13 Nedistributivní práva k informacím

13.1 Informační veřejná dobra

Ke stručné diskusi proměn v axiologii základních ochranných institutů informační společnosti jsme v minulé kapitole použili systematiku založenou na distributivnosti práv. Dospěli jsme k závěru, že většina v současné době dominantně traktovaných informačních práv má distributivní charakter, přičemž jejich aktuálně důležitou součástí je nutně též restriktivní prvek. Odstranění informačních restrikcí jsme pak identifikovali jako dominantní aspekt změn, jimiž právo v současné době prochází a které jej budou charakterizovat i v blízké budoucnosti.

Priorita distributivních informačních práv je logickým důsledkem v minulé kapitole rovněž konstatované orientace euroatlantického práva na člověka a na jeho individuální svobodu. Jak jsme popsali v páté kapitole, reprodukci naší současné informační společnosti však nelze dosáhnout pouze na základě mocenské ochrany distributivních práv, ale nutně též produkcí a aplikací vyššího řádu pravidel, jejichž hlavním garantem je i přes pokračující nástup fenoménu ISP stát.[1]

Roli státu při ochraně nedistributivních organizačních informací lze chápat dvojím způsobem. Jednak lze ztotožnit stát s jeho právním řádem a konstatovat, že veřejná dobra představují sadu pravidel, jejichž nedělitelnost na jednotlivé subjekty vede v důsledku k unikátní možnosti jejich uplatnění ze strany státu.[2] Veřejné dobro je tedy v tomto případě možno chápat jako dobro jednotlivce, jehož ochrana však má kvůli jeho nedělitelnosti charakter přímé státní aktivity.[3] Byť je tedy i veřejné dobro ve svém důsledku směřováno k jednotlivci, není kvůli své podstatě individuálně chráněno, ale jeho ochrana má kolektivní (státní) charakter. Takové chápání nedistributivních práv je běžné v kontinentální Evropě.

Druhou možností je přistupovat k veřejným dobrům prostřednictvím oddělení státu a práva. Veřejná dobra v takovém případě představují klasická distributivní (absolutní) práva, jejichž oprávněným subjektem není jednotlivec ale stát. Právní řád v tomto pojetí tedy státu dává specifický katalog „jeho“ unikátních subjektivních práv a svěřuje mu též aktivní legitimaci k jejich vymáhání.[4] Takové pojetí nedistributivních práv je typické v zemích angloamerické právní kultury.

Z tohoto elementárního rozdílu ve vnímání základní filozofie nedistributivních práv samozřejmě neplynou žádné zásadní materiální závěry – hodnoty společného významu jsou totiž chráněny v obou právních kulturách prakticky ve srovnatelné míře, liší se jen použitá technika a terminologie. Významný je však tento rozdíl při posuzování jednotlivých formálních podrobností souvisejících s jejich ochranou. Je pak například pro angloamerickou právní kulturu filozoficky jednodušší přenést výkon nedistributivních práv na soukromou osobu, neboť charakter těchto práv zůstává tentýž a mění se pouze aktivně legitimovaný subjekt. Naproti tomu je přenos odpovědnosti a kompetencí k výkonu a ochraně

[1] K pojmu nedistributivních práv a kolektivních dober z hlediska sociologického a ekonomického viz např. KIESLING, J. H. *Collective Goods Neglected Goods.* Singapure : Word Scientific Publishing, 2000, str. 29 a násl. K nezastupitelnosti role státu viz SHERAING, C.; WOOD, J. Governing Security for Common Goods. *International Journal of the Sociology of Law*. 2003, roč. 31, č. 3, str. 212.

[2] Hegel k tomu říká: „Stát je jakožto skutečnost substanciální vůle, kterou má ve zvláštním sebevědomí povýšeném do své obecnosti tím, co je o sobě a pro sebe rozumné. Tato substanciální jednota je absolutní nehybný samoúčel, ve kterém svoboda dospívá ke svému nejvyššímu právu, tak jako tento konečný účel má nejvyšší právo vůči jednotlivcům, jejichž nejvyšší povinností je být členy státu.“ – Viz HEGEL, G. W. F. *Základy filozofie práva*, přel. Špalek, V. Praha : Academia, 1992.

[3] Srov. HOLLÄNDER, P. *Základy všeobecné státovědy*. Plzeň : Aleš Čeněk, 2009, str. 104.

[4] Bentham v této souvislosti hovoří o suverénovi jako o nositeli „korektivní moci“ – srov. BENTHAM, J. *Leviathan*. Project Gutenberg, 2002.

nedistributivních práv v Evropě mnohem složitější – vyžaduje totiž nejprve filozoficky obtížnou modifikaci těchto práv na hybrid se znaky distributivního práva a jeho následné přiřazení specifickým subjektům. I proto je v evropské praxi velmi obtížné a často z filozofického i společenského hlediska vysoce citlivé privatizovat výkon nedistributivních práv, ať už jde o ochranu zdraví, zajištění státní bezpečnosti, ochranu veřejného pořádku apod.

Podobně, jako to Warren s Brandeisem konstatovali v případě distributivního práva na ochranu soukromí,[5] platí, že i struktura a obsah dalších právních institutů se vyvíjí v čase v návaznosti na společenském vývoji. Rychlost tohoto vývoje u informačních práv byla v posledních dekádách v důsledku nástupu informačních a komunikačních technologií doslova překotná.[6] Přestože se s důsledky rychlého vývoje v kvantitativních aspektech informační společnosti nejviditelněji potýkáme v případě distributivních práv, je čím dál tím jasnější, že byly nástupem ICT závažným způsobem změněny i možnosti státu dostát jeho primární odpovědnosti, tj. formou prosazování nedistributivních práv a ochrany distributivních práv mocensky zajišťovat společenskou reprodukci.[7] Přestože se tedy zdá být následující výklad co do důležitosti ve zřejmém nepoměru s tématy diskutovanými v předchozí kapitole, domníváme se, že kombinace rychlého technického a společenského rozvoje, faktické důležitosti nedistributivních práv a jejich dosavadní upozaďování může se projevit fatálním způsobem na míře organizovanosti informační společnosti.

Oproti závažným bezpečnostním a systémovým rizikům plynoucím z opomíjení nedistributivních práv, jeví se příkladně široce diskutovaná autorskoprávní otázka (které jsme i zde pohříchu věnovali podstatnou část předchozí kapitoly) jen jako bezvýznamná hra o pár drobných[8]. Z těch nedistributivních práv, která mají dominantně informační charakter,[9] jsme jako aktuálně nejzávažnější vybrali:

- Dostupnost informační infrastruktury
- Kybernetickou bezpečnost
- Informační práva státu

Vzhledem k tomu, že jsme se problému dostupnosti informační infrastruktury věnovali v souvislosti s kvantitativními aspekty budování informační společnosti v předminulé kapitole,[10] zaměříme se v dalším výkladu především na problematiku kybernetické bezpečnosti a informačních práv státu. Vedle shora zmíněné fatální kombinace rychlého technického vývoje, malého společenského zájmu a zásadní důležitosti nedistributivních informačních práv je pro jejich diskusi především v postkomunistické Evropě důležitý ještě

[5] Viz WARREN, S. D.; BRANDEIS, L. D. The Right to Privacy. *Harvard Law Review*. 1890-1891, č. 4, str. 195.

[6] Někteří autoři v této souvislosti poukazují na skutečnost, že zatímco obory jako ekonomie nebo sociologie mají díky masivnímu nástupu ICT bohatý materiál ke zkoumání, historické vědy prakticky nemají, čím by do odborné diskuse přispěly. Srov. WEBSTER, F. Understanding the Information Domain: The Uneasy Relations between Sociology and Cultural Studies and the Peculiar Absence of History. In RAYWARD, W. B. (ed.) *European Modernism and the Information Society*: *Informing the present, understanding the past*. Hampshire : Ashgate Publishing Limited, 2008, str. 27 a násl.

[7] K poměru svobody a reprodukce k mocenským kompetencím státu viz HOLLÄNDER, P. *Filosofie práva*. Plzeň : Aleš Čeněk, 2006, str. 102.

[8] Srov. KOKEŠ, M. Několik poznatků k problematice konkrétních konfliktů mezi právem na informační sebeurčení a ochranou národní bezpečnosti v tzv. době internetové. In ŠIMÍČEK, V. (ed.) *Právo na soukromí*. Brno : Mezinárodní politologický ústav, 2011, str. 119 a násl.

[9] Nástupem ICT byla zasažena celá řada nedistributivních informačních práv, jejichž komponentou jsou též práva informační – těm se však v následujícím výkladu nebudeme věnovat. Jedná se například o zajištění obecného veřejného pořádku, ochrana přirozeného životního prostředí apod. Jedná se však v tomto případě o situace, kdy informační a komunikační technologie slouží jako náhražka jiných (dřívějších) komunikačních kanálů a samotná podstata nedistributivních práv se nijak nemění.

[10] Jedná se v tomto směru zejména o problém digital divide a aproximativní rovnosti uživatelů (potenciálních uživatelů) služeb informační společnosti – viz výklad ke kvantitativním aspektům budování národní a globální informační společnosti v jedenácté kapitole.

další faktor společenských změn souvisejících s relativně nedávnou změnou politického systému. Byla to totiž právě nedistributivní práva, která si autoritářské komunistické režimy braly za záminku drastického omezování distributivních základních práv a svobod.[11] Národní bezpečnost či veřejný pořádek tak byly pravidelným důvodem k omezování svobody slova, soukromí nebo osobní svobody.[12] Jestliže je tedy dnes nutno ošetřit kvalitativně nové formy ochrany informační společnosti a v souvislosti s nimi též řešit proporcionální aplikaci distributivních a nedistributivních práv[13], je třeba předpokládat v postkomunistické části Evropy historicky danou *a priori* nedůvěru k instituci státu a k jeho aktivitám.[14] Až příliš živé je totiž v tomto regionu spojení instituce státu s jevy, jako jsou strach nebo svévole (či spíš buzerace).

> Právě uvedené lze dokumentovat i na rozhodovací praxi v první fázi českého ústavního soudnictví. Náš Ústavní soud původně dokonce odmítal uznat nedistributivní veřejná dobra za dostatečně relevantní k tomu, aby mohla být poměřována se základními právy. V případě, kdy bylo třeba posoudit ústavní konformitu nešťastně upraveného institutu anonymního svědka,[15] tak soud proti sobě nestavěl omezení práva na spravedlivý proces proti zájmu na ochraně veřejného pořádku ale proti individuálnímu distributivnímu právu svědka na ochranu jeho zdraví a života.[16] Elementární empiricko-logická úvaha však prvořadou důležitost ochrany zdraví a života svědka v tomto případě prakticky vylučuje – pokud by zde šlo o to chránit zdraví a život svědka, postačilo by přeci dát mu elegantní možnost odepřít výpověď z důvodu obavy o vlastní bezpečnost (všichni, ovšem kromě státu, by v takovém případě dostali své). Namísto toho jde samozřejmě primárně o to motivovat svědka k tomu, aby vypovídal, a zajistit mu k tomu pocit bezpečí před odplatou tak, aby mohl stát stíhat a trestat závažnou trestnou činnost. Pár let po společensko-politických změnách však evidentně nebylo vhodné poměřovat právo na spravedlivý proces s něčím tak zprofanovaným, jako byl veřejný pořádek či dokonce veřejná bezpečnost.

