úrovni interních předpisů nebo individuálních řídících aktů (tj. v rámci běžného podnikového řízení) formulovat i s vysokou mírou odbornosti a spoléhat přitom na adekvátní předvědění.

U profesí, jejichž pracovní náplň netvoří kybernetická bezpečnost, je naproti tomu v případě definice povinností týkajících se bezpečnosti informačních systémů a sítí nutno postupovat tak, aby interní instrukce nebo jiné akty řízení byly obecně srozumitelné a aby byly z pohledu běžného pracovníka technicky proveditelné. Z toho plyne, že například instrukce typu „uživatel je povinen měnit své přístupové heslo minimálně jednou týdně, heslo musí mít min. 15 znaků, z nichž min. 7 znaků musí být speciální znaky ASCII“ je vadná hned ze dvou důvodů. Jednak není možno rozumně požadovat po běžném uživateli, aby si každý týden zapamatoval nové patnáctiznakové heslo a navíc nelze předpokládat, že bude poučen v tom smyslu, co to jsou speciální znaky ASCII. Takto formulovaná interní instrukce tedy, byť její přečtení příslušný zaměstnanec potvrdí třeba podpisem vlastní krví, nikdy nepovede k právně vynutitelnému závazku.

Z právě uvedeného plyne, že problém disciplinární odpovědnosti zaměstnanců vzhledem k bezpečnostním opatřením zaváděným u povinných subjektů mandatorně na základě zákona o kybernetické bezpečnosti spočívá primárně ve způsobu, kterým budou různým kategoriím pracovníků ukládány příslušné bezpečnostní povinnosti. Neexistuje přitom žádná konkrétní judikatura, o kterou by bylo možno se opřít, to i přes skutečnost, že typově podobná situace jako v případě kybernetické bezpečnosti objevuje se dlouhodobě například v oblasti protipožární ochrany nebo bezpečnosti práce. Případy, jejichž autoritativní řešení máme k dispozici jako vodítko, týkají se spíše frapantních porušení

interních předpisů nebo jiných řídících aktů a neposkytují tím pádem adekvátní návod pro diskutabilní či hraniční případy. Ještě žádného zaměstnavatele tak doposud nenapadlo například žalovat o náhradu škody zaměstnance, který, byť byl proškolen v použití hasicího přístroje, vzal raději před požárem v odpadkovém koši nohy na ramena.

Problematika závaznosti respektive míry závaznosti interních instrukcí na úseku kybernetické bezpečnosti každopádně představuje zajímavé a vysoce žádoucí zadání, jehož řešením se česká právní věda již intenzivně zabývá[78] – přestože by ale měly být základní doktrinální poznatky k těmto otázkám k dispozici v řádů měsíců či jednotek let, budou povinné subjekty vystaveny právní nejistotě až do doby, kdy bude k dispozici adekvátní judikatura vyšších soudů.

Na tomto místě je nutno připomenout, že právě uvedené týká se pouze specifických bezpečnostních povinností, jejichž existence je podmíněna zvláštní autoritativní informací prokazatelně sdělenou zaměstnanci. Zaměstnavatel však samozřejmě nemusí zaměstnanci formou interních instrukcí nebo jiných řídících aktů sdělovat všechny možné požadavky na bezpečné fungování informačních systémů a sítí. Každé pracovní pozici totiž odpovídá implicitně předpokládaná odborná výbava zaměstnance, s níž zaměstnavatel může počítat a kterou nemusí ani zvlášť ověřovat.

Pracovní pozice, u níž se předpokládá znalost práce s osobním počítačem, tedy implicitně předpokládá, že bude zaměstnanec bez dalšího chápat například zákaz psaní přístupových hesel na žluté lístečky a jejich lepení na okraj monitoru (podobně není nutno kancelářské síly školit například v tom, že nemají strkat kancelářské sponky do elektrických zásuvek nebo v pracovní době skákat z oken). Analogicky pak bude zřejmě možno ze strany zaměstnavatele i bez nutnosti přijímat interní instrukce předpokládat, že systémový administrátor je obeznámen se skutečností, že nesmí používat triviální heslo nebo že se má při každém odchodu od počítače odhlásit ze své virtuální identity. Ani v těchto otázkách však nemáme k dispozici žádnou použitelnou judikaturu a vyjma evidentních případů lze spíše předpokládat, že soudy nebudou příliš respektovat presumpci nedbalostního zavinění a budou spíše v případě sporu požadovat

[78] Viz např. aktuálně řešený projekt GAMU MUNI/M/1052/2013, Experimentální výzkum chování uživatelů ICT v oblasti bezpečnosti perspektivou sociálních věd, práva a informatiky.

po zaměstnavateli důkaz skutečnosti, že zaměstnanec příslušné bezpečnostní pravidlo znát mohl a hlavně, že jej vzhledem ke svému pracovnímu zařazení znát měl[79].

5. PERSPEKTIVY DALŠÍHO VÝVOJE ČESKÉHO PRÁVA KYBERNETICKÉ BEZPEČNOSTI

Shora provedená analýza má, jak bylo na několika místech zvlášť zdůrazněno, pouze doktrinální charakter a bez specifické judikatury nelze konstatovat konkrétní tvar jednotlivých institutů aktuálně tvořících českého právo kybernetické bezpečnosti. I v případě právních nástrojů, které již máme v našem právu k dispozici, totiž není jasno v tom, jaké formy může mít jejich aktuální aplikace. Diskutovat za této situace možnosti dalšího vývoje našeho práva kybernetické bezpečnosti je tedy podobno věštění z kávové sedliny.

Následující výklad je zaměřen především na možnosti dalšího vývoje české legislativy, přičemž vychází kromě shora diskutovaného současného stavu též z tendencí patrných v zahraničních právních řádech. České právo má v této souvislosti určitou výhodu spočívající v tom, že máme přístup k dobrým i špatným zkušenostem s různými typy legislativních nástrojů ze států, pro které kybernetická bezpečnost představovala a představuje v porovnání s naší situací daleko naléhavější problém. Můžeme se tedy díky spojeneckým svazkům a tradičním přátelským vazbám poučit ze zkušeností realizovaných v podobném právním prostředí, tj. v situaci standardního demokratického právního státu, ve státech, které kvůli své velikosti nebo zahraničněpolitické aktivitě staly se terčem závažných kybernetických útoků dříve a ve větší míře, než je tomu u nás.

Skutečnost, že v případě USA, Spojeného království nebo například Izraele jde o země fungující na jiných právně-kulturních základech, v tomto případě nebrání vzájemnému srovnání a využití příslušných zkušeností a dalších právních poznatků. Technika fungování právních mechanismů příslušné právní kultury totiž vzhledem k nastavení právních nástrojů pro

[79] K tomu ještě přistupuje podstatný rozdíl mezi interní instrukcí a právním předpisem nebo vrchnostenským aktem spočívající v tom, že interní instrukce se nemůže spoléhat na presumpci správnosti resp. presumpci platnosti – srov. Bělina, M. a kol. *Pracovní právo.* 5. dopl. a podstat. přeprac. vyd., Praha : C.H.Beck, 2012, str. 66.

zajištění národní kybernetické bezpečnosti není nikterak podstatná - hlavní roli při posuzování použitelnosti určitého přístupu, nástroje nebo institutu hraje zde spíše příbuznost hodnotových základů příslušných právních kultur, jimiž jsou v případě českém i v případě právě jmenovaných zemí shodně priorita práv člověka a základní principy demokratického právního státu.

Příkladem takové zkušenosti, která nám ušetřila čas a nemalé zdroje finanční, personální i politické, je původní záměr severoamerické vlády koncipovat národní úpravu kybernetické bezpečnosti na bázi identifikace útočníka[80]. Jedná se o jeden ze dvou způsobů, jak strategicky nastavit právní instituty chránící veřejný zájem na fungování kritické informační a komunikační infrastruktury, který však je vysoce problematický vzhledem k proporcionalitě práv uživatelů služeb informační společnosti (v USA není sice zakotveno právo na ochranu osobních údajů a ochrana soukromí má poněkud jiný charakter než v Evropě, ale právo na anonymní vystupování v prostředí informačních sítí je i tak extrémně silné díky prvnímu dodatku americké ústavy). Politická neprůchodnost tohoto přístupu posloužila nám za vodítko při stanovení základní strategie české resp. evropské právní úpravy kybernetické bezpečnosti, která je namísto zmíněného modelu postavena na strategické prioritě ochrany prostředí[81] s tím, že identifikace a postih útočníka je ponechán na režimu běžného fungování trestního práva resp. na standardní působnosti orgánů činných v trestním řízení.

