Veřejnoprávní ochrana informační společnosti a místní působnost práva

Alice Táborová

1 Úvod

Je těžké určit, zdali se slavnostní pocity mořeplavců při zjevení úzkého pásu pevniny na obzoru dají srovnávat s okamžikem spuštění počítačové sítě. První kroky ke stvoření fenoménu, který v současnosti nazýváme internetem, na konci šedesátých let 20. století však neoddiskutovatelně tvoří historický mezník významem srovnatelný s objevením nové země. Otevřela se pomyslná dvířka do nového prostoru *ubi leones erant* a hranice existence, doposud spoutané vazbou na fyzický svět, se rozšířily takřka do nekonečna.

Nový virtuální svět prozatím nedotčený aktivitami člověka byl pro mnohé symbolem začátku nové éry lidstva spojované s návratem k původním hodnotám a svobodě. Byla to příležitost pro vytvoření utopického světa, kde morálka je nejvyšším zákonem a kde jakýkoli autoritativní dozor či vynucení není nezbytné.[1] Zmenšenou verzi takového ideálního světa lze pozorovat zvláště v počátcích internetu, kdy byl kyberprostor „hřištěm pro vybrané hráče" z převážně vědeckých a odborných kruhů. Polčák[2] toto období velmi trefně přirovnává k Ovidiovu zlatému věku lidstva, kdy převládal samovolný respekt k věrnosti a právu.

S rostoucí popularizací internetu a rozšiřováním uživatelské základny však došlo k pozvolné degradaci ideálu kybernetického světa a jeho postupnému ztotožňování se světem reálným. Virtuální povaha kyberprostoru nemohla zabránit převzetí některých záporných společenských jevů, mezi nimiž na předním místě figuruje i kriminalita. Přenesení prvků deviantního chování na virtuální scénu a vytváření nových charakteristických skutkových podstat trestných činů znamená těžký úder pro myšlenku kybernetické svobody a pozitivní anarchie bez nutnosti dozoru a donucení. Kyberzločin[3] se tak stává novým fenoménem, nechtěným dítětem technického pokroku a lidské zkaženosti.

Vývoj kriminality je nerozlučně spjat s vývojem společnosti a jednotlivými sférami jejího fungování. Každá oblast lidské činnosti, ať už jde o činnost z „pozemského" světa[4] nebo tu zcela novou a pro virtuální svět specifickou, je následována stínem deviantního chování, které ji má za cíl narušit. Vytváří se tak paralela mezi vývojem společnosti a vývojem jednání, které má za cíl ji poškozovat. Nevídaně rychlá a radikální politická, sociální a ekonomická restrukturalizace světa, která proběhla v posledních několika desetiletích, s sebou přinesla i revoluci ve světě zločinu. Zejména postupná virtualizace mnoha sfér lidské komunikace a všeobecně uplatňované tendence k zjednodušení a zpřístupnění kyberprostoru širokým masám usnadnily i nevídaný rozvoj na poli kriminality.