Při diskusi bezpečnostních opatření k ochraně informační infrastruktury se v našem regionu automaticky rozpomínáme na cenzuru a při debatách o telekomunikačních provozních údajích nás nutkají myšlenky na komunistické fízlování. Paradoxně pak jsou často reakce na pokusy o ochranu nedistributivních informačních práv na internetu vedoucích vždy nutně k solidárnímu omezení individuální svobody jednotlivce mnohem citlivější v postkomunistické Evropě, než je tomu v tradičně liberálních státech západní Evropy nebo v USA.[17]

13.2 Koncepční otázky kybernetické bezpečnosti

K problému kybernetické bezpečnosti je třeba přistupovat pragmaticky a prostřednictvím aktuálních empirických informací. Určující roli v diskusi o tom, zda a jak by se právo mělo otázkou kybernetické bezpečnosti zabývat, tedy musí hrát ústřední roli údaje o charakteru infrastruktury, kterou je třeba chránit, jakož i zkušenosti s dosavadními bezpečnostními

[11] Srov. GÁBRIŠ, T. Posilňovanie roly štátu a verejného práva v Československu v rokoch 1948-1989. In BOBEK, M.; MOLEK, P.; ŠIMÍČEK, V. (eds.). *Komunistické právo v Československu*. Brno : Masarykova univerzita, 2009, str. 145.
[12] Srov. ROSE, R. *Understanding post-communist transformation: a bottom up approach*. Oxon : Routlege, 2009, str. 97.
[13] Problému proporcionality v ochraně distributivních a nedistributivních informačních práv se specificky ve vztahu k ochraně informační diskrece věnuje Pavol Holländer v práci HOLLÄNDER, P. Zásada proporcionality: Jednosměrná ulice nebo hermeneutický kruh? Na příkladech veřejných dober a základních práv kolidujících s právem na soukromí. In ŠIMÍČEK, V. (ed.) *Právo na soukromí*. Brno : Mezinárodní politologický ústav, 2011, str. 20 a násl.
[14] Viz tamtéž, str. 153.
[15] Viz nález pléna Ústavního soudu ze dne 12.10.1994, sp. zn. Pl.ÚS 4/94, 214/1994 Sb., N 46/2 SbNU 57. Dostupné z: <www.nalus.usoud.cz>.
[16] Soud k tomu v odůvodnění doslova uvedl: „Základní je v této souvislosti maxima, podle které základní právo či svobodu lze omezit pouze v zájmu jiného základního práva či svobody."
[17] Důvody této dnešní situace shrnuje Eliška Wagnerová v textu WAGNEROVÁ, E. Základní práva. In BOBEK, M.; MOLEK, P.; ŠIMÍČEK, V. (eds.). *Komunistické právo v Československu*. Brno : Masarykova univerzita, 2009, str. 330 a násl.

problémy.[18] Nemá smysl předvídat budoucí technický vývoj a vytvářet specifické ochranné instituty resp. budovat ochranné veřejnoprávní instituce k bezpečnostním hrozbám, jejichž výskyt můžeme teprve tušit.[19] Dosavadní zkušenosti totiž ukazují, že předpovědi dalšího bezpečnostního vývoje informační sítě v horizontu odpovídajícímu legislativnímu cyklu se jen zřídka naplňují.[20] Alokaci zdrojů je třeba namísto toho nejprve pragmaticky zaměřit na řešení současných (tj. známých) problémů, jejichž výskyt již začíná mít pro standardní fungování státu fatální rozsah.[21]

Národní analýzy kybernetické bezpečnostní situace[22] se shodují v tom, že kritická komunikační infrastruktura státu zahrnuje nejen státní informační kanály a informační zdroje ale též standardní komunikační prostředky užívané širokou veřejností.[23] I výpadek nebo poškození důvěryhodnosti na první pohled banálních služeb informační společnosti, jako jsou služby mobilních komunikací, e-mail apod., totiž může způsobit značné ekonomické ztráty, chaos nebo snížení společenské a mezinárodní důvěry ve stát a jeho instituce.[24] Zajištění kybernetické bezpečnosti je tedy i na nejvyšší úrovni otázkou ochrany nejen vitálních informačních funkcionalit státu, ale též síťové informační infrastruktury užívané podnikatelským sektorem a širokou veřejností.[25] Alokaci zdrojů, jakož i tvorbu právních pravidel je tedy třeba směřovat nejen ke státním informačním strukturám, ale je nutno k zachování vitálních společenských funkcionalit státu komplexně chránit i komunikační infrastrukturu soukromého resp. občanského sektoru.[26]

Dosavadní analýzy rovněž vedou k závěru, že část kybernetických útoků a jiných bezpečnostních incidentů lze kategorizovat,[27] popsat jejich standardní rysy a vypracovat

[18] Srov. SKOUDIS, E. Information Security Issues in Cyberspace. In KRAMER, D. F.; STARR, S. H.; WENTZ, L. K. *Cyberpower and National Security*. Dulles : Protomac Books, 2009, str. 171 a násl.

[19] Z psychologického hlediska by sice bylo lépe žít s pocitem, že jsme připraveni na budoucí hrozby, společnost se však již začíná postupně smiřovat s jistou mírou rizika a bezmocnosti ve vztahu k novým typům hrozeb – srov. ZATKO, P. M. Psychological Security Traps. In ORAM, A.; VIEGA, J. *Beautiful Security*. Cambridge : O'Reilly Media, 2009, str. 2.

[20] Pokud už nějaké prognózy existují, mají charakter velmi obecných výhledů nebo nekonkrétních upozornění na to, že problematika kybernetické bezpečnosti bude nabývat na společenské, ekonomické i mezinárodně-politické důležitosti – srov. např. příručku *National Telecommunications Board, Cybersecurity Today and Tomorrow: Pay Now or Pay Later*. Washington, D. C. : National Academy Press, 2002 nebo též GALLAHER, M. P.; LINK, A. N.; ROWE, B. *Cybersecurity – Economic Strategies and Public Policy Alternatives*. Cheltenham : Edvard Elgar Publishing Limited, 2008, str. 16.

[21] Daniel Geer shrnuje důležitost otázek kybernetické bezpečnosti a odkazuje přitom na národní hymnu USA následovně (překlad RP): „Toto jsou zásadní problémy. Týkají se základů suverenity i základů kultury. Týkají se základů 'land of the free and home of the brave'. Nemohou být řešeny centrálně, ale přitom nemohou být řešeny bez centrální pomoci." – viz GEER, D. E. Cybersecurity and National Policy. *Harvard National Security Journal*. 2010, č. 1, str. 12.

[22] Vzhledem k tomu, že metodika analyzování kybernetických bezpečnostních hrozeb se teprve vyvíjí, mohou být dílčí závěry dosavadních statistik zavádějící. Je však třeba pragmaticky pracovat s daty, která jsou k dispozici, neboť, prostě řečeno, nic lepšího prozatím nemáme. To mimo jiné dokládá nutnost použití pragmatické metodologie – srov. NICHOLS, E. A. Beautiful Security Metrics. In ORAM, A.; VIEGA, J. *Beautiful Security*. Cambridge : O'Reilly Media, 2009, str. 33.

[23] Viz dokument Souhrnná informace o stavu kybernetické bezpečnosti v České republice a předpoklady jejího zajištění na období 2011-2015 [on-line]. Centrum kybernetické ochrany ČR [cit. 20. 7. 2011]. Dostupné z: <www.govcert.cz>. Konkrétní příklad provázanosti kybernetické bezpečnosti s vitálním prvkem národní infrastruktury dávají Sarnikar a Johnsen v ekonomické analýze kybernetické bezpečnostní situace vzhledem k finančním trhům – viz SARNIKAR, S., JOHNSEN, D. B. Cybersecurity in the National Market Systém. *Rutgers Business Law Journal*. 2009, č. 6, str. 1.

[24] Příkladem mohou být kybernetické bezpečnostní incidenty, při nichž byla ochromena národní informační infrastruktura Estonska nebo Gruzie – viz McGAVRAN, W. Intended Consequences: Regulating Cyberattacks. *Tullamore Journal of Technology and Intellectual Property*. 2009, č. 12, str. 263. Další studie méně známých, avšak rovněž závažných bezpečnostních incidentů z Jižní Koreje z roku 2009 nebo z Japonska z roku 2010 přidává článek REICH, P. C.; WEINSTEIN, S.; WILD C.; CABANLONG A. S., Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents - and the Dilemma of Anonymity. *European Journal of Law and Technology*. 2002, roč. 2, č. 1, str. 14 a násl.

[25] Srov. FISHER, E. A. Creating a National Framework of Cybersecurity. In CHOI, L. V. (ed.) *Cybersecurity and Homeland Security*. New York : Nova Science Publishers, 2004, str. 14.

[26] Viz SOLMS, S. H. *Information Security Governance*. New York : Springer Media, 2009, str. 23. Spolupráci se soukromým sektorem nelze v tomto případě považovat za nějaké klišé či povinnou jízdu – Daniel Geer ve své eseji o národní kybernetické bezpečnosti píše, že jen tak lze docílit toho, že se vzhledem ke kebyrnetické bezpečnosti „posuneme od kultury strachu ke kultuře povědomí, ke kultuře znalosti" – viz GEER, D. E. Cybersecurity and National Policy. *Harvard National Security Journal*. 2010, č. 1, str. 2.

[27] Srov. např. v naší literatuře pokus o takovou systematiku v práci POŽÁR, J. *Informační bezpečnost*. Plzeň : Aleš Čeněk, 2005.

k jejich ošetření automatizované nebo alespoň standardizované mechanismy.[28] Vzhledem ke stálému vývoji ICT však řadu kybernetických hrozeb předem nelze popsat a nelze k nim ani vytvořit obranný mechanismus – obrana proti nim tak musí být záležitostí adekvátní reakce na vzniklou situaci za užití kreativního přístupu a aktuálních odborných znalostí.[29]

Z výše uvedeného plyne, že právní rámec pro zajištění nedistributivní národní kybernetické bezpečnosti musí předně počítat se dvěma druhy kompetencí, tj. vzhledem ke státní a soukromé informační infrastruktuře. Rovněž pak je třeba nastavit kompetence a zajistit odpovídající institucionální zázemí k řešení standardních incidentů, jakož i k instantnímu kreativnímu vývoji a implementaci bezpečnostních opatření v reakci na nové formy bezpečnostních incidentů a hrozeb.

Z právního hlediska představují pro efektivní zajištění kybernetické bezpečnosti zásadní výzvu především princip, že státní orgány mohou činit jen to, co jim právo ukládá nebo umožňuje a dále pak skutečnost, že efektivní bezpečnostní opatření včetně nasazení odpovídajících technických prostředků téměř vždy vyžadují zásah do distributivních informačních práv člověka. První jmenovaný princip je problematický především z toho důvodu, že vyžaduje dostatečně konkrétní specifikaci jednotlivých možností státních orgánů aktivně jednat.[30] V situaci, kdy zajištění kybernetické bezpečnosti permanentně vyžaduje průběžnou tvorbu kvalitativně nových řešení k reakci na kybernetické útoky, pak dochází k dilematu mezi faktickou nemohoucností státu a příliš obecným vymezením příslušných kompetencí. Je tedy třeba v tomto případě volit, ostatně jako vždy v podobných případech, kompromis mezi neakceschopností státu a rizikem zneužití státní moci.

Situace je navíc u kybernetických bezpečnostních hrozeb specifická v tom, že zatímco se reprodukční cyklus standardních forem, v nichž je zasahováno do nedistributivních veřejných statků, počítá na dekády, je v tomto případě třeba reagovat v řádu let nebo dokonce měsíců. I tam, kde je možno popsat standardní kybernetické hrozby, tedy dochází k tomu, že specificky určené možnosti státu mohou zastarat ještě před tím, než příslušná legislativa vstoupí v platnost.[31]

Právě pojmenovaný problém však má v oblasti kybernetické bezpečnosti specifickou možnost řešení, a to formou zapojení institucí, které mohou sledovat veřejný zájem a jednat přitom *praeter legem*. Stát může motivovat (zejména finančně) ke spolupráci akademický, podnikatelský a občanský sektor k aktivnímu zapojení do systému ochrany kybernetické bezpečnosti – tyto subjekty pak mohou dělat vše, co jim není zákonem výslovně zapovězeno, a to včetně vývoje a implementace bezpečnostních opatření proti nově vyskytnuvším se kybernetickým hrozbám.[32] Možností, jak tuto formu spolupráce realizovat, je celá řada – od přímých smluv nebo grantové podpory až po zavedení povinného sektorového používání blíže

[28] Srov. např. TANG, Y.; LUO, X.; CHANG, R. Protecting Internet Services from Low-Rate DOS Attacks. In GETZ, E.; SHENOI, S. (ed.) *Critical Infrastructure Protection*. New York : Springer Science+Business Media, 2008, str. 251 nebo McGAVRAN, W. Intended Consequences: Regulating Cyberattacks. *Tullamore Journal of Technology and Intellectual Property*. 2009, č. 12, str. 261 a násl.

[29] Srov. CORDESMAN, A. H. *Cyber-threats, information warfare, and critical infrastructure protection*. Westoport: Prager Publishers, 2002, str. 153.

[30] Tento problém ve vztahu k ochraně soukromí diskutuje Pavel Mates v publikaci MATES, P. *Ochrana soukromí ve správním právu*. Praha : Linde Praha, 2006, str. 14. 225.