5.1 ZÁKONNÁ TYPOLOGIE UŽIVATELŮ VYBRANÝCH SYSTÉMŮ A SÍTÍ

Z právě uvedeného plyne, že individuální odpovědnost koncového uživatele, ať je jím útočník nebo i jen subjekt, jehož systém se z nějakého důvodu podílí na kybernetickém bezpečnostním incidentu, představuje politicky velmi citlivou otázku. Předpokladem uplatnění individuální odpovědnosti uživatele, ať už má jít o odpovědnost soukromoprávní nebo trestní, je totiž jeho ztotožnění. To přitom vyžaduje použití takových mechanismů, které mohou obecně ohrozit shora zmíněnou anonymitu (jako

[80] Srov. Sales, S. A. Regulating Cyber-Security, *Northwestern University Law Review*, roč. 107, číslo 4, str. 1503.

[81] K tomu viz např. věcný záměr zákona o kybernetické bezpečnosti nebo průvodní dokumentaci k návrhu směrnice o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii, COM/2013/048 final - 2013/0027 (COD).

nutnou komponentu práva na svobodu projevu) a mohou být především kontradiktorní s kategorickými požadavky výjimečně rigorózně nastavené evropské ochrany soukromí a osobních údajů.

Právě ochrana soukromí, osobních údajů, svobody projevu či obecně vzato práva na informační sebeurčení jsou důvodem toho, že se zřejmě v dohledné době nesetkáme s ničím takovým, jako internetový občanský či řidičský průkaz. Na druhé straně však je možno uvažovat o proporcionální ochraně vitálních zájmů na fungování kritických součástí informační a komunikační infrastruktury prostřednictvím specifické individuální odpovědnosti lidí, kteří na profesionální bázi s kriticky důležitými informačními systémy nebo sítěmi pracují.

Jednou z možností legislativního řešení je maďarský model definice stupňů bezpečnostní důležitosti informačních systémů a sítí a založení práva pracovat s těmito systémy pouze uživatelům s určitým stupněm znalostní certifikace[82]. Nemusí přitom jít pouze o povinnost pro správce příslušného systému nebo sítě spočívající v nutnosti proškolit své zaměstnance respektive najmout si pro jejich obsluhu odborně náležitě vybavený personál. Zprostředkovaně může jít též o vytvoření specifických povinností na straně samotného uživatele založených předpisy na úseku kybernetické bezpečnosti, zakládajících správní odpovědnost za přestupky nebo jiné správní delikty spočívající v neodborném přístupu ke kriticky důležitým systémům nebo sítím a odstupňované adekvátně k jejich bezpečnostní klasifikaci.

Je docela pravděpodobné, že potřebu takové úpravy pocítí v první řadě především správci kritické informační a komunikační infrastruktury poté, co konstatují nutnost až příliš sofistikované tvorby interních instrukcí tak, aby bylo v případě problému na straně uživatele nebo operátora kriticky důležitého systému nebo sítě možno regresně vyvodit alespoň disciplinární odpovědnost. Problémem interních instrukcí totiž je, že jejich závaznost či praktická vynutitelnost není jen otázkou jejich bezrospornosti se zákonem, ale též jejich srozumitelnosti a formy komunikace (viz dále). Byť to může

[82] Srov. maďarský zákon o elektronické informační bezpečnosti ústředních a místních správních orgánů ze dne 15. dubna 2013 – ke stažení v anglické verzi on-line na adrese http://www.nbf.hu/anyagok/Act%20L%20of%202013%20on%20the%20Electronic%20Information%20Security%20of%20Central%20and%20Local%20Government%20Agencies.docx.

znít na první pohled poněkud problematicky, je proto pro zaměstnavatele nepoměrně jednodušší, pokud se může spolehnout na zákonnou nebo podzákonnou definici konkrétních bezpečnostních povinností svých zaměstnanců, než pokud by takovou definici měl sám vytvářet a implementovat. Individuální správní odpovědnost je navíc sama o sobě silným motivačním faktorem, který může pro příslušné zaměstnance představovat ještě pádnější důvod k obeznámení se s bezpečnostními pravidly a k jejich dodržování, než je tomu v případě disciplinární odpovědnosti nebo omezené odpovědnosti za škodu způsobenou zaměstnavateli.

Ve vazbě k výše uvedenému je možno uvažovat též o zákonem založené povinnosti pro správce vybraných typů vysoce bezpečnostně exponovaných informačních systémů a sítí vyčlenit resp. zaměstnat pracovníka přímo odpovědného za plnění požadavků zákona o kybernetické bezpečnosti. Podobně, jako je tomu v agendě ochrany utajovaných informací[83] nebo v některých členských státech v agendě ochrany osobních údajů[84], mohl by tento zaměstnanec mít v organizační struktuře příslušného správce ze zákona dané specifické postavení a jeho disciplinární odpovědnost by mohla být rozdělena mezi zaměstnavatele a národního regulátora (tj. v našem případě zřejmě Národní bezpečnostní úřad).

5.2 OMEZENÁ ODPOVĚDNOST BĚŽNÝCH UŽIVATELŮ

Nejen z politických důvodů je zřejmě nereálné předpokládat, že by právní úprava kybernetické bezpečnosti v dohledné době specificky založila objektivní odpovědnost koncových uživatelů nebo zavedla nějaký zvláštní mechanismus jejich identifikace. Přes všechny více či méně argumentované požadavky na to, aby uživatelé odpovídali za bezpečné fungování svých systémů bez ohledu na své zavinění, je totiž třeba v první řadě zohlednit skutečnost, že i relativně jednoduché technologie určené k běžnému použití v domácnostech (typicky např. mobilní telefony, domácí wifi routery apod.) jsou z podstaty extrémně technicky složité. Běžný uživatel tedy

[83] Srov. § 71 zákona č. 412/2005 Sb.

[84] Povinnost zřídit u větších subjektů tuto funkci se plánuje k celoevropskému zavedení v připravované nové úpravě evropské ochrany osobních údajů – k tomu viz dokumentaci k návrhu nařízení o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů) - COM(2012) 11 final, 2012/0011 (COD).

nejenže nechápe (resp. nemusí chápat) ani základní principy jejich fungování, ale nelze po něm požadovat ani to, aby se zvlášť věnoval jejich zabezpečení proti možnému zneužití. Jestliže tedy prostý spotřebitel např. neprovede instalaci bezpečnostní záplaty a v důsledku toho je jeho systém zneužit k útoku typu DDoS, není v dohledné době možno uvažovat o tom, že by za takový útok měl nést spoluodpovědnost.

Z hlediska proporcionality dotčených práv nesrovnatelně schůdnějším řešením by byla regulace spotřebitelské dostupnosti informačních a komunikačních technologií v závislosti na míře jejich bezpečnosti. Lze tedy uvažovat o tom, že budou pro určité typy informačních a komunikačních technologií zavedeny mandatorní požadavky na jejich kvalitu, které zahrnou i nutnou jejich bezpečnostní výbavu. Podobně, jako je tomu pravidlem v síťových odvětvích, tj. např. v energetice, telekomunikacích nebo v dopravě, může i v oblasti kybernetické bezpečnosti vzniknout katalog požadavků na shodu, který zahrne nejnutnější bezpečnostní prvky a bez jejichž dodržení nebude možno příslušnou technologii spotřebitelsky šířit na tuzemském trhu. I v tomto případě by šlo zprostředkovaně o zatížení koncového uživatele – nikoli sice přímými povinnostmi či odpovědností, ale nutností zaplatit příslušné zabezpečení včetně jeho administrativních externalit v konečné ceně produktu nebo služby. Takové řešení je však stále z hlediska ochrany práv nesrovnatelně schůdnější, než shora diskutovaná objektivní odpovědnost.