Tento článek si klade za cíl popsat některé z problémů, které vznikají v souvislosti s právní ochranou před společensky nežádoucími aktivitami provozovanými v prostředí globalizované informační sítě. Autorka se zde zaměří především na obor trestního práva a pokusí se diskutovat otázku, do jaké míry představuje existence kyberprostoru pro veřejné právo kvalitativně nový jev a jak právo na tento jev reaguje. V úvodní kapitole bude proveden obecný výklad zaměřený na definování povahy a podstaty fenoménu kyberkriminality. Komentovány budou také některé ze základních problémů, které v souvislosti s aplikací tradičních konceptů trestního práva vznikají. Následující kapitola poskytne rozbor jednotlivých principů, na jejichž základě je v kyberprostoru určována jurisdikce a působnost práva. Tyto principy jsou prakticky totožné s tradičními zásadami aplikovanými v „pozemském" světě, v prostředí informačních technologií však jejich uplatnění nabývá zcela nový rozměr, na který musí být brán zvláštní zřetel. V kapitole třetí se autorka pokusí nastínit přehled právní úpravy předmětné problematiky. Část zvláštní již bude věnována konkrétním otázkám veřejnoprávní ochrany globalizovaných informačních struktur, především zhodnocení práv a povinností poskytovatelů služeb informační společnosti[5] (angl. *Internet Service Provider*, dále jen „ISP"), daných normami trestního práva. V kapitole čtvrté tak bude proveden rozbor institutu trestněprávní odpovědnosti ISP především ve vztahu k českému právu. Kapitola pátá se zaměří na aktuální otázky konstrukce a realizace pravomocí státních orgánů blokovat či odpojovat komunikační linky z pohledu české i zahraniční právní úpravy. Tato problematika je velmi úzce spojena s okruhem otázek souvisejících s prokazováním jednotlivých deliktů v procesech autoritativní aplikace práva, kterým se chce autorka ve svém výkladu taktéž průběžně věnovat.

2 Kyberkriminalita

2.1 Stručný nástin problémů spojovaných s trestněprávní regulací kyberprostoru

Pokusy o definování kyberzločinu s sebou přinášejí řadu nejasností. Jednou z těch základních je otázka, zdali a v jaké míře se tento fenomén odlišuje od dnes již klasického pojetí „pozemského" trestného činu. Jinými slovy sledujeme otázku nezbytnosti vytváření nových specifických skutkových podstat trestných činů, jejichž základní charakteristikou je právě to, že jsou vázány na virtuální svět kybeprostoru. Ptáme se, do jaké míry lze například v právní úpravě použít „staré známé pojmy", jakými mohou být třeba podvod, terorismus nebo šikana, a zdali vznikne přenesením do nehmotného virtuálního světa zcela nová skutková podstata, nebo jde jen o rozšíření původní skutkové podstaty na novou oblast.

Dalším problémem je rozhodování, které oblasti je vůbec vhodné trestněprávně regulovat. Názory na tuto otázku se liší – svou roli hraje geografie, specifika právní kultury a sociálně-politického myšlení v jednotlivých oblastech. Jako

1 Na základě této vize vznikla i organizace *Electronic Frontier Foundation*, jedno z nejvýznamnějších hnutí za svobodný internet, které se již dvacet let angažuje proti jakémukoli omezování svobody jedince na internetu. Zajímavý příběh jejího vzniku, často spojovaný se jménem amerického umělce a politického aktivisty J. P. Barlowa, podrobně popsali autoři Goldsmith a Wu ve své knize: GOLDSMITH, J. – WU, T. *Who controls the Internet: Illusions of a borderless World*. 2. vyd. Oxford: Oxford University Press, 2008. s. 17 – 22.

2 Viz GŘIVNA, T. – POLČÁK, R. – HERCZEG, J. et al. *Kyberkriminalita a právo*. 1. vyd. Praha: Nakladatelství Auditorium, 2008. s. 17.

3 Termín *„zločin"* resp. *„kyberzločin"* používaný v tomto článku je zvolen záměrně jako nejvhodnější překlad anglického slova *„crime"* resp. *„cybercrime"*. Nejedná se tedy o pojem zločinu, jak jej upravuje ustanovení §14 odst. 3 zákona č. 40/2009 Sb., trestního zákoníku, ve znění pozdějších předpisů. V terminologii českého trestního práva je zde používaný pojem *„kyberzločin"* ztotožnitelný s pojmem *„trestný čin v kyberprostoru"* resp. *„počítačový trestný čin"*.

4 Jedná se o překlad anglického výrazu *„terrestrial world"*, použitého v článku: GOODMAN, M. D. – BRENNER, S. W. The Emerging Consensus on Criminal Conduct in Cyberspace. *International Journal of Law and Information Technology*. 2002, roč. 10, č. 2, s. 150.