[31] Srov. GALLAHER, M. P.; LINK, A. N.; ROWE, B. *Cybersecurity – Economic Strategies and Public Policy Alternatives.* Cheltenham : Edvard Elgar Publishing Limited, 2008, str. 62 nebo FISHER, E. A. Creating a National Framework of Cybersecurity. In CHOI, L. V. (ed.) *Cybersecurity and Homeland Security*. New York : Nova Science Publishers, 2004, str. 25.

[32] Tento přístup zdůrazňuje i Eric Fisher v návrhu systematického řešení národní kybernetické bezpečnosti USA – viz FISHER, E. A. Creating a National Framework of Cybersecurity. In CHOI, L. V. (ed.) *Cybersecurity and Homeland Security*. New York : Nova Science Publishers, 2004, str. 33 a násl.

nespecifikovaných bezpečnostních technologií s tím, že vývoj těchto technologií, tj. jejich aktuální stav, bude otázkou průmyslové standardizace a případně i veřejnoprávní certifikace.[33]

Poslední jmenovaná možnost jeví se být velmi vhodnou alternativou, neboť implementace bezpečnostních opatření nemusí být nutně vždy spojena s rozhodovací pravomocí. Často tedy není třeba, aby na kybernetickou hrozbu reagoval operátor, ale postačí implementace technologie, která se o adekvátní reakci postará automaticky. Stát pak může nařídit používání určité technologie a formou certifikace dohlížet na její kvalitu, přičemž její kontinuální vývoj a implementace změn již nevyžaduje další legislativní práci.

Právě uvedené potvrzuje poněkud problematický trend ztráty přímé regulatorní kontroly státu nad informační společností, který jsme popsali v páté kapitole. Jedná se totiž o situaci, kdy stát nedefinuje konkrétní pravidla chování (v tomto případě konkrétní pravidla fungování informační infrastruktury vzhledem k bezpečnostním hrozbám), ale pouze kontroluje, aby příslušně motivovaná soukromá nebo občanská normotvorba (zde formou tvorby konkrétních parametrů bezpečnostní technologie) odpovídala státnímu zájmu.[34] Skutečná právní regulace má v tomto případě charakter nikoli bezprostřední definice norem chování pro jejich adresáty, ale pouze nastavení základních regulačních parametrů, delegace technických kompetencí a následného dohledu nad definičními autoritami přímo provádějícími technickou (faktickou) regulaci.

Ideální by samozřejmě bylo, kdyby mohl stát tyto technické bezpečnostní funkcionality realizovat bezezbytku sám. Podobně jsme takovou ideální situaci popsali i v případě státní informační infrastruktury, systému promulgace práva, systémů k podpoře soudního rozhodování aj. Realita však bohužel ukazuje, že stát, často vlastní vinou, připravil se o technické kompetence a technologický potenciál a není tedy schopen následovat dnes aktuální technický a společenský vývoj. Pragmaticky tedy v tomto případě neexistuje volba z nějakých alternativ respektive lze volit pouze mezi hybridním modelem právní regulace při zapojení soukromých, občanský či akademických definičních autorit a modelem rezignace na ochranu nedistributivních veřejných statků, v tomto případě národní kybernetické bezpečnosti.[35]

Model spolupráce státu se soukromým, občanským nebo akademickým sektorem je úspěšně uplatňován v zemích, kde se otázka veřejné kybernetické bezpečnosti řeší již po několik let nebo dokonce dekád. Přístupy zavedené v USA, Německu či Spojeném království jsou vesměs postaveny na kombinaci přímých státních pravomocí, dohledového systému a státem dozorované certifikace bezpečnostních technologií, jejichž používání je dobrovolné formou průmyslové standardizace či *best practices*[36] nebo povinné jako podmínka k provozování veřejné komunikační infrastruktury.[37] Tam, kde je předmětem ochrany státní komunikační infrastruktura, pak jsou přímo aplikovány nekompromisní organizační a regulační mechanismy respektive přímo nasazeny výkonné složky státního ochranného aparátu (policie, bezpečnostní úřady, informační služby, armáda apod.) – tím, kdo je takovými bezpečnostními opatřeními v tomto případě omezen, je totiž na rozdíl od veřejné komunikační

[33] Někteří autoři hovoří v této souvislosti o vytvoření národní či dokonce mezinárodní základny nástrojů, z nichž bude možno vybírat adekvátní kombinaci pro každý typický případ – srov. REICH, P. C.; WEINSTEIN, S.; WILD, C.; CABANLONG, A. S. Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents - and the Dilemma of Anonymity. *European Journal of Law and Technology*. 2002, roč. 2, č. 1, str. 31.

[34] Srov. SHARP, W. G. The Past, Present and Future of Cybersecurity. *Journal of National Security Law and Policy*. 2010, č. 4, str. 22.

[35] Srov. OPHARDT, J. Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield. *Duke Law and Technology Review*. 2010, č. 3, str. 6, 16.

[36] Srov. BALACHEF, B.; CHEN, L.; PEARSON, S.; PROUDLER, G.; CHAN, D. Computing Platform Security in Cyberspace. *Information Security Technical Report*. 2000, č. 5, str. 54.

[37] Přehled systému ochrany národního kyberprostoru za užití kombinace různých opatření a institucionálních přístupů v USA podává dokument *The National Strategy to Secure Cyberspace* [on-line]. US-CERT [cit. 25. 3. 2009]. Dostupné z: <www.us-cert.gov/reading_room/cyberspace_strategy.pdf>.

infrastruktury pouze sám stát a není tedy třeba zásadně řešit citlivou otázku proporcionality distributivních a nedistributivních práv.

Jak vyplývá z výše uvedeného, představuje problematické zadání pro legislativní a organizačně-institucionální zajištění kybernetické bezpečnosti především ochrana veřejného kyberprostoru, tj. veřejné komunikační infrastruktury (zejm. internetu a mobilních komunikačních sítí). Částečně problematická je však též ochrana vlastní informační infrastruktury státu – ta totiž není koherentní, ale dělí se dle kompetencí jednotlivých státních orgánů. Dělení této komunikační infrastruktury tak v první řadě kopíruje ústavní princip dělby moci na zákonodárnou, výkonnou a soudní.[38] V rámci moci výkonné či soudní pak můžeme vidět další specifikaci, přičemž řada institucí nebo jejich součástí je budována na principu silné vzájemné nezávislosti.

Jestliže opatření k zajištění kybernetické bezpečnosti státu vyžadují vždy určitý zásah do informační diskrece chráněných prvků, plyne z výše uvedeného zejména problém zachování vzájemné nezávislosti státních institucí při současném zajištění žádoucí centralizace bezpečnostních řešení.[39] Je velmi problematické spojit žádoucí centralizaci ve sběru, vyhodnocování a reakci na informace o kybernetické bezpečnostní situaci s rovněž žádoucím mocenským oddělením jednotlivých státních institucí. I jen pouhý přístup k provozním údajům z informační infrastruktury jednoho státního orgánu totiž může příslušnému orgánu bdícímu nad bezpečností kyberprostoru přinést informace respektive kompetence, kterých lze v často nikoli otevřeně přiznaném avšak nepochybně existujícím vzájemném soupeření státních orgánů jednoduše využít.

> K ilustraci právě uvedeného můžeme použít jednoduchý příklad ze vztahu mezi mocí soudní a výkonnou. V České republice jsou jednotlivé soudy připojeny k internetu prostřednictvím Ministerstva spravedlnosti. Znamená to, že veškerá internetová komunikace soudů může být ministerstvem prakticky libovolně monitorována (nic takového jako šifrování e-mailů nebo skrývání identity při prohlížení www stránek v naší justici neexistuje). Už to samo o sobě vyvolává značné pochybnosti, pokud jde o oddělení soudní moci od moci výkonné (resp. politické). Ministerstvo jako ultimátní definiční autorita však jde ještě dále, když s poukazem na bezpečnostní rizika filtruje soudům připojení k cílovým místům prostřednictvím protokolu http (tj. k webovým stránkám) – až směšně jednoduchý systém filtrování na základě klíčových slov pak příkladně blokoval justici přístup na stránky prezidenta republiky s poukazem na to, že obsahují extremistické výrazy. Nehledě na to, že je v tomto případě justice pasována do role malého dítěte, kterému jeho starostlivý rodič (zde ministerstvo) předepisuje, na co se smí na internetu dívat, působí takové „bezpečnostní opatření“ dokonce i problémy v každodenní soudní praxi. Soudce studující internetové projevy webových extremistů nebo posuzující případ internetové sítě distribuující dětskou pornografii se k informacím potřebným pro meritorní rozhodnutí ve věci prostě nedostane (nehledě na nemožnost provést v jednací síni, nedovolí-li to blahosklonně ministerský informatik, důkaz webovou stránkou). Je v tomto směru s podivem, že tato skandální situace mající charakter totálního uplatnění informační kontroly správní (politické) moci nad soudnictvím, trvá již několik let.[40]

Nekompromisní řešení kybernetické bezpečnosti samozřejmě může v některých případech vyžadovat i určitou míru kontroly nad obsahovou stránkou komunikace. Řada bezpečnostních hrozeb, např. virů, trojských koní apod. má totiž ve svém zárodku charakter kvantitativními

[38] K důvodu a podstatě tohoto dělení viz např. HOLLÄNDER, P. *Základy všeobecné státovědy*. Plzeň : Aleš Čeněk, 2009, str. 326.

[39] K potřebě centralizace tam, kde fakticky existuje informační konkurence mezi jednotlivými státními institucemi, se na příkladu USA vyjadřuje Mark Young v důkladném analyticko-historickém článku YOUNG, M. D. National Cyber-Doctrine: The Missing Link in the Application of American Cyber Power. *Journal of National Security Law and Policy*. 2010, č. 4, str. 180.

[40] Namísto razantních reakcí se doposud objevují jen občasná povzdechnutí soudců – viz např. KÜHN, Z. *Exekutivní blokování internetu justice* [on-line]. Jiné právo, 07. 01. 2010 [cit. 15. 10. 2011]. Dostupné z: <jinepravo.blogspot.com/2010/01/exekutivni-blokovani-internetu-justice.html>.

formálními znaky neodhalitelné informace.[41] Je-li škodlivý kód například obsažen v příloze běžného e-mailu nebo jako součást funkčního prvku webové stránky, lze takové riziko odhalit pouze sémantickou analýzou příslušných informací.

Bezpečnostní řešení však je v každém případě nutno nastavit proporcionálně, to i vzhledem k faktické a personální rizikovosti respektive k institucionální situaci. Obrazně řečeno je tedy třeba pamatovat nejen na to, že by bylo mohlo být potenciálně nebezpečné, pokud by soudce na svém pracovním počítači stahoval terabyty dětské pornografie ze stránek obsahujících trojské koně, ale i brát v potaz, že soudci mají obvykle jiné zájmy než v pracovní době sledovat pornografii a že soud není psychiatrická léčebna, kde je nutno chovance permanentně sledovat a chránit před tím, aby neohrozili sebe ani své okolí.

Z výše uvedeného plyne i druhý základní koncepční problém kybernetické bezpečnosti, tj. skutečnost, že bezpečnostní opatření obvykle vedou k zásahu do distributivních informačních práv člověka. Zvýšení míry bezpečí tak je prakticky vždy spojeno s omezením svobody jednotlivce.[42] V tomto případě tedy platí, že se dvě základní hodnoty informační společnosti rozebrané v jedenácté kapitole, tj. svoboda a solidarita, dostávají do přímé kolize.

Distributivním právem, do něhož je třeba při budování systémů k zajištění kybernetické bezpečnosti zasahovat nejčastěji, je právo na informační sebeurčení. Jakékoli systematické řešení totiž musí být postaveno na informacích z příslušné komunikační infrastruktury, přičemž část těchto informací se nutně týká diskreční sféry člověka.[43] K tomu, aby mohl systém kybernetické bezpečnosti fungovat, je tedy třeba připustit do určité míry zásah do pasivní složky informačního sebeurčení, tj. do ochrany soukromí respektive do ochrany osobních údajů – vzhledem k tomu, že v tomto případě jde o komplexní otázku realizace specifických informačních práv státu, rozebíráme ji důkladněji v dalších podkapitolách.