Velmi zajímavou možnost řešení individuální odpovědnosti uživatele přinesl doposud výjimečný případ, který řešily americké soudy. Šlo v něm, stručně řečeno, o infekci využívající bezpečnostní díru v systémech společnosti Microsoft, která umožňovala skryté využití napadených systémů jako součástí botnetu pro útoky typu DDoS. Spol. Microsoft se v tomto případě odhodlala k právně originálnímu řešení, když zažalovala organizátory botnetu a v návrhu rozhodnutí též de facto navrhla postihnout i uživatele, kteří své systémy nezabezpečili bezpečnostní záplatou[85].

Pro právní řády z právní kultury common law je totiž typické, že umožňují uplatnit civilní postih i proti osobám, které sice nejsou určeny jménem a adresou, ale jejichž specifikace je dostatečně přesná na to, aby

[85] Viz rozhodnutí ve věci 3:13-CV-00319-GCM okresního soudu pro Western District of Notrh Carolina, Charlotte Division, ke stažení on-line na adrese http://botnetlegalnotice.com/citadel/files/Order_Granting_Def_Jdgmt_PI.pdf.

bylo možno podle příslušného znaku konkrétní subjekt v důsledku identifikovat. Žalovaný tedy v tomto případě může být určen konkrétním znakem bez toho, aby žalobce znal jeho přesnou identitu. V důsledku to pak znamená, že žalovaný ani nemusí vědět o tom, že je žalován (přestože je mu doručováno za známý e-mail).

Plán založit nepřímou odpovědnost koncových uživatelů jeví se být sice ve světle shora uvedených argumentů jako prostá marnost. V tomto případě se však spol. Microsoft podařilo velmi inovativním způsobem vyřešit rovnováhu mezi deliktem a jeho odpovědnostním důsledkem. Žalobní petit totiž nezněl na náhradu škody nebo jiné plnění, ale „pouze" na povinnost uživatele strpět dálkový zásah do svého systému, kterým Microsoft přesměruje za účelem vyšetření celého incidentu případný útok na své vlastní servery. Tento nárok byl díky tomu shledán proporcionálním k deliktu a následně přiznán. Microsoft tedy mohl nepozorovaně zasáhnout do infikovaných systémů a díky přesměrování jejich komunikace nejen zabránit škodám, které by botnet mohl způsobit, ale též získat cenná data k vyšetření celého incidentu.

Tento případ není pro českou právní praxi inspirativní do té míry, že by bylo snad možno uvažovat o podobném řešení v našich podmínkách. Naše procesní právo totiž nedovoluje žalovat na základě identifikačního znaku, nelze-li podle něj přímo v řízení ztotožnit konkrétní subjekt. I pro naše právní prostředí je však zajímavá úvaha soudu ohledně toho, že i běžný uživatel má určitou míru povinnosti vědět o potřebě zabezpečení svého vlastního systému a že tuto povinnost lze uvést do souvislosti s adekvátním typem odpovědnostního následku, tj. nikoli např. hradit škodu ale „pouze" strpět dálkový zásah do svého systému.

Prostředkem, který by bylo možno využít namísto shora popsaného řešení, mohlo by se stát opatření obecné povahy. To totiž umožnuje identifikovat své adresáty na základě obecných znaků a uložit jim určitou povinnost. Je pak možno svěřit konkrétnímu úřadu (v našem případě by zřejmě šlo o Národní bezpečnostní úřad nebo Český telekomunikační úřad) kompetenci vydávat za přesně stanovených okolností tato opatření a ukládat jimi i běžným (nic netušícím) uživatelům podobné povinnosti strpět zásah do jejich systémů, jako se stalo ve shora zmíněném případě.

5.3 SPECIFICKÁ ÚPRAVA OUTSOURCINGU

Jádrem aktuální zákonné úpravy i podzákonných prováděcích předpisů v oblasti kybernetické bezpečnosti jsou bezpečnostní opatření. Požadavky na standard zabezpečení informační a komunikační infrastruktury spravované povinnými subjekty jsou zákonem stanoveny velmi obecně a prováděcí předpisy pak obsahují jen takovou míru jejich konkretizace, která nezasahuje do principu technologické neutrality a umožňuje povinným subjektům autonomii při volbě konkrétních řešení. Tento model jeví se jako vhodný hned ze dvou důvodů – předně je povinný subjekt tím nejvíce povolaným, pokud jde o detailní technické znalosti příslušného informačního systému nebo sítě a má tedy nejlepší možnost posoudit, jaká konkrétní bezpečnostní řešení nejlépe splní zákonné požadavky. Vedle toho je velmi pravděpodobné, že relativní otevřenost standardních požadavků povede společně s jistotou investic k motivaci dodavatelů různých bezpečnostních řešení k investicím do vývoje. To může přinést vítaný impuls k dalším inovacím v oboru ICT bezpečnosti.

Relativně velká míra autonomie u povinných subjektů ohledně způsobu plnění zákonných požadavků však na druhé straně vyvolává i nejistotu ohledně řešení typických případů, kdy správce nerealizuje jednotlivá bezpečnostní opatření sám nebo alespoň ve vlastní režii, ale provádí jejich komplexní outsourcing. Především u středně velkých a menších povinných subjektů lze kromě vzájemné koordinace jejich aktivit při akvizicích bezpečnostních řešení očekávat i společné postupy při komplexním řešení bezpečnostních opatření včetně jejich fungování v reálném čase. Lze si tedy například představit, že místní utility typu vodáren nebo tepláren vytvoří společný podnik, který bude jim bude zajišťovat realizaci a fungování bezpečnostních opatření např. i včetně provozu lokálního CERT, reportování incidentů, spolupráce s národním nebo vládním dohledovým pracovištěm apod.

Zákon a podzákonné předpisy sice možnost outsourcingu bezpečnostních opatření nevylučují a v konkrétních částech s ní přímo počítají. Pravidla pro externí dodavatele bezpečnostních řešení však se omezují pouze na obecné povinnosti mít dokumentovány a kontrolovány vztahy s externími dodavateli.

Vzhledem k tomu, že zákon o kybernetické bezpečnosti stojí na výlučné odpovědnosti správce příslušného informačního systému nebo sítě, není v jeho současné struktuře obsažena speciální úprava postavení dodavatele nebo provozovatele bezpečnostních opatření. Je tedy plně na správci, jak si vztahy s externími subjekty vyřeší a jak bude ve vztahu k nim zajišťovat například plnění povinností vyplývajících z kontrolních pravomocí Národního bezpečnostního úřadu nebo regresní nároky v případě deliktní odpovědnosti.

Zatímco volnost ve smyslu konkrétní formy bezpečnostních opatření jeví se jako vhodná a není důvod předpokládat v brzké budoucnosti nějaké zásadní změny, je otázku totální volnosti povinných subjektů ohledně outsourcingu bezpečnostních opatření možno považovat za místo, kde bude zákonná úprava průběžně doplňována na základě praktických zkušeností. Nejde pouze o možnost založení přímých pravomocí Národního bezpečnostního úřadu vůči subjektům poskytujícím bezpečnostní řešení jako službu, ale například i o možnost správní regulace činnosti takových subjektů (nabízí se například varianta speciální vázané živnosti). Především ve vztahu k informačním systémům veřejného sektoru spadajících pod rozsah zákona o kybernetické bezpečnosti (tj. k informačním systémům veřejné správy a dalším informační systémům provozovaným veřejnoprávními korporacemi, které budou spadat pod rozsah kritické informační infrastruktury nebo významných systémů) lze očekávat i podrobnější úpravu požadavků na outsourcing, která by měla odstranit standardní bezpečnostní nešvary vyskytující se v procesech zadávání veřejných zakázek na ICT.

Vedle konkrétnější úpravy zákonných a podzákonných parametrů outsourcingu bezpečnostních opatření lze předpovědět i nepoměrně rychlejší vývoj smluvních nástrojů a alternativních forem řešení obchodních sporů, a to především u soukromoprávních povinných subjektů. Dokonce ještě před platností (nikoli až účinností) zákona o kybernetické bezpečnosti byly některé velké korporace včetně energetických společností nuceny zahrnovat do outsourcingových smluv klauzule zakládající pro dodavatele resp. poskytovatele služby specifické povinnosti v návaznosti na budoucí zákonné bezpečnostní požadavky.

Konstrukce těchto klauzulí, kontrola příslušných plnění v reálném čase (může totiž jít o mnohaleté smlouvy) nebo mechanismy řešení vzájemných sporů představují oblast smluvního ICT práva, která sice u nás není úplně zanedbána, bude však zřejmě ještě procházet velkým rozvojem. Namísto legislativní asistence však je v tomto směru spíše nutno očekávat, že si budou muset soukromoprávní povinné subjekty, zjednodušeně řečeno, pomoci samy – přispět ke zdárnému vývoji smluvních nástrojů, procedur výběru dodavatelů nebo procedur řešení dodavatelských sporů mohou kromě organizací typu Hospodářské komory především oborové asociace. Kvalitně fungující vztahy s dodavateli bezpečnostních opatření totiž nepředstavují otázku vzájemné konkurence mezi subjekty působícími na týchž trzích a přímo se tak nabízí vzájemná bezkonfliktní spolupráce a koncentrace zdrojů k zajištění efektivně fungujících právních řešení.

5.4 DALŠÍ VÝVOJOVÉ PERSPEKTIVY PRÁVA KYBERNETICKÉ BEZPEČNOSTI

K právě uvedenému lze spekulativně připojit i další oblasti, z nichž na prvním místě se bude zřejmě jednat o postupnou národní i mezinárodní konkretizaci pojmu informační suverenity státu. Primárním těžištěm tohoto problému bude zřejmě mezinárodní právo veřejné a výstupy můžeme očekávat především z jeho doktríny. Přestože ideálním řešením by v tomto směru byla mezinárodní úmluva, nedá se vzhledem ke zcela rozdílným pohledům na věc a zcela odlišným zájmům jednotlivých národních vlád očekávat, že by k přípravě takové úmluvy mohlo v dohledné době dojít. Příliš pravděpodobný není ani vznik judikatury Mezinárodního soudního dvora, neboť státy, které by toho byly schopny, nemají, stručně řečeno, k přednesení aktuálně se vyskytujících konfliktních situací tomuto fóru prakticky žádnou motivaci. Namísto toho je spíše důvod očekávat další rozvoj vzájemné spolupráce na základě existujících obecných spojeneckých svazků, z nich nejvýznamnější a doposud nejproduktivnější je spolupráce v rámci NATO[86].

[86] Z doktrinálního hlediska nejvýznamnější výstupem této spolupráce je činnost centra excelence CCD CoE v estonském Talinu, jejíž manuál se stal všeobecně uznávaným standardem doktríny mezinárodního práva veřejného pro kybernetickou bezpečnost. Manuál je on-line ke stažení ze http://issuu.com/nato_ccd_coe/docs/tallinnmanual.

Nesrovnatelně jednodušší je co do synergie základních hodnot a zájmů situace v rámci Evropské unie. Díky tomu lze v brzké době očekávat finalizaci směrnice o kybernetické bezpečnosti (resp. směrnice o síťové a informační bezpečnosti) a další rozvoj stávajících evropských bezpečnostních struktur, zejm. ENISA a CERT-EU. Poslední vývoj návrhu cit směrnice směruje sice spíše k obecnějšímu rozsahu a nižšímu standardu povinností členských států – podobně jako v případě českého zákona o kybernetické bezpečnosti je však i v tomto případě zřejmě vhodné přistoupit k fixaci určitého právně bezproblémového a politicky akceptovatelného řešení a to pak dále rozvíjet institucionální a legislativní aktivitou na základě praktických zkušeností.

V českém právním prostředí můžeme nad rámec toho, co bylo diskutováno v předchozích kapitolách, očekávat především konkretizaci spolupráce vládního a národního CERT, jakož i konkretizaci spolupráce Národního bezpečnostního úřadu s ostatními orgány veřejné moci, do jejichž zájmu spadá oblast národní kybernetické bezpečnosti (vedle bezpečnostních služeb jde především o Policii ČR, Armádu ČR a ústřední orgány státní správy mající jurisdikci nad kritickými či významnými informačními systémy a sítěmi)[87]. Podobně lze očekávat též rozvoj spolupráce mezi Národním bezpečnostním úřadem a soukromoprávními korporacemi, profesními sdruženími a akademickou sférou – ta může mít charakter neformálních aktivit, memorand, činnosti expertních skupin apod. a může řešit problémy, které z nějakého důvodu není možno nebo vhodno pokrýt veřejnoprávními aktivitami (typicky např. otázky certifikace, vzdělávání, podpory inovací apod.)

Jako nanejvýš vhodná jeví se v tomto směru být tendence zahrnovat kybernetickou bezpečnost mezi aktuální politické priority – to umožní podporovat shora uvedené činnosti v rámci standardních forem spolupráce mezi soukromým, akademickým a veřejným sektorem typu podpory vědeckých nebo rozvojových projektů, exportu, investic, rozvoje občanské společnosti aj.

[87] Národní bezpečnostní úřad již v tomto směru publikoval několik podpůrných dokumentů jako např. blokové schéma zákona o kybernetické bezpečnosti nebo pomůcky k určení prvku kritické informační infrastruktury a významných systémů – dokumenty jsou ke stažení on-line na adresách: www.govcert.cz.

6. PERSPEKTIVY DALŠÍHO POLITICKÉHO A ORGANIZAČNÍHO VÝVOJE AGENDY KYBERNETICKÉ BEZPEČNOSTI V ČESKÉ REPUBLICE

6.1 CERTIFIKACE A COMPLIANCE CHECK

Jak uvedeno shora, pracuje návrh české právní úpravy s principem autonomie vůle regulovaných subjektů. Jedním z projevů tohoto principu ve spojení s principem technologické neutrality je mandatorní stanovení cílových charakteristik bezpečnostních opatření (organizačních i technických) a ponechání konkrétní formy realizace na úvaze příslušného povinného subjektu. Vhodnost takového řešení je vedle obecně menší regulatorní zátěže pro povinné subjekty dána též skutečností, že příslušné bezpečnostní řešení může být vždy realizováno na míru konkrétního systému. Regulovaný subjekt má tedy praktickou volnost ve výběru architektury, technologie i dodavatelů.

Určitou nevýhodou tohoto jinak vhodně zvoleného řešení však je skutečnost, že povinné subjekty budou mít jen omezenou míru právní jistoty ohledně otázky, zda právě jejich konkrétní řešení odpovídá zákonným požadavkům, tj. zda v případě kontroly ze strany Národního bezpečnostního úřadu nebudou shledány vzhledem k zákonným požadavkům nějaké nedostatky. Byť jsou totiž požadované parametry bezpečnostních opatření definovány s maximální mírou určitosti, nelze se, a to ani při konkretizaci jednotlivých parametrů formou podzákonných právních předpisů, ubránit relativně velké míře abstrakce a výsledné nejistoty plynoucí vedle relativně abstraktních zákonných a podzákonných pojmů též z velkého množství různých organizačních a technických kritérií.

K relativní neurčitosti zákonných resp. podzákonných požadavků pak ještě přistupuje určitá míra nejistoty ohledně implementace a následného provozu bezpečnostních opatření. Zákonné požadavky totiž nesměřují jen ke statické formě bezpečnostních opatření (tj. k jejich statickým formálním parametrům) ale též k jejich implementaci a fungování v reálném čase. I bezpečnostní řešení dostatečně dimenzované vzhledem k zákonným požadavkům totiž může ve svém výsledku porušovat zákonné podmínky

kvůli neadekvátní implementaci nebo nedostatečné pozornosti vzhledem k jeho trvalému provozu.