Kromě zásahu do pasivní složky informačního sebeurčení se typická opatření k ochraně národního kyberprostoru neobejdou ani bez zásahů do jeho aktivní komponenty. Prostředky používané k obraně před kybernetickými útoky totiž musí být v některých případech vybaveny efektivní možností zasahovat do informačních toků, a to včetně extrémně citlivé otázky blokování komunikačního provozu.[44]

V předchozí kapitole jsme argumentovali názor, že blokování přístupu člověka ke službám informační sítě představuje extrémní zásah do práva na informační sebeurčení. Rovněž jsme dospěli k závěru, že použití tohoto prostředku k ochraně restriktivní složky majetkových práv autorských je zásadně neproporcionální a tedy neospravedlnitelné. I v případě kybernetické bezpečnosti je tedy třeba vycházet z toho, že aktivní komponenta informačního sebeurčení člověka představuje jednu z nejdůležitějších hodnot chráněných právem.

Na rozdíl od v předchozí kapitole diskutovaných velmi problematických opatření používaných, byť sporadicky, k odpojování uživatelů od internetu za účelem ochrany restrikcí autorského práva, však je v případě opatření k zajištění kybernetické bezpečnosti situace poněkud jiná. Kybernetický útok je totiž v běžných případech veden buďto za užití velkého množství skutečných či imitovaných počítačů nebo individuálně prostřednictvím skrytého kódu umožňujícího vzdálenou kontrolu cílového systému. V obou případech dochází zpravidla k zapojení počítačů, jejichž uživatelé ani netuší, že jejich stroj je k takovému útoku

[41] K charakteru počítačových virů a jim podobných forem škodlivého kódu viz např. ZHANG, Y.; LI, T.; QIN, R. Computer Virus Evolution Model Inspired by Biological DNA. In HUANG, D. S.; WUNSCH, D. C.; LEVINE, D. S. (eds.) *Advanced Intelligent Computing Theories and Applications*. Berlin-Heidelberg : Springer Verlag, 2009, str. 943 a násl.

[42] Nejde přitom pouze o nutnost strpět následný zásah do distributivních práv, ale obecná povinnost strpět takový zásah jako součást preventivní opatření – srov. FOGGETTI, N. Cyber-Terrorism and the Right to Privacy. *Masaryk University Journal of Law and Technology*. 2009, roč. 3, č. 3, str. 375.

[43] Jedním z nejdiskutovanějších právních instrumentů byl v tomto směru americký Patriot Act – odbornou analýzu viz např. v článku PODESTA, J. D.; GOYLE, R. Lost in Cyberspace? Finding American Liberties in a dangerous Digital World. *Yale Law and Policy Review*. 2005, č. 23, str. 513 a násl.

[44] K problému nastavení aktivních obranných mechanismů viz např. YOUNG, M. D. National Cyber-Doctrine: The Missing Link in the Application of American Cyber Power. *Journal of National Security Law and Policy*. 2010, č. 4, str. 173.

použit. Jejich odpovědnost nebo jiný postih *in personam* pak není z hlediska zajištění kybernetické bezpečnosti státu primárně podstatný – nejdůležitějším zájmem je v tomto případě zamezení útoku.[45]

Technicky lze řadu kybernetických útoků odrazit prostě tak, že jsou na území pod jurisdikcí příslušného orgánu veřejné moci dočasně přerušeny komunikační linky, jejichž prostřednictvím je útok veden.[46] Tam, kde se tedy příkladně aktivuje botnet[47] útočící na nějaký z prvků strategické informační infrastruktury státu (soukromé nebo veřejné), lze takovému útoku zamezit tak, že se počítačům používaným útočníkem prostě znemožní komunikovat (tj. dojde k jejich odpojení od informační sítě). Takové odpojení přitom nemusí být dlouhodobé – standardně postačí i několik vteřin či minut.[48]

Vedle ultimátního zásahu formou odpojení počítačů nebo celých dílčích sítí od národního kyberprostoru lze samozřejmě k obraně před kybernetickými útoky využít řadu dalších technických prostředků. Prvním nutným požadavkem k tomu, aby bylo blokování (odpojování) možno považovat za proporcionální prostředek ochrany kybernetické bezpečnosti, tedy je možnost jeho použití až jako *ultimae rationis*.

S právě uvedeným souvisí též druhé pravidlo k použití blokování jako nástroje k ochraně kybernetické bezpečnosti, a to minimální nutný rozsah. Blokovat komunikační možnosti tak lze jen v nezbytně nutné míře – tam, kde lze od sebe oddělit útok od ostatní komunikace, je nutno postupovat specificky pouze proti útoku. Opatření, kterým je zasaženo do aktivní složky informačního sebeurčení, je k tomu třeba aplikovat pouze na nezbytně nutnou dobu.[49]

Druhým nutným předpokladem ústavní konformity tohoto vysoce citlivého bezpečnostního nástroje pak je jeho faktické zaměření vůči systému (nikoli vůči člověku), jakož i konkrétní individuální zdůvodnění fakticky probíhajícím nebo bezprostředně hrozícím útokem. Nejde totiž v tomto případě o konkrétního člověka a jeho jednání (uživatel útočícího systému navíc zpravidla o útoku prováděném jeho systémem ani sám nic neví), ale o konkrétní systém respektive o způsob, kterým aktuálně takový systém funguje. Člověk tak v tomto případě, byť se to vzhledem k dříve popsané základní orientaci práva může zdát paradoxní, vlastně není *de facto* subjektem rozhodování o uplatnění technického opatření a není ani přímým adresátem výsledného opatření.

Otázkou v tomto směru je, do jaké míry je rozhodování o blokování jako o obraně před kybernetickým útokem vlastně rozhodováním o právech a povinnostech člověka. V důsledku totiž vede uplatnění tohoto ultimátního ochranného prostředku k omezení práva na informační sebeurčení, neboť po dobu blokování je uživateli (pokud zrovna pracuje s příslušným koncovým zařízením) znemožněn přístup ke službám informační sítě. Blokován je v tomto případě systém jako celek (či dokonce celá partikulární síť), neboť je ve většině případů technicky nemožné oddělit, jak uvedeno shora, od sebe samotný útok od ostatní komunikace.

[45] V tomto směru je podstatné poukázat na elementární, avšak i v odborných kruzích ne vždy zcela pochopený, rozdíl mezi kybernetickou bezpečností a potíráním internetové kriminality. Bezpečnostní opatření nejsou primárně zaměřena na vyšetření nebo postih kriminálního jednání, ale na ochranu státu a veřejnosti před bezpečnostními hrozbami. S trochou nadsázky lze říci, že u bezpečnostních opatření nejde o to najít a odstíhat pachatele sebevražedného pumového útoku (pokud z něj po provedení útoku něco zůstalo), ale zajistit, aby k takovému útoku vůbec nedošlo.

[46] Srov. LIN, H. S. Offensive Cyber Operations and the Use of Force. *Journal of National Security Law and Policy*. 2010, č. 4, str. 66.

[47] Tento pojem označuje uměle vytvořenou síť dálkově ovládaných počítačů, které, nejčastěji bez vědomí svých uživatelů, provádějí plánovaný útok – viz VACCA, J. R. *Computer and Information Security Handbook*. Oxford : Elsevier, 2009, str. 120.

[48] Dalším krokem je poté odstranit z napadených zařízení škodlivý kód, který je nepozorovaně zapojuje do aktivit botnetu – viz tamtéž, str. 132.

[49] Tomuto požadavku odpovídá tzv. omezený test proporcionality zahrnující pouze zhodnocení otázky, zda byl při využití institutu zasahujícího do základního práva takový zásah proveden v nezbytně nutné míře. Omezeným testem proporcionality tedy není řešena existence institutu jako takového, jen je při jeho užití předcházeno svévoli – k pojmu srov. HANUŠ, L. *Právní argumentace nebo svévole*. Praha : C. H. Beck, 2008.

Není tedy pochyb o tom, že je uživateli v takovém případě určitým způsobem zasaženo do aktivní komponenty práva na informační sebeurčení.

Spojíme-li výše uvedené základní požadavky na proporcionalitu blokování jako prostředku obrany před kybernetickým útokem, tj.

- užití blokování jako *ultimae rationis*,
- minimalizace blokování na nezbytně nutnou míru (rozsah, doba),
- uplatnění blokování na základě technických charakteristik jednání (tj. na základě empiricky ověřitelných poznatků o faktickém nebo bezprostředně hrozícím kybernetickém útoku) a
- adresnost blokování k systému (nikoli k člověku),

se základními empirickými poznatky získanými z typických situací z praxe, tj.

- útok často provádí systém bez vědomí uživatele
- přestože lze identifikovat útočící systém, identita uživatele může být neznámá, respektive se uživatel může nacházet mimo jurisdikci (totéž platí pro pachatele)
- útok lze odrazit za užití blokování, často stačí délce vteřin nebo minut
- blokování je třeba nařídit okamžitě po vyhodnocení bezprostřední hrozby nebo probíhajícího útoku (i prodlení v délce minut může vést k fatálním škodám)
- uživatel může předejít potencialitě blokování adekvátním zabezpečením svého systému
- blokování chrání nejen informační síť nebo její strategicky důležitou část před útokem ale rovněž zamezí aktivitě systému, za kterou by mohl být uživatel i bez svého vědomí objektivně odpovědný,

dospíváme k závěru, že blokování je proporcionálně použitelným nástrojem státu k ochraně kybernetické bezpečnosti. Rovněž lze z výše uvedených důvodů argumentovat názor, že založení pravomoci blokovat komunikační provoz v rámci národního kyberprostoru nemusí nutně znamenat též nutnost tvorby zvláštního správního nebo soudního řízení s konkrétně určeným účastníkem.
Dle našeho názoru tedy může mít proces blokování podobný charakter jako jiné instantní zakročovací povinnosti státní orgánů. Při zachování striktních zákonných podmínek uvedených shora lze příslušnému státnímu orgánu nebo i dokonce soukromoprávnímu subjektu svěřit tuto technickou kompetenci s tím, že kontrola jejího uplatnění a případný postih za svévoli nebo jinou formu *ad hoc* překročení ústavních nebo zákonných limitů budou až následné.

13.3 Řešení kybernetické bezpečnosti České republiky

Vzhledem k tomu, že Česká republika je jedním z posledních civilizovaných států, kde doposud nedošlo k implementaci národního řešení kybernetické bezpečnosti, zaměříme se v následujícím stručném výkladu především na diskusi současných možností. Budeme se věnovat zejména institucionálním (organizačním) a ústavněprávním aspektům navrhovaného koncepčního řešení, které v létě roku 2011 schválila Bezpečnostní rada státu.[50]

[50] Viz dokument *Strategie pro oblast kybernetické bezpečnosti České republiky na období 2011 – 2015* [on-line]. Centrum kybernetické ochrany ČR [22. 7. 2011]. Dostupné z: <www.govcert.cz>.

Vytvoření systematické, efektivní a ústavně konformní ochrany českého kyberprostoru se nijak zvlášť neliší od podobného zadání v ostatních evropských státech.[51] I v případě České republiky tak má hlavní iniciativu vláda, přičemž však je nutno zapojit do samotného procesu realizace jednotlivých opatření i správní orgány stojící mimo strukturu vlády a dále pak též soudnictví a právotvornou moc. Obejít se konečně nelze ani bez akademického, občanského a soukromého sektoru.

Vzhledem ke shora zmíněné specifikaci orgánů státní správy se navíc jeví jako vhodné, pokud je centrální funkční prvek, tj. centralizované dohledové pracoviště, budován a provozován správním orgánem, jehož vazba na vládu respektive na ostatní složky státní moci je nepřímá (tj. orgán, který není vládě přímo podřízen a nepřijímá od ní konkrétní úkoly). Jestliže byla u nás gesce nad budováním centrálního úseku národní kybernetické bezpečnosti aktuálně svěřena Národnímu bezpečnostnímu úřadu, jedná se dle našeho názoru o řešení vhodné a z hlediska možných rizik plynoucích ze shora popsané informační dominance i relativně bezpečné. Národní bezpečnostní úřad již dnes víceméně úspěšně disponuje centralizovanou informační kompetencí zasahující prakticky všechny složky státní správy a dohled nad bezpečností českého kyberprostoru se této kompetenci v mnohém podobá.

Není smyslem tohoto textu řešit konkrétní otázky personální či organizační – v nich samozřejmě, zejména pokud jde o schopnost financovat poměrně rozsáhlou a typově novou bezpečnostní infrastrukturu, mohou nastat závažné organizační obtíže. Relativní stabilita úřadu typu NBÚ daná jeho postavením však dává dobrý předpoklad k tomu, aby mohl být systém národní kybernetické bezpečnosti rozvíjen koncepčně, kontinuálně a na základě důkladné a dlouhodobé strategické úvahy. Právě dlouhodobost, stabilita a vázanost ke strategické koncepci je naopak kamenem úrazu u řady aktivit správních orgánů, jejichž vysoké i střední vedení má silně politický (tím pádem měňavý) charakter.[52]

Navrhovaný systém k zajištění kybernetické bezpečnosti České republiky počítá se vznikem vládního a národního dohledového pracoviště (CERT).[53] Vládní CERT má být vybaven k centralizovanému sledování státní informační infrastruktury a vzhledem k této infrastruktuře má mít též vcelku rozsáhlé zakročovací kompetence. Údaje, které má vládní CERT zpracovávat, mají pocházet z lokálních dohledových systémů, které již dnes částečně provozují různé složky státního aparátu,[54] nebo bezprostředně přímo z těch částí státní informační infrastruktury, které doposud nejsou kryty dohledem ani jinou zabezpečovací technologií.[55]

Podobně, jako bude vládní CERT působit jako dohledové pracoviště pro státní informační infrastrukturu, má tyto funkce plnit národní CERT pro veřejnou komunikační infrastrukturu. Podstatný rozdíl mezi národním a vládním CERTem spočívá v tom, že národní CERT bude vybaven pouze dohledovou, nikoli však zakročovací kompetencí. Národní CERT tedy bude shromažďovat a vyhodnocovat informace o bezpečnostních hrozbách z veřejné komunikační infrastruktury a formou informační zpětné vazby a doporučení koordinovat činnost lokálních CERTů. Tam, kde lokální CERT nebude aktivní (tzn. tam, kde bude lokální CERT chybět

[51] Srov. dokument *Budování pracoviště CERT v České republice* [on-line]. Centrum kybernetické ochrany ČR [22. 7. 2011]. Dostupné z: <www.govcert.cz>.

[52] Lze v tomto směru poukázat na obecně problematickou situaci, kdy jsou zejména na ministerstvech často i odborné posty na úrovni ředitelů odborů obsazovány nikoli kariérně ale politicky. Tato skutečnost se negativně projevila i na budování systému kybernetické bezpečnosti v době, kdy jej mělo v gesci Ministerstvo vnitra.

[53] Běžně se používá zkratek CERT (Computer emergency response team – česky zřejmě něco jako sbor pro řešení počítačových pohotovostí) nebo CSIRT (Computer Security Incident Response Team – česky zřejmě sbor pro řešení počítačových bezpečnostních událostí). České oficiální dokumenty pracují vesměs se zkratkou CERT, proto budeme i zde tuto zkratku nadále používat.

[54] Vlastní dohledové systémy provozují vedle bezpečnostních složek také některé ústřední orgány státní správy.

[55] Zde je třeba podotknout, že tam, kde je příslušná součást státní informační infrastruktury relativně identická, tj. například v justici, je třeba uvažovat o tvorbě autonomního dohledového mezičlánku (tj. zvláštního pracoviště) – ponechání dohledu nad často relativně rozsáhlým systémem na vládním pracovišti by totiž nejen toto pracoviště organizačně a technicky zatěžoval, ale vedlo by také k nežádoucí bezprostřednosti výkonu státní správy vzhledem k soudnictví.

nebo nebude reagovat na výzvu k ošetření bezpečnostního incidentu), a bezpečnostní hrozba dosáhne určité intenzity, předá národní CERT informaci o bezpečnostním incidentu vládnímu CERTu. V ultimátním případě pak vládní CERT nařídí jako nejzávažnější formu protiopatření blokování příslušné části komunikační infrastruktury.

Podobně, jako je tomu u státní komunikační infrastruktury, i ve veřejné komunikační síti již fungují lokální CERTy, které mohou vcelku jednoduše spolupracovat s centrálním národním respektive vládním dohledovým pracovištěm.[56] Povinnost poskytovat informace o bezpečnostních hrozbách a incidentech centralizovanému pracovišti respektive provádět navržená bezpečnostní opatření včetně odpojení příslušné části informační infrastruktury však na rozdíl od sféry přímo kryté vládním CERTem vyžaduje kvalitativně jiné právní řešení.

Na úrovni státní informační infrastruktury totiž může být povinnost místního CERTu reagovat na pokyn vládního CERTu respektive založení přímé kompetence vládnímu CERTu k odstavení části sítě založena i jen prostřednictvím podzákonného normativního právního aktu (typicky nařízením vlády). Obdobnou povinnost respektive kompetenci vládního CERTu zakročit v případě bezpečnostního incidentu proti veřejné komunikační infrastruktuře však nelze založit jinak než zákonem – to z důvodu elementárního principu kontinentální právní kultury, že totiž povinnost lze založit výlučně zákonem. Právo na zpracování údajů z činnosti veřejné komunikační infrastruktury (viz dále) jakož i právo a povinnost zakročit proti bezpečnostním incidentům tedy musí být vládnímu CERTu svěřena formou primárního pramene práva.

Zákon však v tomto případě nemusí být nutně zcela specifický. Specifikaci konkrétních technických kompetencí vládního CERTu lze totiž provést i zprostředkovaně, a to formou odkazu k podzákonnému předpisu nebo i prostřednictvím zákonného požadavku na použití určité bezpečnostní technologie. Zákon tedy může například stanovit provozovatelům komunikační infrastruktury povinnost používat bezpečnostní technologii, jejíž konkrétní parametry budou předmětem prováděcího předpisu nebo dokonce i jen specifikace konkrétního technického řešení a která bude přímo spolupracovat s technologií vládního CERTu.

Nelze samozřejmě příslušné zákonné oprávnění formulovat až příliš obecně a otevřít tím prostor k faktickému zakládání práv a povinností podzákonným předpisem či dokonce i jen průmyslovým standardem.[57] Stejně nelze při zákonné specifikaci pominout ani úpravu kontrolních mechanismů a opatření k minimalizaci rizik spojených se založenou kompetencí. Míra specifičnosti úpravy zákonných kompetencí stejně jako míra specifičnosti ochranných a kontrolních mechanismů nepředstavuje v tomto případě jen nějakou formální legislativně technickou otázku, ale vzhledem k dotčení práva na informační sebeurčení se jedná o základní materiální problém ústavní konformity[58].

> Nedostatečná specifičnost technických a organizačních záruk ochrany práva na informační sebeurčení byla jedním z důvodů nedávného zrušení úpravy uchovávání provozních údajů z veřejných služeb elektronických komunikací naším Ústavním soudem. Soud k tomu doslova uvedl: *„Navrhovateli napadená právní úprava dle názoru Ústavního soudu rovněž zcela nedostatečně, příp. vůbec nestanovuje jasná a detailní pravidla obsahující minimální požadavky na zabezpečení uchovávaných údajů, zejména v podobě zamezení přístupu třetích osob, stanovení procedury vedoucí k ochraně celistvosti a důvěrnosti údajů a procedury jejich ničení. Dále je třeba napadené úpravě vytknout, že dotčení jednotlivci nedisponují dostatečnými zárukami proti riziku zneužití údajů a svévole. Nezbytnost*

[56] Dohledová pracoviště pro dohled nad vlastní informační infrastrukturou provozují větší podniky, banky, telekomunikační operátoři, univerzity apod.

[57] Typickým příkladem, kde se tento vysoce problematický model uplatnil, jsou datové schránky – provozovatel systému tak příkladně určuje, po jaké době se zprávy ze schránky automaticky mažou.

[58] Srov. KOKEŠ, M. Několik poznatků k problematice konkrétních konfliktů mezi právem na informační sebeurčení a ochranou národní bezpečnosti v tzv. době internetové. In ŠIMÍČEK, V. (ed.) *Právo na soukromí*. Brno : Mezinárodní politologický ústav, 2011, str. 119 a násl.

disponovat takovými zárukami se přitom v posuzovaném případě plošného a preventivního sběru a uchovávání údajů v rámci elektronické komunikace stává pro jednotlivce naléhavější právě v dnešní době, kdy díky enormnímu rozvoji a výskytu nových a komplikovanějších informačních technologií, systémů a komunikačních prostředků nevyhnutelně dochází k plynulému posunu hranice mezi privátním a veřejným prostorem, a to ve prospěch veřejné sféry, neboť ve virtuálním prostoru informačních technologií a elektronické komunikace (v tzv. kyberprostoru) jsou, zejména díky rozvoji internetu a mobilní komunikace, každou minutou zaznamenávány, shromažďovány a fakticky zpřístupněny tisíce, ba miliony dat, údajů a informací, které zasahují i do soukromé (osobnostní) sféry každého jednotlivce, ačkoliv on sám do ní vědomě nikoho vpustit nechtěl.“ [59]

S otázkou rozdělení a specifikace konkrétních technických kompetencí vládního CERTu mezi zákon, podzákonný předpis a parametry konkrétní dohledové či ochranné technologie souvisí i nastavení možností vládního CERTu spolupracovat s akademickým, soukromým či občanským sektorem. Jak bylo uvedeno v úvodu této kapitoly, je delegace kompetencí k ochraně nedistributivních práv v naší právní kultuře vzhledem k jejich chápání vždy problematická. Nelze tedy bez dalšího přijmout tezi, že cokoli se bude vymykat z technických schopností vládního CERTu, je možno prostě přenést na akademický, soukromý nebo občanský sektor.

Na druhou stranu však je nepochybně možno využít shora rovněž diskutované možnosti nestátních subjektů jednat *praeter legem*, ať už jde o výzkum, vývoj nebo dokonce o aktivní implementaci nejrůznějších protiopatření. Aktivní obrana může v tomto případě zahrnovat i techniky, jejichž zákonný popis a na něm založené oprávnění vládního CERTu prostě nelze legislativně technicky provést, neboť jejich základní parametry nejsou známy (taková protiopatření se vyvíjejí až v reakci na konkrétní útok). Jejich cílem může navíc být i informační infrastruktura umístěná mimo jurisdikci České republiky, což zapojení vládního CERTu dále komplikuje.[60]

Právě uvedené samozřejmě neznamená, že by měl vládní CERT najímat akademické, soukromé nebo občanské kapacity na nějakou protiprávní špinavou práci. Mezi legislativně předvídatelnými a ústavně konformním způsobem upravitelnými kompetencemi na jedné straně a protiprávními aktivitami na straně druhé (tj. špinavou prací) však je stále poměrně velký manévrovací prostor. Za užití náležité motivace tak lze docílit vysoce efektivního synergického efektu, který může kromě samotné dohledové respektive ochranné činnosti zahnout též výzkum a vývoj, experimentální aktivity, výměnu poznatků a zkušeností se zahraničními a mezinárodními organizacemi apod.[61]

Posledně jmenovaný aspekt spolupráce, tj. zahraniční výměna informací a účast na činnosti mezinárodních fór, může mít pro náš systém kybernetické bezpečnosti zásadní význam. Česká republika totiž nepatří mezi státy, jejichž národní kyberprostor by představoval oblíbený či standardní cíl kybernetických útoků a tomu odpovídá i relativně velmi nízká úroveň investic do výzkumu a vývoje v tomto oboru. Různé bezpečnostní incidenty se u nás také vyskytují až s určitým zpožděním oproti státům stojícím takříkajíc na frontové linii. Jsou to pak právě zkušenosti ze států, které praktická nutnost donutila významně investovat do vývoje bezpečnostních opatření, které nám mohou výrazně pomoci při vytváření a implementaci

[59] Viz nález pléna Ústavního soudu ze dne 22.3.2011, sp. zn. Pl.ÚS 24/10, 94/2011 Sb., odst. 50. Dostupné z: <www.nalus.usoud.cz>.

[60] Příkladem může být odpověď na hrozbu vyvolanou tzv. phishingovým útokem – útočník se v takovém případě snaží proniknout přes bezpečnostní opatření vylákáním přístupových údajů od uživatelů prostřednictvím fingovaných přihlašovacích www stránek. Efektivní obranou *praeter legem* v tomto případě je například zavalit útočníkovy stránky masou fiktivních přihlašovacích údajů.