Nejistota ohledně toho, zda projektované, pořízené, implementované a provozované bezpečnostní řešení splňuje zákonné parametry, představuje závažný problém především pro střední a velké podniky, jakož i pro veřejnoprávní korporace. U středních a velkých podniků jedná se především o otázku compliance, přičemž především nadnárodní korporace často řeší otázky a priori plnění zákonných požadavků v příslušných jurisdikcích jako naprostou prioritu. Aktuálně se to týká např. otázek ochrany osobních údajů, bezpečnosti práce, požární bezpečnosti, utajovaných informací apod. Pro podnik velkého rozsahu je totiž zásadně důležité vyčíslení nákladů na plnění právních povinností v příslušné jurisdikci a priori – jen tak s nimi totiž lze kalkulovat do finančních plánů. Situace, kdy je velká nebo střední korporace nucena kalkulovat potenciální náklady na plnění právních povinností a posteriori, vždy generuje značnou míru nejistoty, neboť právní odpovědnost (postih) se v komplexních případech jen velmi těžko odhaduje a těžké je i provést takovou kalkulaci do všech možných důsledků (k tomu viz výše).

V případě naší právní úpravy kybernetické bezpečnosti tak jde příkladně o to, jaké mohou být právní následky implementace a používání takového systému bezpečnostních opatření, o kterém se následně prokáže, že nesplňuje zákonné požadavky. U velkého nebo středního podniku je v tomto směru případná pokuta jen jedním z mnoha možných následků, neboť nezákonnou implementací mohou být způsobeny např. škody třetím osobám nebo může v důsledku nařízených opatření k nápravě dojít k omezení provozu či k potřebám zásadních organizačních změn.

Dokonce i tam, kde lze počítat s konkrétní výší např. pokut, náhrad škody nebo škod způsobených zastavením nebo omezením provozu, představuje u všech typů podnikatelských subjektů a posteriori řešení právní rizikovosti velmi nevítanou alternativu. Není totiž žádným tajemstvím, že podnikatelské aktivity mohou být významně poškozeny už tím, že se orgány státní moci nějakou formou o příslušný podnik zajímají. Typicky pak může i pouhá kontrola nebo vyšetřování ze strany oprávněných orgánů státní moci způsobit jen těžko předvídatelné komplikace a vést ke ztrátám, jejichž hodnotu lze jen stěží předem vyčíslit.

To platí samozřejmě i pro případy, kdy vyšetřování nebo kontrola nevedou ve vztahu k příslušnému orgánu veřejné moci k žádném sankčnímu důsledku, neboť i pouhá vrchnostenská přítomnost na kontrolovaných pracovištích může se negativně projevit na výkonu celého podniku.

U veřejnoprávních korporací je otázka a priori souladu s požadavky právního řádu ještě důležitější než u podnikatelských subjektů. V porovnání se soukromoprávními subjekty jde dokonce o prioritní otázku bez ohledu na jejich velikost. Je-li totiž k pořízení nebo provozu bezpečnostních opatření užito veřejných prostředků, nelze riskovat dodatečnou kvalifikaci těchto opatření jako nesouladných se zákonnými požadavky.

Lze navíc předpokládat, že investice veřejného sektoru do kybernetické bezpečnosti budou minimálně z podstatné části kryty prostředky z různých rozvojových projektů – příjemce takových prostředků si pak dvojnásob nemůže dovolit rizikovost investice vzhledem ke splnění zákonných požadavků resp. nemůže si dovolit riskovat situaci, kdy projektové prostředky použije způsobem, který je dodatečně (např. na základě kontroly) označen za nikoli souladný s platnou právní úpravou. Poskytovatel dotace má totiž v takovém případě právo či dokonce povinnost dovolávat se podmínek jejího poskytnutí a požadovat vrácení poskytnutých prostředků.

Z právě popsaných důvodů lze mezi středními a velkými soukromoprávními subjekty a veřejnými korporacemi očekávat velkou poptávku po a priori aprobačních procedurách poskytujících nezávislé ujištění ohledně toho, že implementované resp. provozované řešení bezpečnostních opatření je v souladu s požadavky účinné právní úpravy. Objektivně ideální variantou řešení tohoto problému by byla zákonná certifikační procedura realizovaná přímo příslušným orgánem státní exekutivy (v českém právním prostředí zřejmě Národním bezpečnostním úřadem) nebo jím pověřeným a dozorovaným nezávislým expertním pracovištěm.

Skutečnost, že taková procedura není součástí struktury navrhované právní úpravy, však lze jen sotva vnímat jako chybu právotvůrce nebo jako pravou mezeru v právu. Taková procedura musela by totiž být podrobně a rigorózně upravena, aby nevzniklo riziko privatizace výkonu nedistributivních práv resp. aby nebyl indukován korupční potenciál. Je

přitom jen velmi obtížné takovou rigorózní úpravu provést v situaci, kdy jsou k dispozici v tomto ohledu jen velmi omezené zkušenosti (zde je nutno připomenout, že stávající komerční certifikační procedury zaměřují se především na problematiku organizačních opatření, nikoli už na technologie k zajištění kybernetické bezpečnosti nebo na spolupráci s centrálními dohledovými pracovišti).

Zavedení státní certifikace by rovněž vyžadovalo důkladnou přípravu institucionální a personální a je třeba v tomto směru konstatovat, že na našem pracovním trhu zdaleka není přebytek pracovní síly disponující dostatečnou mírou kvalifikace v oboru kybernetické bezpečnosti a k tomu náležitě motivované za aktuálních platových podmínek ke vstupu do státní služby. Příprava adekvátní procedury by tedy z hlediska organizačního i personálního vyžadovala takovou časovou a finanční dotaci, kterou si vzhledem k vývoji bezpečnostní situace nemůže v současné době Česká republika dovolit (kromě toho je třeba po bohatých našich legislativních zkušenostech připomenout, že nemá smysl uvádět v účinnost právní úpravu, na jejíž implementaci není státní exekutiva náležitě připravena).

Ve prospěch státního řešení certifikace může naopak hovořit pozitivní zkušenost s obdobnou procedurou v agendě ochrany utajovaných informací. Ani v tomto případě přitom nebylo možno ji realizovat okamžitě, ale příslušné kapacity se postupně vytvářely. Skutečnost, že v tomto případě nejde o korupčně exponovanou situaci, navíc ukazuje, že je v případě Národního bezpečnostního úřadu možno předpokládat takovou kvalitu institucionálních opatření, která vzniku a rozvoji korupčního rizika účinně brání. V případě kybernetické bezpečnosti by navíc bylo možno v porovnání s technologiemi a postupy pro ochranu utajovaných informací učinit celý certifikační proces ještě transparentnějším (tj. vystavit jej ve větší míře veřejné kontrole v tomto případě vykonávané především dodavateli vzájemně konkurenčních bezpečnostních řešení) a lze tedy konstatovat, že korupční rizikovost by bylo možno v takovém případě prakticky vyloučit.

Problémem však každopádně zůstává shora konstatovaná a jen těžko okamžitě řešitelná dlouhodobost náběhu veřejnoprávní certifikační procedury daná nutností vytvořit na straně NBÚ odborně zdatný

a dostatečně robustní personální substrát[88]. Jedinou variantou přímého zapojení orgánu veřejné moci do a priori certifikace bezpečnostních řešení tedy zůstává institucionální nebo produktová aprobace certifikační procedury realizované nezávislým subjektem s dostatečnou personální kapacitou, tj. akademickou institucí, profesním či oborovým sdružením nebo komerčním poskytovatelem.

Role zájmových sdružení a organizací zajišťujících expertní spolupráci soukromého a veřejného sektoru je v tomto směru zřejmě klíčová. Ve vzájemné spolupráci s orgány odpovědnými za výkon vrchnostenské správy na úseku kybernetické bezpečnosti a nezávislými akademickými institucemi mohou tyto organizace pomoci s vytvořením nezávislých certifikačních procedur praeter legem, které nebudou mít vrchnostenský charakter, ale přesto poskytnou zájemcům z řad soukromého a veřejného sektoru nezávislé komplexní posouzení jejich bezpečnostních opatření vzhledem k zákonným a podzákonným požadavkům. Charakter zájmového sdružení v tomto případě kombinuje aspekt transparentnosti (tj. je jasné, že jde o aktivitu obchodní komunity) a profesní specializaci (tj. zaměření na konkrétní ekonomické odvětví) s legitimitou společného postupu, tj. nejde pouze o zájem jednoho podnikatele, ale aktivita sdružení odráží vůli jinak si vzájemně konkurujících subjektů.