[61] Nelze v tomto směru pominout skutečnost, že naše státní instituce mají tradičně velký problém dobře zaplatit špičkové odborníky jako své zaměstnance. Dochází pak k paradoxní situaci, kdy jedinou možností, jak takového experta najmout k práci pro stát (o kterou často nejen z finančních důvodů takový expert velmi stojí), je prostřednictvím externí organizace, tj. typicky univerzity nebo soukromého subjektu (zde totiž není třeba respektovat platové tabulky nebo se obávat vulgární kritiky za to, že špičkový odborník vydělává víc než ministr či prezident republiky).

obdobných tuzemských opatření. Nákladný vlastní vývoj lze tedy u nás v tomto případě nahradit mnohem méně náročnou mezinárodní výměnou poznatků s méně šťastnými státy, které, co se týče investování do primárního vývoje bezpečnostních opatření, prostě nemají na výběr.

13.4 Informační práva státu

Informace představují pro běžné fungování státu přinejmenším stejně důležitou komoditu, jakou jsou lidské či přírodní zdroje, finance nebo mezinárodní vztahy.[62] V předchozích kapitolách jsme dokonce konstatovali, že podstatná část činností, jimiž se stát zabývá, má ve své podstatě povahu tvorby, zpracování nebo komunikace informací. Informačními právy státu pak rozumíme práva získávat, zpracovávat a komunikovat informace k tomu, aby mohl plnit své standardní funkce.[63]

Na rozdíl o výše diskutované problematiky kybernetické bezpečnosti nemají informační práva státu originární charakter, ale jsou akcesorická. Nemá tedy valného smyslu hovořit o nich samostatně, ale vždy ve vazbě na agendu, v níž jsou informace používány. Příkladně tedy není smysluplné diskutovat otázku získání, zajištění a provedení důkazu (tj. procesní skutkové informace) bez vazby na to, v jakém řízení respektive za jakým účelem má být důkazu použito.

Právě uvedené potvrzuje i tezi o generickém spojení informační technologie a účelu jejího použití, kterou jsme argumentovali ve druhé kapitole. Nelze totiž izolovaně uvažovat o získávání, zpracovávání nebo komunikaci informací ani o technologiích k jejich podpoře bez úvahy o adekvátnosti jejich smyslu a účelu. Stejně tak, jako nemůže být úvaha o vývoji a nasazení informačních a komunikačních technologií pouze instrumentální, nesmí být instrumentální ani úvaha o informačních právech. Jako je nelegitimní takové nasazení informačních a komunikačních technologií, které je neúčelné nebo účel postrádá, je nelegitimní i založení informačního práva bez akcesorické vazby na konkrétní účel existence a fungování demokratického právního státu.

Axiomatickým paradoxem v tomto směru rozumíme situaci, kdy je informační právo státu vnitřně rozporné nebo kdy jeho existence či nastavení pojmově odporují jeho smyslu a účelu. Především v případech, kdy má být informačním právem státu zajištěno nedistributivní právo, však v otázce hodnocení míry jeho paradoxnosti působí relativně nové informační a komunikační technologie často zmatení a nejistotu.[64] Je totiž v takových případech krajně obtížné posoudit, zda je v nové situaci dané překotným použitím informačních a komunikačních technologií adekvátní často i samotná existence nebo rozsah určitého informačního práva státu.[65] I náš Ústavní soud při aplikaci druhého prvku testu proporcionality, tj. testu potřebnosti, pochopitelně rovněž tápe a v obtížných situacích má tendenci rozhodovat ve vztahu ke státu spíš restriktivně.[66]

---

[62] Srov. FOUNTAIN, J. E. *Building the Virtual State*. Washington, D.C. : Brookings Institution, 2001, str. 3.

[63] Význam informací pro národní bezpečnost potvrzuje i pevné místo informačních funkcionalit v základní struktuře bezpečnostních aspektů existence státu. Informace, respektive služby, které je zajišťují, tak stojí na stejné úrovni jako armáda, policie nebo zahraniční vztahy – srov. DIFFIE, W.; LANDAU, S. *Privacy on the Line*. Cambridge : MIT Press, 2007, str. 87 a násl.

[64] Problémy už činí odlišit od sebe ve vztahu k informačním právům státu problematiku národní bezpečnosti a autoritativní aplikace práva. Naše právotvorné i soudní orgány k tomuto odlišení ještě bohužel nedospěly a informační služby tak často musí pracovat se stejnými procesními požadavky jako policie nebo státní zastupitelství – v problému viz např. DIFFIE, W.; LANDAU, S. *Privacy on the Line*. Cambridge : MIT Press, 2007, str. 137 a násl.

[65] Obecně k této diskusi viz např. REICH, P. C.; WEINSTEIN, S.; WILD C.; CABANLONG A. S., Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents - and the Dilemma of Anonymity. *European Journal of Law and Technology*. 2002, roč. 2, č. 1.

[66] Odpovídá to i titulu *libri amicorum* sestavené k životnímu jubileu jedné z nejvýraznějších postav českého ústavního soudnictví, soudkyni Elišce Wagnerové – viz POSPÍŠIL, I.; KOKEŠ, M. *In dubio pro libertate. Úvahy nad ústavními hodnotami a právem*. Brno : Masarykova univerzita, 2009. Lze však diskutovat o tom, zda relativně nově vytvořené (i přesto

Tento přístup se projevil v *obiter dictu* shora cit. rozhodnutí Ústavního soudu. V tomto případě soud vyslovil pochybnost, zda je rozsáhlého a systematického zásahu do práva informační sebeurčení člověka vzhledem ke chráněným zájmům vůbec třeba respektive zda tyto zájmy nelze informačně zajistit jinými (tradičními) způsoby. Soud k tomu doslova uvedl: *„Pouze toliko ve formě obiter dicta Ústavní soud konstatuje, že si je samozřejmě vědom skutečnosti, že ruku v ruce s rozvojem moderních informačních technologií a komunikačních prostředků dochází i k výskytu nových a sofistikovanějších způsobů páchání trestné činnosti, kterým je nutné čelit. Nicméně Ústavní soud vyjadřuje pochybnosti nad tím, zda samotný nástroj plošného a preventivního uchovávání provozních a lokalizačních údajů téměř o veškeré elektronické komunikaci je z hlediska intenzity zásahu do soukromé sféry nepřeberného množství účastníků elektronické komunikace nástrojem nezbytným a přiměřeným.“* [67]

Informační práva státu přistupují k distributivním i nedistributivním právům. Důkazy, zpravodajské informace nebo soudní rozhodnutí tak slouží nejen k ochraně nedělitelných veřejných hodnot (např. shora zmíněné kybernetické bezpečnosti), ale též k ochraně distributivních práv (tj. např. v předchozí kapitole diskutovaného soukromí, vlastnictví aj.) Legitimační vztah mezi chráněným právem a oprávněním státu shromažďovat, zpracovávat a používat související informace je přitom dvousměrný.[68] V situaci, kdy zajištění příslušného distributivního nebo nedistributivního práva přímo závisí na možnosti státu opatřit si a zpracovat příslušné informace, můžeme konstatovat, že informační práva státu jsou nejen legitimována svým účelem, ale že jejich založení současně představuje i *conditio sine qua non* existence jimi zajištěných práv. Bez informačního fundamentu totiž nelze příslušná distributivní nebo nedistributivní práva efektivně sankcionovat, což představuje fundamentální problém pro jejich existenci lhostejno, zda tuto problematiku nazíráme pohledem pozitivistickým[69] nebo přirozenoprávním.[70]

Dospíváme tedy k závěru, že absence akcesorických informačních práv státu má *de facto* za následek oslabení různých distributivních i nedistributivních práv o sankci a tím praktické popření jejich existence.[71] Sankcí v tomto případě nemusíme nutně chápat pouze adresovaný trest za nesplnění právní povinnosti, ale též i jen nutnost strpět zásah do pasivní složky informačního sebeurčení tam, kde má informace ze soukromé sféry člověka (případně informace z diskreční sféry právnické osoby) posloužit státu k plnění jeho funkcí.

Typickým příkladem legitimace ochranného institutu informačním právem státu je soukromoprávní ochrana osobnosti v případech, kdy je zásah do osobnostní sféry způsobem anonymním uživatelem internetu. Nedosahuje-li jednání intenzity trestného činu, nemá stát možnost aktivně využít svých informačních práv k zajištění informací o tom, kdo se mohl příslušného jednání dopustit. Poškozený však k tomu, aby mohl tento zásah civilně žalovat, potřebuje informace o identitě žalovaného (nelze žalovat „neznámého žalovaného“) – ty si však bez možnosti zapojit stát není schopen obstarat (pokud nemá výjimečně přátelské vztahy s příslušnými definičními autoritami). Přestože tedy v tomto případě právo konstruuje nárok, není tento z důvodu absence akcesorického informačního práva prakticky uplatnitelný.

13.5 Axiologické paradoxy informačních práv státu

Orientace systému právních pravidel na člověka má za následek mimo jiné i výše naznačené napětí mezi ochranou různých typů distributivních práv. Tento rozpor může být standardně řešen za užití kompletního nebo omezeného testu proporcionality. Distributivní

---

však nesporně silné a sugestivní) pravidlo *in dubio pro libertate* není důvod posunout poněkud zpět k původním základům římského práva, které by mohlo vyjadřovat spíše pravidlo „*in dubio pro civitate*.“

[67] Viz nález pléna Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl.ÚS 24/10, 94/2011 Sb., odst. 55. Dostupné z: <www.nalus.usoud.cz>.

[68] Srov. např. HERCEG, J. *Meze svobody projevu*. Praha : Orac, 2004, str. 50 a násl.

[69] Srov. KELSEN, H. *Všeobecná teorie norem*. Brno : Masarykova univerzita, 2000, str. 147.

[70] Srov. FULLER, L. *Morálka práva*, přel. Přibáň, J. Praha : OIKOYMENH, 1998, str. 78.

[71] Shodně viz GEER, D. E. Cybersecurity and National Policy. *Harvard National Security Journal*. 2010, č. 1, str. 5.

informační práva však mají i vcelku unikátní paradoxní vlastnost, že totiž při zapojení státu do jejich vymáhání mohou popírat sama sebe.

Typicky právo na ochranu soukromí má charakter ochrany před zásahem do diskreční informační sféry. Jestliže má stát zajistit jeho vynutitelnost (tj. formální existenci), lze toho dosáhnout pouze za cenu využití nedistributivních informačních práv – stát si tedy musí opatřit informace o jednání, kterým bylo do informační sféry jednotlivce zasaženo, přičemž takové informace musí být jednoznačně personalizovány.[72] Přístupem k těmto informacím však je nutně zasaženo do individuální informační diskrece.

V tomto směru lze poukázat na shora cit. případ, v němž Ústavní soud posuzoval ústavní konformitu institutu uchovávání provozních údajů. Soud v tomto případě sice konstatoval, že mechanismus uchovávání těchto údajů je obecně přípustný,[73] avšak právotvůrce nevyužil všech možností k tomu minimalizovat zásah do distributivních informačních práv člověka. Proti ochraně soukromí a osobních údajů zde soud postavil dominantní důvody zavedení institutu uchovávání provozních údajů, tj. zejména ochranu před zvlášť závažnou trestnou činností. Ústavní soud k tomu uvedl: *„Uvedený způsob (ne)vymezení spektra oprávněných orgánů veřejné moci, jakož i (ne)vymezení účelu, pro který jsou uchovávané údaje oprávněny požadovat, Ústavní soud nepovažuje za dostatečný a předvídatelný. Ačkoliv podle citovaného ustanovení § 88a odst. 1 trestního řádu použití uchovávaných údajů podléhá soudní kontrole, a to v podobě vydání povolení ze strany předsedy senátu (a v přípravném řízení soudce), bylo primárně povinností zákonodárce, aby v napadených ustanoveních anebo v citovaném ustanovení § 88a odst. 1 trestního řádu namísto zcela neurčitého vymezení podmínky použití uchovávaných údajů ‚o uskutečněném telekomunikačním provozu' za účelem ‚objasnění skutečností důležitých pro trestní řízení' zřetelněji a jednoznačněji stanovil jak předpoklady a podmínky pro jejich použití, tak i rozsah jejich použití. Zejména je nezbytné, aby s ohledem na závažnost a míru zásahu do základního práva jednotlivců na soukromí v podobě práva na informační sebeurčení (ve smyslu čl. 10 odst. 3 a čl. 13 Listiny), jež použití uchovávaných údajů představuje, zákonodárce omezil možnost použití uchovávaných údajů jen pro účely trestních řízení vedených pro zvlášť závažné trestné činy a jen pro případ, že nelze sledovaného účelu dosáhnout jinak."*

Uchovávání provozních údajů a jejich následná analýza se však v praxi hojně používají i pro méně závažné (z hlediska státního zájmu) informační incidenty, jakými jsou právě zásahy do ochrany soukromí, narušení ochrany osobních osobních údajů, informační šikana (*stalking*) a jiné formy porušení práva na informační sebeurčení.[74] U řady typických forem informační kriminality jsou dokonce provozní údaje jediným solidním důkazem, který lze k příslušnému deliktnímu jednání zajistit[75] – k jednání totiž často dochází výlučně v prostředí informační sítě a neexistují k němu fyzické stopy, svědci apod. Pokud by tedy skutečně došlo k omezení možností uchovávat a zpracovávat provozní údaje ve jménu ochrany informačního

[72] Personalizace v tomto případě zajistí především adresnost následných represivních akcí. Má však i ochrannou funkci vzhledem ke státu – při přeshraničním kybernetickém útoku totiž může prokázáním přičitatelnosti konkrétní osobě odvrátit stát původu odvetnou reakci dotčeného státu nebo mezinárodního společenství – srov. OPHARDT, J. Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield. *Duke Law and Technology Review*. 2010, č. 3, str. 1.