Takové certifikační procedury samozřejmě nebudou disponovat vrchnostenským charakterem a jejich výstupy nebudou zavazovat orgány veřejné moci při hodnocení souladu příslušných bezpečnostních řešení se zákonem a podzákonnými předpisy. Při nalezení adekvátního modelu spolupráce s vrchnostenskými orgány však lze tímto prostřednictvím docílit faktické akceptace těchto certifikačních procedur alespoň v procesním smyslu. Jinými slovy tedy takový certifikát nemůže sice absolutně ochránit příslušný subjekt před kontrolou nebo následnou sankcí, jeho udělení však může být při případné kontrole fakticky zohledněno. Zatímco tedy může být za běžných podmínek prováděna kontrola bezpečnostních opatření bez jakékoli presumpce, může Národní bezpečnostní úřad kontrolovat certifikovaná bezpečnostní řešení s presumpcí souladu. Takové procesní řešení může pak pragmaticky posloužit nejen povinným osobám, ale

[88] S tímto problémem se každopádně nepotýká jen Česká republika – srov. Devost, M. G., Moss, J. Pollard, N. A. Stratton, R. J. III. All Done Except the Coding, *Georgetown Journal of International Affairs*, roč. 11, str. 197 a násl.

samotnému Národnímu bezpečnostnímu úřadu – logicky ale jeho implementace vyžaduje především vzájemnou důvěru, kterou může zajistit pouze skutečná nezávislost certifikační procedury, jakož i její vysoká odborná úroveň. Obojí je v našem prostředí řešitelné v první řadě spoluprací s renomovanými akademickými institucemi.

Především z hlediska povinných subjektů užívajících k investicím do pořízení nebo provozu bezpečnostních opatření veřejné prostředky (v tomto případě je lhostejno, zda jde o soukromoprávní nebo veřejnoprávní organizace) je shora popsané řešení vhodné i z důvodu možné inkorporace do zadávací dokumentace resp. do mandatorních požadavků na dodavatelská řešení. Namísto relativně neurčitých formulací ohledně souladu bezpečnostních opatření s platnou právní úpravou budou tyto subjekty moci v implementačních nebo realizačních smlouvách využít ujednání odkazující na získání konkrétních typů certifikací a sjednat si tím vyšší míru právní jistoty. Obdobná může být též situace u dlouhodobých outsourcingových kontraktů, kde požadavek na certifikaci příslušného bezpečnostního řešení na aktuálně účinný standard může být na straně odběratele adekvátně řešit jistotu ohledně průběžného plnění zákonných resp. podzákonných povinností, u nich lze oprávněně očekávat, že se budou v čase výrazně vyvíjet a měnit (k tomu viz výše).

K právě uvedenému je nutno doplnit, že příslušná certifikační řešení zdaleka nemusí být unikátní nebo monopolní resp. že pro různé typy bezpečnostních řešení mohou fungovat různé procedury. Certifikace tak může být prováděna např. formou prověrky ve fázi projektu informačního systému nebo sítě, kontroly jeho implementace nebo provozních zkoušek jako součásti různých fází akceptace příslušných dodávek. Formu certifikace mohou mít též například i penetrační testy nebo jiné typy operačních prověrek běžících systémů nebo sítí. Tento model může být využíván především u dlouhodobých outsourcingových kontraktů, přičemž odběratel může mít díky němu stálou kontrolu nad kvalitou dodávané služby a nad skutečností, že služba např. i po několika letech stále plní aktuální požadavky právní úpravy (v tomto směru je třeba připomenout relativně vysokou pravděpodobnost postupných změn požadavků na bezpečnostní opatření v návaznosti na obecný technický vývoj). Certifikací mohou konečně procházet vedle celých bezpečnostních řešení i jen dílčí

systémy nebo dokonce jejich jednotlivé komponenty – typicky tak může být systém nebo síť podrobena experimentální bezpečnostní expozici v testovacím polygonu a na základě kvality její odezvy může být certifikační autoritou doporučena/nedoporučena pro nasazení v určitém typu informačního systému nebo sítě.

Vzhledem k tomu, že bezpečnostní opatření mohou být dle platné právní úpravy šita přímo na míru konkrétním systémům nebo sítím, je vhodné podporovat i takové certifikační iniciativy, které budou směřovány do konkrétních hospodářských resp. veřejnoprávních sektorů[89]. Lze očekávat, že profesně resp. sektorově orientované iniciativy mohou být v tomto směru mnohem efektivnější – je přitom logické, že typická bezpečnostní řešení v justici se budou zřejmě na úrovni technické i organizační zásadně odlišovat od bezpečnostních opatření aplikovaných v oblasti energetických systémů a sítí. Profesně resp. sektorově orientované iniciativy mohou v tomto směru přinést ve smyslu efektivity nejen odpovídající úroveň znalostí v oboru kybernetické bezpečnosti ale také poznatky ohledně specifických požadavků v příslušném odvětví nebo oboru.

Jako problematická jeví se konečně v současné situaci též rizika plynoucí z čistě podnikatelsky orientovaných iniciativ, které může indukovat shora popsaná poptávka. Nebude-li totiž problematika a priori aprobace bezpečnostních opatření řešena formou spolupráce orgánů veřejné moci, akademických institucí a odborně orientovaných a ideálně i agregovaných soukromých iniciativ, vytvoří se tím prostředí pro živelný vznik samozvaných razítkovacích produktů. Bude pak extrémně složité dostat takový čistě ekonomicky motivovaný chaos do situace, kdy bude možno se na příslušné certifikáty či jiné formy potvrzení z odborného hlediska skutečně spolehnout. Jen těžko si pak lze představit, jaké praktické důsledky by mohla mít situace, kdy by aprobaci bezpečnostních opatření nezávisle prováděli např. jednotliví znalci (bude-li zachována současná situace ohledně podmínek pro výkon a odbornou úroveň znalecké činnosti).

[89] Ke specifickým požadavkům v oboru energetiky viz např. Oliveira, D. Cyber-Terrorism & Critical energy Infrastructure Vulnerability to Cyber-Attacks, *Environmental & Energy Law & Policy Journal*, roč. 5, číslo 2, str. 519 a násl.

6.2 AKTIVNÍ OBRANA – BEST PRACTICES

K tématu aktivní obrany je nutno předeslat, že v současné době neexistuje žádná obecně uznávaná taxonomie jejích typických forem. Pokud už je téma aktivní obrany[90] předmětem odborných publikací, zaměřuje se debata buďto na technické aspekty konkrétních typů obranných opatření nebo na základní systematiku v rámci relativně úzce vymezených typů. Nelze však hovořit o žádné komplexní systematice a dokonce ani o definici, která by mohla pojem aktivních obranných opatření (aktivních protiopatření) alespoň rámcově popsat.

Za této situace je problematika aktivní obrany logicky spíše vědeckým zadáním a měla by být řešena spíše formou výzkumných aktivit a iniciativ. Jediným použitelným zárodkem obecné taxonomie aktivních protiopatření je tzv. Dagstuhlská taxonomie[91], která byla sestavena v rámci specializovaného semináře Leibnizovy nadace na podzim 2013 a reflektovala požadavky na systematiku z hlediska informatiky i právní vědy. Ani tato taxonomie však není prakticky použitená, neboť obsahuje pouze náznak základních kategorií a bude tedy nutno ji dále vyvíjet a doplňovat.

Aktuální praxe kybernetické bezpečnosti však nemůže čekat na výstupy vědeckých projektů, neboť aplikace aktivních protiopatření představuje v běžném fungování služeb informační společnosti každodenní nutnost. Vzhledem k tomu, že reálně užívaná aktivní protiopatření často zasahují do vlastnických či závazkových práv nebo dokonce naplňují formální znaky skutkových podstat trestných činů, představuje jejich uplatňování doposud šedou zónu a podnikatelé, kteří tato opatření používají, tak zpravidla činí skrytě. Dokonce ani technici vyvíjející a aplikující tato opatření na objednávku soukromoprávních subjektů často ani nejsou s těmito subjekty v žádném oficiálním právním vztahu.

Poněkud lepší je v tomto směru situace ve veřejném sektoru, přičemž typicky výkonné orgány mohou při užití aktivních protiopatření aplikovat

[90] K pojmu viz Kesan, J. P., Hayes, C. M. Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace, *Harvard Journal of Law And Technology*, roč. 25, číslo 2, str. 431.

[91] Viz Freiling, F. C., Hornung. G. Polcak, R. (eds.) Forensic Computing – report from Dagstuhl Seminar 13482, Dagstuhl: Dagstuhl Publishing, 2014, str. 204-205, publ. on-line na adrese http://drops.dagstuhl.de/opus/volltexte/2014/4442/pdf/dagrep_v003_i011_p193_s13482.pdf

obecná oprávnění založená jim v návaznosti na charakter chráněného zájmu. Ani v tomto případě však není situace úplně ideální, neboť při aplikaci obecných oprávnění často vyvstávají otázky ohledně rozsahu příslušných institutů. Orgány veřejné moci jsou rovněž v užití aktivních ochranných prostředků obecně omezeny mlhavými hranicemi vlastní institucionální legitimity – typicky tak armádní složky mohou užít svých extrémně širokých oprávnění pouze za situace, kdy jde o věc národní suverenity, bezpečnostní složky mohou aktivně jednat pouze v zájmu vnitřní nebo vnější národní bezpečnosti a orgány činné v trestním řízení mají manévrovací prostor vymezen agendou vyšetřování a stíhání trestných činů resp. ochranou veřejného pořádku.

Na jednoduchou otázku, jaké aktivní prostředky může užít policista zařazený do obvodního oddělení (je-li toho samozřejmě technicky schopen), když zjistí útok na web místního podnikatele, tedy neexistuje dokonce ani obecná odpověď. Podobně nejsme schopni odpovědět dokonce ani na mnohem prozaičtější otázky nemající charakter bezpečnostních problémů, typicky na otázku, jaké konkrétní aktivní prostředky lze použít při získávání elektronických důkazů z informační a komunikační infrastruktury.

Jak je však uvedeno shora, nemůžeme si dovolit reagovat na faktickou situaci jen pokrčením ramen a vývojem či tolerováním šedé zóny prakticky používaných, účinných a potřebných aktivních opatření, která však existují zcela mimo účinnou právní úpravu. Roli soukromoprávních iniciativ lze v tomto směru vidět především v komunikaci praktických potřeb a sběru a vyhodnocování informací ohledně prakticky používaných technik v různých odvětvích hospodářství a společenského života a v následném zpracovávání těchto poznatků do podoby technických resp. právovědných zadání pro další výzkum a legislativní praxi.

V porovnání se shora popsanou potřebou řešení certifikačních procedur však každopádně platí, že v otázce aktivní obrany nemáme prozatím k dispozici ani představu ohledně konkrétních potřeb a z nich vycházejících zadání pro organizační, technickou nebo legislativní realizaci. O to víc je samozřejmě nutno tuto otázku aktivně zpracovávat a řešit. V tomto směru je však nutno připomenout, že nemá smysl začít pracovat na řešení jakýchkoli partikularit bez současné představy o smyslu a účelu aktivních

protiopatření jako takových a o jejich reflexi základními principy, na nichž stojí náš právní řád.

6.3 KYBERNETICKÁ BEZPEČNOST JAKO AGENDA PODPORY INVESTIC

Jedním ze základních principů, na nichž stojí legitimita české právní úpravy, je princip bdělosti vzhledem k ostatním státům a mezinárodnímu společenství. Vedle shora popsané, byť stále nikoli prakticky uplatňované, částečné přičitatelnosti kybernetického útoku státu neschopnému při vynaložení rozumného úsilí zabránit zneužití informační a komunikační infrastruktury pod vlastní jurisdikcí, projevuje se tento princip i mnohem bezprostředněji, a to ve vztahu k ochraně investic. Česká republika je vázána obecnými procedurálními pravidly řešení sporů mezi státy a soukromoprávními investory doplněnými řadou bilaterálních dohod o ochraně investic zakládající pravomoc příslušných rozhodčích institucí – tato právní úprava vede ve výsledku k možnému založení odpovědnosti České republiky za investice zmařené v důsledku nelegitimního výkonu státní moci resp. v důsledku toho, že stát příslušné investice adekvátně neochrání.

Ve vztahu ke kybernetické bezpečnosti je možno konstatovat, že investor má v našich geopolitických reáliích oprávněná očekávání nejen co do fyzické bezpečnosti ale též co do obecné funkčnosti služeb informační společnosti. V případě, že stát není schopen zajistit fungující informační a komunikační infrastrukturu, jedná se z hlediska investora nejen o faktor při rozhodování o samotné lokalizaci investice ale může se jednat i o důvod založení odpovědnosti státu v případě, že investice byla uskutečněna a informační a komunikační infrastruktura není v důsledku bezpečnostní expozice adekvátně funkční.

Jedná se o podobnou situaci, jako kdyby stát nejprve nalákal investory na fungující dopravní infrastrukturu – ta by ale po nějakém čase přestala být použitelnou v důsledku častého výskytu dopravních přestupků, které policie nezvládá řešit. Podobnost s dopravní infrastrukturou však z hlediska investic samozřejmě není úplná - z tohoto srovnání však každopádně vychází jako dokonale absurdní zjištění, že kybernetická bezpečnost stále není předmětem agendy investiční konkurenceschopnosti České republiky.

V porovnání s dopravní infrastrukturou je potřeba investic do kybernetické bezpečnosti z hlediska nákladovosti o několik řádů méně náročnou. Současně lze poukázat na skutečnost, že bezpečně fungující informační a komunikační infrastruktura je relevantním faktorem lokalizace přesně těch typů investic, které jsou pro Českou republiku prioritní, tj. investic do oborů s vysokou mírou přidané hodnoty- Naproti tomu investice do dopravní infrastruktury, nepoměrně ve všech směrech náročnější, zdaleka neindukují jen ten typ investičního potenciálu, o který má mít Česká republika zájem (namísto toho jde o investice do nekvalifikované mechanické práce nebo jen manipulace se zbožím typu montoven nebo logistických center). Z toho plyne, že je absurdní, pokud Česká republika investuje v režimu podpory investic do rozvoje silniční nebo železniční sítě, aniž by ve stejném režimu investovala do zajištění služeb informační společnosti nebo kybernetické bezpečnosti.

Úloha soukromoprávních iniciativ typu oborových či profesních sdružení je v tomto směru evidentní především v otázkách přenosu informací mezi podnikatelským sektorem a veřejnou mocí. K náležitému nastavení resp. zaměření příslušných investic je totiž třeba především znát reálné potřeby adresátů investiční podpory. Platí přitom, že středně velcí a velcí mezinárodní investoři zpravidla nemají zájem o podporu nebo dokonce o zajištění interních systémů bezpečnosti informací. Naopak lze podle zahraničních zkušeností předpokládat, že adekvátní zaměření investiční podpory má vést k zajištění bezpečného fungování služeb informační společnosti a poskytovat v reálném čase metodiku a asistenci pro zvládání závažných kybernetických bezpečnostních incidentů s původem mimo příslušné podnikatelské subjekty.