[73] Shora zmíněná pochybnost ohledně adekvátnosti použité metody byla v tomto případě vyjádřena jen v obiter dictu cit. rozhodnutí. Souhlasně k metodě, ale nesouhlasně ke konkrétnímu provedení se postavila i řada dalších evropských ústavních soudů a jim obdobných instancí – srov. FEILER, L. The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection. *European Journal of Law and Technology*. 2010, roč. 1, č. 3.

[74] Ústavní soud v tomto případě navíc zcela pominul skutečnost, že provozní údaje bývají neocenitelným a často také jediným solidním zdrojem informací například v případech pátrání po pohřešovaných osobách – tehdy jsou státní orgány aktivní i bez toho, aby byl spáchán trestný čin.

[75] Někteří autoři se v tomto směru domnívají, že okruh protiprávního jednání, k němuž bude do budoucna k dispozici jen elektronický důkazní materiál, se bude i nadále výrazně rozšiřovat – srov. např. LANGE, M. C. S; NIMSGER, K. M. *Electronic Evidence and Discovery – What Every Lawyer Shoudl Know Now*. Chicago : American Bar Association, 2009, str. 4.

sebeurčení jednotlivce, vedlejším efektem by bylo i popření faktické existence řady institutů, které informační sebeurčení jednotlivce chrání.[76] Důslednou ochranou soukromí člověka by tedy v tomto případě stát prakticky zbavil člověka ochrany soukromí.

Ve výsledku se tento axiologický paradox projevuje nutností proporcionálně vážit táž práva pro různé obecně se vyskytující situace. U uchovávání provozních údajů je tedy nutno posuzovat nikoli ochranný institut jako takový ale jeho jednotlivé aplikace. To odpovídá i poněkud nepříjemnému avšak logickému závěru, který jsme učinili v předchozí kapitole, tj. že restriktivní ochrana diskreční informační sféry je do budoucna neudržitelná[77] – namísto omezování ve sběru informací tak je třeba zaměřit pozornost na účel, k nimž jsou tyto informace zpracovávány, na způsoby, kterými se tak děje a na instituce, které k těmto informacím mají přístup.[78]

Přestože i náš Ústavní soud staví do popředí svého zájmu teleologii zpracování informací chráněných distributivními informačními právy, můžeme v tomto směru pozorovat druhý axiologický paradox plynoucí v tomto případě z upřednostnění formálního principu autonomie vůle.[79] Proces, kterým si stát sjednává výkon svých nedistributivních informačních práv na úkor distributivních informačních práv člověka, je velmi složitý a citlivý. Stát je v tomto případě, a to zcela po právu, pod drobnohledem institucí, jakými jsou ústavní soudy, ochránci lidských práv nebo představitelé liberálních politických proudů.

Na druhou stranu však lze především ze strany komerčního sektoru sjednat přístup do diskreční informační sféry člověka velmi jednoduše, a to díky jeho souhlasu. Právo v tomto případě prakticky totálně respektuje souhlas člověka s tím, aby byla jeho informační diskrece nebo jiná distributivní informační práva omezena či prakticky vyloučena ve prospěch soukromoprávního subjektu.[80] Tento souhlas však bývá ve valné většině případů pouze formální – typicky uživatelé služeb sociálních sítí, síťových úložišť, wembailů a dalších služeb poskytovaných *prima facie* zdarma dávají obvykle provozovateli této služby totální souhlas s použitím všeho, co prostřednictvím takové služby komunikují. Tento souhlas se zpravidla skrývá za nánosem nejrůznějších všeobecných smluvních podmínek, které obvykle žádný uživatel nečte (a pokud ano, jen málokterý uživatel skutečně chápe, co znamenají, neboť jejich pravý, roz. formální, význam často zůstává skryt i zkušenému profesionálovi).[81]

> Příkladně část všeobecných podmínek pro používání služby facebook týkající se ochrany soukromí je napsána na plných dvaceti normostranách textu. Jednotlivá ustanovení dávající na první pohled dojem vysokého stupně ochrany uživatelů však obsahují mimo jiné i drobné pasáže typu (překlad RP): *„Sdílíme vaše informace se třetími stranami, pokud věříme, že jste s tím souhlasili, k nabízení našich služeb nebo pokud to jsme k tomu povinni dle zákona.“* [82] Méně kamuflážní charakter, avšak totožný efekt mají zásady ochrany osobních údajů jiného dominantního poskytovatele služeb typu UGC, společnosti Google. V přehlednějším a tentokrát česky psaném dokumentu se uživatel se zájmem o tuto

[76] Když Sean Condron varuje před přílišnou ochranou distributivních práv (občanských svobod) na úkor národní bezpečnosti, pozastavuje se i nad otázkou, jak bude tato práva možno zajistit v situaci, kdy bude systém národní bezpečnosti (užívaný rovněž k ochraně distributivních práv) prakticky nefunkční – srov. CONDRON, S. M. Getting It Right: Protecting American Critical Infrastructure in Cyberspace. *Harvard Journal of Law and Technology*. 2007, roč. 20, č. 2, str. 418.

[77] Shodně viz CHESTERMAN, S. *One Nation Under Surveillance*. Oxford : Oxford University Press, 2011, str. 223 a násl.

[78] Srov. CHESTERMAN, S. *One Nation Under Surveillance*. Oxford : Oxford University Press, 2011, str. 205.

[79] K uplatnění principu autonomie vůle v ochraně soukromí a osobních údajů viz např. BAMBERGER, K. A.; MULLIGAN, D. K. Privacy on the Books and on the Ground. *Stanford Law Review*. 2011, roč. 63, č. 2, str. 101.

[80] Zajímavé je, že posvátnost formálního souhlasu je srovnatelná v soukromém právu i v právu správním – nejen civilní ochranu soukromí, ale také administrativní ochranu osobních údajů lze tedy obejít vhodně zvoleným mechanismem udělení uživatelského souhlasu – srovnávací studii evropského a severoamerického přístupu srov. BENNETT, C. J. *Regulating Privacy: Data protection and Public Policy in Europe and The U.S.* Ithaca : Cornell University Press, 1992, str. 153.

[81] Problematikou spotřebitelského souhlasu se zpracováním osobních údajů a jiných diskrétních informací se dlouhodobě zabývá celoevropský vědecký projekt CONSENT. Mimo jiné byla v rámci tohoto projektu provedena analýza více než stovky smluvních podmínek služeb typu UGC. Výstupy projektu jsou průběžně publikovány na adrese <www.consent.law.muni.cz>.

[82] Přestože jsou služby sociální sítě Facebook nabízeny i v českém jazyce, překlad podmínek ochrany soukromí z nějakého důvodu stále chybí. Viz Facebook's Privacy Policy na adrese <www.facebook.com/policy.php>.

problematiku dočte, že: *„Google sdílí osobní údaje s jinými společnostmi nebo osobami mimo Google pouze v následujících omezených případech:*

- *Máme váš souhlas. V případě sdílení jakýchkoli citlivých osobních údajů požadujeme váš výslovný souhlas.*
- *Takové údaje poskytujeme svým pobočkám, přidruženým společnostem nebo jiným důvěryhodným podnikům a osobám za účelem zpracování osobních údajů naším jménem. Vyžadujeme, aby tyto strany souhlasily se zpracováním údajů podle našich pokynů a v souladu s těmito Zásadami ochrany osobních údajů a všemi dalšími příslušnými opatřeními za účelem utajení a zabezpečení.*
- *Jsme v dobré víře přesvědčeni, že přístup k takovým informacím, jejich použití, uchování nebo zveřejnění takových informací jsou nutné za účelem: (a) dodržení platného zákona, nařízení, právního postupu nebo vynutitelného státního požadavku, (b) uplatnění platných Smluvních Podmínek, včetně vyšetření jakéhokoli jejich možného porušení, (c) zjištění, zabránění nebo jiného postupu proti podvodu, technickým či bezpečnostním problémům nebo (d) ochrany před poškozením práv, majetku nebo bezpečnosti Google, jeho uživatelů nebo veřejnosti tak, jak to vyžaduje nebo povoluje zákon.“* [83]

Spíše výjimkou jsou v tomto směru služby, které i přes skutečnost, že by ze shora uvedených důvodů nepochybně získaly i totální souhlas svých uživatelů, této možnosti plně nevyužívají. Například smluvní podmínky k užívání služeb portálu seznam.cz obsahují následující ustanovení:

„d) Provozovatel se zavazuje, že informace, které o sobě Uživatel při vytvoření svého uživatelského účtu (-) uvedl, neposkytne třetí osobě s výjimkou oficiálních žádostí Policie ČR a orgánů státní správy oprávněných k vyžádání daných informací dle zákona.

e) Provozovatel se zavazuje, že obsah emailových zpráv (ať už přijatých, rozepsaných či odeslaných) neposkytne jakékoli třetí osobě, nebude obsah zpráv editovat, cenzurovat ani monitorovat, s výjimkou monitorování počtu zpráv, které uživatel dostává a rozesílá a dále systémového monitorování obsahu emailů antispamovými a antivirovými programy, které zabraňují přijímání spamových a zavirovaných emailů. Tímto není dotčeno ustanovení písmena d) tohoto Smluvního ujednání výše, které se vztahuje i na obsah emailových zpráv.“

Existence uživatelského souhlasu, byť nevědomého respektive neinformovaného, vede v praxi k paradoxní právní situaci, kdy ochrana soukromí a osobních údajů nechrání příslušné subjekty (ty se totiž veškeré ochrany vzdávají svým souhlasem) ani veřejný zájem (stát k těmto údajům zpravidla nemá přístup, respektive si tento přístup sám omezuje), ale pouze ty provozovatele příslušných služeb informační společnosti, kteří si takový souhlas dokážou opatřit.[84] Chráněni pak jsou tito vládci nad soukromím svých uživatelů nejen před potenciální konkurencí ale i před státem. Policie, informační služby a další státní orgány, jejichž nedistributivní informační práva často nezahrnují možnost se k takto zpracovávaným osobním údajům a jiným diskrétním informacím legálně dostat, pak jsou pasovány do role prosebníka. Není pak žádnou výjimkou, když informační služby, policie nebo armáda nakupují u provozovatelů služeb UGC v tuzemsku nebo v zahraničí informace k ochraně distributivních nebo nedistributivních informačních práv nebo když se dokonce aktivně podílejí na zakládání služeb typu UGC, aby se k takovým údajům oklikou (prostřednictvím souhlasu uživatelů) samy dostaly.

Poslední axiologický paradox, kterému se zde budeme stručně věnovat, týká se nakládání s informacemi tvořenými nebo zpracovávanými státem. Nejde v tomto případě pouze o informace, které stát na základě svých informačních práv získává z diskreční sféry osob pod svou jurisdikcí, ale o obrovskou množinu informací veřejného sektoru, tj. informací, které stát při různých činnostech vytváří, zpracovává a komunikuje.[85] Vedle obsahů soudních spisů

[83] Viz *Zásady ochrany osobních údajů* [on-line]. Centrum pro ochranu osobních údajů Google [cit. 2. 9. 2011]. Dostupné z: <www.google.com/intl/cs/privacy/privacy-policy.html>.