Jinými slovy má z hlediska investora význam, pokud hostitelský stát investuje do nástrojů k obecnému zajištění bezpečného fungování informační a komunikační infrastruktury. V tomto směru je nutno připomenout, že investory vedle provozu jejich vlastních informační struktur zajímá též dostupnost informačních a komunikačních technologií ze strany jejich obchodních partnerů a široké veřejnosti, jakož i využití veřejně dostupných služeb informační společnosti k interním organizačním procesům (práce z domova, komunikace mezi pobočkami, provoz distančních spotřebitelských terminálů apod.) Profesní či oborové

organizace přitom mohou pomoci identifikovat konkrétní otázky v příslušných průmyslových odvětvích a koordinovat komunikaci mezi obchodní komunitou a orgány veřejné moci.

Pozitivní příklady důvěryhodné, efektivní a oboustranně výhodné vzájemné spolupráce na odborné úrovni není každopádně nutno brát jen ze zahraničí, byť je tato forma účasti průmyslových podniků na řešení odborných otázek veřejnou mocí běžná například v Německu, Spojeném Království nebo USA. Příkladem dobré praxe může být i shora zmíněný proces přípravy věcného záměru a posléze i textu paragrafového znění zákona o kybernetické bezpečnosti, kde se podařilo vést věcný dialog mezi podnikatelskou sférou a dotčenými veřejnoprávními korporacemi.

6.4 KYBERNETICKÁ BEZPEČNOST JAKO AGENDA ROZVOJOVÉ POMOCI

V současné době existují mezi jednotlivými státy velké rozdíly co do formy a intenzity řešení problematiky národní kybernetické bezpečnosti. Nedávná studie UNODC ukázala v tomto směru nikoli překvapivé obrovské rozdíly mezi rozvojovými a rozvinutými státy zjednodušeně označované jako rozdíly mezi severem a jihem[92]. Při následném projednávání výstupů této studie v rámci expertní skupiny UNODC pro kyberkriminalitu a kybernetickou bezpečnost byly tyto rozdíly nejen evidentní ale z nebývale ostré výměny názorů vyplynula potřeba zabývat se otázkou kybernetické bezpečnosti jako integrální součástí agendy rozvojové pomoci. Důležitost dostupnosti bezpečně fungující informační a komunikační infrastruktury je totiž možno srovnat s důležitostí ostatních základních společenských funkcionalit. Vlády rozvojových států však nedisponují dostatečnými finančními ani technickými kapacitami k jejímu zajištění[93].

Z výše uvedeného plyne, že účast rozvinutých států na investicích do bezpečnosti informační a komunikační infrastruktury v rozvojových státech má být motivována a legitimována stejnými morálními důvody jako např. potravinová pomoc nebo pomoc s rozvojem základní technické nebo

[92] Viz dokument Srovnávací studie počítačové trestné činnosti, publ. on-line na adrese http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

[93] Srov. Bande, L. C. A Case for Cybercrime Legislation in Malawi, *Malawi Law Journal*, roč. 5, str. 93.

dopravní infrastruktury. V tomto případě však nemusí být motivace rozvinutých států pouze morální resp. sociální, ale může jít o prostý důsledek utilitaristické úvahy ekonomické resp. politické.

Obecně platí, že je z hlediska nákladovosti výhodnější pokrývat kybernetické bezpečnostní incidenty pokud možno co nejblíže místu jejich vzniku, a to z hlediska časového i geografického. Poskytují-li pak rozvojové země z důvodu neschopnosti investovat do bezpečnostních opatření něco jako bezpečné přístavy pro vznik a vývoj kybernetických bezpečnostních incidentů, je logicky zájmem cílových států (a většinou jde naopak právě o státy rozvinuté) pokrýt příslušná bezpečnostní rizika shora popsaným způsobem.

Strategické zaměření rozvojové pomoci do sektoru kybernetické bezpečnosti může nikoli jen zprostředkovaně ale přímo pomoci řešení bezpečnostní situace nejen ve státech, kam pomoc přímo směřuje ale možná i významnějším způsobem v zemích, kde se kybernetické bezpečnostní incidenty projevují. Dárce tedy v tomto případě chrání prostřednictvím své intervence sám sebe (podobně jako např. rozvojová pomoc směřující ke zvyšování kvality života vede ke snižování nelegální migrace a omezování následných problémů ekonomických, sociálních apod.)

Rozvojová pomoc v sektoru kybernetické bezpečnosti má speciálně v případě České republiky ještě další rozměr, a to podporu tuzemského výzkumu, vývoje a průmyslu v oboru pokročilých informačních a komunikačních technologií. Česká republika se, dlužno říci i přes dosavadní absenci prakticky jakékoli veřejné resp. politické podpory, dostala na špici v oboru kybernetické bezpečnosti, ať už jde o oblast primárního výzkumu (nikoli jen v oboru ICT, ale i v oboru práva, psychologie nebo sociálních věd), experimentálního a aplikovaného vývoje či komerčních aplikací. Existuje tedy v současné době u nás řada akademických pracovišť a podnikatelských subjektů, jejichž výsledky jsou plně srovnatelné v mezinárodním (nikoli jen evropském) měřítku a mohou řešit nejen aktuální problémy naší národní kybernetické bezpečnosti, ale jsou použitelné prakticky v libovolném národním nebo nadnárodní prostřední. Zaměří-li se pak do toho sektoru prostředky určené na rozvojovou pomoc (tj. pokud budou české instituce díky českým

rozvojovým programům řešit problémy kybernetické bezpečnosti rozvojových zemí), bude tímto způsobem možno obecně podporovat další rozvoj tohoto sektoru v České republice, to přitom bez toho, aby se jednalo o zakázanou veřejnou podporu nebo jinou formu zakázaného narušování tržního prostředí.

7. SHRNUTÍ

V tomto textu jsme se zabývali vybranými problémy českého pojetí právní úpravy fenoménu kybernetické bezpečnosti. První část je věnována pojmové klasifikaci kybernetické bezpečnosti, jejím specifickým rysům a především pragmatické metodě, jejíž implementace jeví se být vhodná k řešení partikulárních regulatorních otázek. Ohledně metodologie práva kybernetické bezpečnosti dospěli jsme k závěru, že určující význam technologických aspektů tohoto regulatorního fenoménu prakticky vylučuje důsledné využití metod pozitivistických i přirozenoprávních. Za riziko pragmatické (realistické) metody jsme pak označili náchylnost k postupné hodnotové degradaci, přičemž jsme jako preventivní faktory identifikovali solidnost institucionálního a personálního zajištění implementace příslušných právních pravidel.

Další část textu byla věnována principům českého zákona o kybernetické bezpečnosti a dále pak stručnému rozboru základních institutů, na nichž zákon obsahově spočívá. Z pochopitelných důvodů nebylo možno zde provést kritickou analýzu účinné právní úpravy vzhledem k aktuální judikatuře a vzhledem k relativní unikátnosti českého legislativního řešení nebylo možno učinit ani odpovídající srovnání s příbuznými právními řády. Pokusili jsme se však alespoň kriticky diskutovat smysl a účel jednotlivých našich zákonných institutů, popsat jejich vzájemné systematické vazby a též zhodnotit formální konzistenci s deklarovanými principy resp. s hodnotovými fundamenty českého práva.

Poslední část textu byla věnována perspektivám dalšího vývoje fenoménu kybernetické bezpečnosti v České republice. Výklad byl rozdělen na legislativní zadání a na úkoly k politickým či organizačním úvahám. Společným motivem legislativních i politicko-organizačních perspektiv byla na prvním místě úzká spolupráce mezi veřejným a soukromým sektorem,

která jako jediná může vzhledem k zásadní důležitosti konkrétních forem technické implementace zákonných povinností zajistit skutečné fungování celého regulatorního systému. Druhým podstatným momentem diskutovaným v této části pak byly výjimečně dobré výsledky české vědy a průmyslu v oboru informační bezpečnosti i pozoruhodné úspěchy té části veřejné moci, do jejíž kompetence spadal vývoj a implementace specifických právních pravidel – k nim však stojí v naprosté kontrapozici pouze občasný verbální zájem o tuto problematiku ze strany českých politických elit. Přestože tedy na poli kybernetické bezpečnosti hrají některé české akademické, soukromé i veřejné instituce příslovečnou Ligu mistrů, je povědomí a podpora ze strany politických špiček v této oblasti spíše na úrovni župního přeboru.