[84] V brzké budoucnosti nebudou pozoruhodnou masou takových informací disponovat jen poskytovatelé služeb informační společnosti, ale také například dodavatelé energií, pronajímatelé nemovitostí apod. – srov. CRONIN, M. J. *Smart Products, Smarter Services*. Cambridge : Cambridge University Press, 2010, str. 169, 201.

[85] Pro tyto informace se vžila zkratka PSI – public sector information. Je třeba upozornit, že jde v tomto případě o veškeré informace produkované nebo zpracovávané státem včetně informací chráněných autorským právem, utajovaných skutečností a jiných informací spadajících mimo rozsah informační svobody (u nás označované jako právo na svobodný přístup k informacím).

nebo zpravodajských analýz tato kategorie zahrnuje například též běžnou úřední korespondenci, veřejnoprávní účetnictví, meteorologické informace, statistická data, jízdní řády veřejné dopravy apod. Charakter informací veřejného sektoru má rovněž například státem financovaná filmová produkce, veřejnoprávní televizní vysílání, výsledky státem financovaného výzkumu apod.

Nepovažujeme v tomto směru za paradoxní, že stát zpracovává, produkuje či komunikuje informace jdoucí nad rámec jeho primárního (minimálního) fungování. I v jiných než informačních oborech má především kontinentální Evropa dlouhodobé pozitivní zkušenosti s aktivním angažmá státu mimo výkon jeho primárních povinností či mimo základní ochranu práv.[86]

K paradoxu však dochází v situaci, kdy stát s využitím veřejných zdrojů produkuje nebo zpracovává informace, to však k selektivnímu soukromému užitku. Podobně paradoxní je i situace, kdy stát sice produkuje hodnotné informace, jejichž další využití by mohlo být společnosti ku prospěchu (společenskému i ekonomickému)[87] – tyto informace však nejsou veřejně dostupné a užitek z nich je mimo příslušný státní orgán prakticky nulový.

Typickou formou tohoto paradoxu jsou exkluzivní smlouvy na výkon státních informačních agend nebo na další zpracování informací veřejného sektoru. Namísto toho, aby informace produkované státem sloužily veřejnému zájmu (tím může být i zájem na ekonomické aktivitě, zaměstnanosti apod.), jsou zde informační kompetence státu využívány jen konkrétním (vyvoleným) podnikatelským subjektem.[88] Příkladem mohou u nás být Evropskou komisí identifikované avšak stále neřešené případy databáze spojení veřejné hromadné dopravy nebo agendy Obchodního věstníku.[89] Stát v těchto případech pověřil (otázkou navíc je, na základě jakého výběrového klíče) výkonem veřejné informační agendy konkrétní soukromý subjekt – ten sice agendu spravuje zdarma, vyhrazuje si však k výsledným informacím exkluzivní práva.[90] Vzniká pak paradoxní situace, kdy stát sice zákonným právem definuje veřejnou informační agendu (to navíc často s informační povinností různých subjektů do této agendy aktivně přispívat), nezabývá se však její správou, ekonomicky nezužitkovává její potenciál a dokonce formou exkluzivity přispívá k nepřirozeným informačním restrikcím. Ekonomický užitek by přitom mohly přinést nejen nabídka a zpoplatnění dalšího užití předmětných informací, ale i jejich prosté uvolnění k dalšímu komerčnímu využití zdarma – dosavadní šetření přitom ukazují, že právě

[86] V České republice tak příkladně stát chová koně nebo vaří a prodává pivo.

[87] Srov. odst. 5 preambule ke Směrnici Evropského parlamentu a Rady 2003/98/ES o opakovaném použití informací veřejného sektoru: *„Informace veřejného sektoru jsou důležitým výchozím materiálem výrobků a služeb digitálního obsahu a s rozvojem bezdrátových služeb obsahu se stanou ještě důležitějším zdrojem obsahu. V této souvislosti bude rovněž důležité široké zeměpisné pokrytí překračující hranice států. Rozšířené možnosti opakovaného použití informací veřejného sektoru by měly mimo jiné umožnit evropským společnostem využívat jejich potenciálu a přispívat k hospodářskému růstu a vytváření pracovních míst.“* Podrobnou studii ekonomického potenciálu PSI obsahuje poziční dokument COM (1998)585 - Green Paper on the Convergence of the Telecommunications, Media and Information Technology Sectors, and the Implications for Regulation Towards an Information Society Approach. V České republice se snahy podnikatelského sektoru o rozhýbání sekundárního trhu PSI soustředí okolo iniciativy CzechPSI, přičemž žádná viditelná veřejná iniciativa s výjimkou několika izolovaných projektů některých ústředních orgánů státní správy a krajů u nás neexistuje.

[88] Mimo jiné i z tohoto důvodu jsou exkluzivní dohody na další užití PSI zásadně zakázány. České zákonné právo je však v porovnání se shora cit. směrnicí mnohem méně důrazné a harmonizace ust. čl. 11 formou ust. § 14a odst. 3 a 4 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, je co do svého obsahu na hranici eurokonformity (nehledě na to, že zařazení problematiky dalšího využití PSI do struktury svobodného přístupu k informacím je z podstaty věci systematicky vadné).

[89] Srov. studii *PSI: Identification of potential Exclusive Agreement – Czech Republic* publikovanou na základě rektifikačního dokumentu COM/2009/0212 [on-line]. European Commission [cit. 25. 3. 2011]. Dostupné z: <www.ec.europa.eu/information_society/policy/psi>.

[90] Nepřípustnost takového řešení respektive jeho velký korupční potenciál diskutuje řada odborných publikací – srov. AICHHOLZER, G; BURKERT, H. *Public Sector Information in the Digital Age*. Northampton : Edward Elgar Publishing Limited, 2004, str. 12, 102.

bezúplatné nediskriminační zpřístupnění informací veřejného sektoru s sebou nese pro stát v řadě odvětví ten nejlepší ekonomický efekt.[91]

13.6 Shrnutí kapitoly

V této kapitole jsme se zabývali otázkou nedistributivních informačních práv státu. V úvodní části jsme konstatovali, že je v naší právní kultuře tomuto typu práv věnována poměrně menší pozornost v porovnání s distributivními právy, to především z důvodu základní orientace systému právních pravidel na člověka. Rovněž jsme konstatovali technický rozdíl v chápání nedistributivních práv mezi kontinentální evropskou právní kulturou a právní kulturou angloamerickou, který však nemá vliv na konstrukci nebo důležitost těchto práv – podstatný však je tento rozdíl, pokud jde o postavení státu a možnost delegace jejich výkonu.

Z aktuálních nedistributivních informačních práv státu jsme vybrali práva související s dostupností služeb informační společnosti, práva k zajištění informační bezpečnosti a konečně pak akcesorická informační práva státu konstruovaná k ochraně jiných distributivních nebo nedistributivních práv. Vzhledem k tomu, že byl kvantitativní dostupnosti služeb informační společnosti částečně věnován výklad předminulé kapitoly, zaměřili jsme se dále na diskusi kybernetické bezpečnosti a informačních práv státu.

Dospěli jsme k závěru, že ochrana národního kyberprostoru představuje aktuálně pro stát zásadní výzvu. Rezignaci na kybernetickou bezpečnost jako na nedistributivní veřejné dobro za situace, kdy se podstatná a stále se zvětšující část společenského života odehrává v prostředí informačních sítí, označili jsme za nebezpečí pro samotnou existenci státu a legitimitu práva. Současně však jsme připomněli, že ochrana veřejné (národní) bezpečnosti s sebou nese též nutnost zásahu do distributivních informačních práv člověka, konkrétně zejména do práva na informační sebeurčení. V tomto směru jsme dospěli k názoru, že jako adekvátního prostředku lze ve specifických případech proporcionálně užít i jinak nepřípustného blokování.

Podobně, jako jsme v páté kapitole konstatovali nutnost spolupráce státu a definičních autorit, dospěli jsme i v případě kybernetické bezpečnosti k závěru, že jedinou možností jejího efektivního zajištění je součinnost státu se soukromým, akademickým a občanským sektorem. Jako vhodné řešení jsme označili rozdělení dohledové činnosti mezi národní a vládní dohledová pracoviště a úpravu jejich kompetencí formou kombinace zákonných pravomocí vládního dohledu a povinností poskytovatelů veřejných služeb informační společnosti provozovat státem certifikované bezpečnostní technologie. Současně jsme poukázali na naléhavou potřebu řešit institucionální zajištění dělby moci respektive na vzájemné oddělení různých státních orgánů tak, aby žádný z orgánů politické moci nemohl pod záminkou ochrany kybernetické bezpečnosti získat nad ostatními informační dominanci.

V poslední části této kapitoly jsme se věnovali informačním oprávněním státu. Konstatovali jsme jejich akcesorický charakter, neboť jejich výkon zajišťuje faktickou existenci primárních distributivních nebo nedistributivních práv (informačních i jiných). Absence informačních práv státu pak může vést k situaci, kdy distributivní právo člověka nebo nedistributivní veřejné dobro existují jen teoreticky, tj. bez možnosti uplatnění (typicky bez sankce). Jako jeden z axiomatických paradoxů informačních práv jsme v tomto směru označili existenci deliktní odpovědnosti, kterou však bez konkrétních možností státu zajistit skutkové informace nelze uplatnit.

Specificky jsme pak diskutovali otázku identické proporcionality práva na informační sebeurčení. Akcesorická informační práva státu zde sice zasahují do práva na informační sebeurčení člověka, to však mimo jiné i k ochraně téhož práva. Příkladně soukromí tak lze v informačních sítích chránit pouze za cenu jeho omezení.

[91] Jednotlivé národní studie ze států, které implementovaly režim systematického zpoplatněného nebo bezúplatného poskytování PSI k dalšímu využití jsou k dispozici na portále iniciativy epsiPLUS. na adrese <www.epsiplatform.eu>.

Test proporcionality je v takovém případě prakticky zbaven třetího prvku, neboť při posuzování adekvátní míry zásahu stojí proti sobě vnitřně rozdělený tentýž právní princip – poměřování pak se děje nikoli ve vztahu ke chráněnému zájmu ale ke kontextu, v němž má být příslušná ochrana aplikována. Z toho mimo jiné plyne i skutečnost, že náhled na adekvátní proporcionalitu v rámci jednoho práva (zde práva na informační sebeurčení) se může měnit v čase nepoměrně rychleji, než je tomu ve standardních případech posuzování různých v kolizi stojících právních principů.

Za druhý axiomatický paradox informačních kompetencí státu jsme označili vztah stále formálně extenzivnější ochrany informační diskrece a přiznání platnosti formálním úkonům majícím povahu souhlasu člověka se zásahem do diskreční informační sféry. Především u služeb typu UGC jsme diskutovali situaci, kdy uživatel výměnou za atraktivní službu vzdává se prakticky ochrany pasivní složky práva na informační sebeurčení, a to ve prospěch podnikatelského subjektu. Ochranné instituty pak *de facto* nechrání informační sebeurčení člověka ani veřejný zájem, ale pouze výlučné postavení podnikatele, který disponuje formálním souhlasem. Paradoxně tak dochází k situaci, kdy i státní orgány jsou k ochraně distributivních nebo nedistributivních práv (včetně práv na informační sebeurčení) nuceny pokorně žádat tyto podnikatele o informace či za takové informace dokonce platit.

Jako poslední axiomatický paradox informačních práv státu jsme ke stručné diskusi vybrali postup státu v případech užití informací veřejného sektoru. Zatímco na jedné straně konstatuje stát formou zákona nebo podzákonného předpisu potřebu veřejnoprávní tvorby, zpracování nebo komunikace informací (to často dokonce současně se založením adresných informačních povinností), zajišťuje v některých oblastech existence exkluzivních smluv užitek z této informační aktivity primárně privilegovaným podnikatelským subjektům. Jakoby tedy i v tomto případě nefungovala nedistributivní informační práva jako akcesorické instituty k ochraně práv či státních zájmů, ale spíše jako nástroj k selektivní realizaci zisku. V porovnání s druhým axiomatickým paradoxem se v tomto případě situace liší ve výběru „vyvoleného“ podnikatelského subjektu – zatímco v prvním případě je to provozovatel atraktivní služby, který dokáže své uživatele pokoutně přesvědčit k tomu, aby mu potvrdili souhlas se zásahem do svého soukromí, je u exkluzivní smlouvy dáno vyvolení tím, že si příslušný státní orgán, Bůh ví z jakého důvodu, určitého podnikatele arbitrárně vybere.