5 Informační společnost popisuje Polčák jako sociální systém, který je organizovaný prostřednictvím informací a ve kterém je zároveň umožněno jejich spontánní vytváření, zpracování a výměna. Podrobněji viz: GŘIVNA, T. – POLČÁK, R. – HERCZEG, J. et al. *Kyberkriminalita a právo*. 1. vyd. Praha: Nakladatelství Auditorium, 2008. s. 23.

klasický příklad může být použito srovnání chápání rasistických projevů v České Republice a v USA. Zatímco dle zákona č. 40/2009 Sb., trestního zákoníku, ve znění pozdějších předpisů (dále jen „trestní zákoník“) můžeme po naplnění skutkové podstaty trestného činu označit rasistické projevy jako hanobení národa, rasy, etnické nebo jiné skupiny osob (ustanovení § 355 trestního zákoníku), je ten samý projev (tzv. „*hate speech*“) v USA chráněn Prvním dodatkem Ústavy Spojených států amerických jako výraz svobody slova.[6] Ten samý čin je tedy paradoxně v jednom státě právem chráněn a ve druhém právem potírán. V „pozemském“ světě tento rozpor v praxi větší problémy nepřináší, přeneseme-li však meritum věci do světa virtuálního, kde fyzické hranice nehrají roli a jakýkoli čin je schopen vyvolat následky na druhé straně zeměkoule, dostává otázka trestnosti a potrestání zcela nový rozměr.

Globální charakter kyberzločinu přinesl nové výzvy i do oblasti nadnárodní spolupráce. Mezinárodní společenství si již uvědomilo negativní potenciál nově vznikajícího fenoménu. Hledání všeobecného konsenzu, který by umožnil vytvoření právního předpisu na mezinárodní úrovni, však kromě teoretických otázek uvedených výše poznamenává i pomalost a nepružnost celého systému mezinárodní spolupráce. V porovnání s rychlostí vývoje v kyberprostoru jsou pak přijímaná opatření mnohdy zpozdilá a nedostatečná.[7] Vzhledem k technickému charakteru kyberzločinu je také stále více aktuální hledání odpovídajících technologických regulací a všeobecných standardů. I zde je adekvátní nadnárodní spolupráce na všech úrovních naprosto nezbytná.

Otázky položené výše jsou pouhým letmým nástinem problémů, kterými je třeba se při hledání vhodné regulace zaobírat. Předchozí odstavce tak znázorňují klasický vzorec zákonodárného uvažování – hledání definic, snaha problém pojmenovat a „narýsovat střih“, tedy otázka: „*Co regulovat?*“ Následné stříhání, měření, šití a přešívání, „aby nový oblek seděl na míru“, čili: „*Jak regulovat?*“ Před „šitím obleku“ je však nezbytné položit si jinou základní otázku – „Je oblek vhodným oděvem pro danou příležitost? Bude tento oblek skutečně nošen nebo zůstane viset ve skříni?“ Jinými slovy: „*Regulovat vůbec?*“ Pokud ano, pak: „Je pro tuto příležitost skutečně nezbytné šít nákladný oblek, nestačil by méně formální oděv, který už ve skříni visí?“ Časté opomíjení poslední otázky ze strany zákonodárce neodrazuje experty od hledání jiných forem regulace kyberprostoru, než je právní předpis. Jak již bylo zmíněno v předchozí podkapitole, objem procesů ve virtuálním světě již přesáhl hranice možností samoregulace a mnohdy je nezbytný zásah „vyšší moci“ reprezentované státem.

2.2 „Lessigův kód“

Otázkou tedy stále zůstává, jaký je nejúčinnější způsob, kterým se lze zasadit o komplexní harmonické fungování ve světě kyberprostoru, a jak lze v tomto naprosto specifickém nehmotném světě efektivně eliminovat entropické vlivy a v případě narušení dosáhnout co nejrychleji tolik potřebné rovnováhy. Cestu k hledání odpovědi není možno započít bez charakterizování entit, které svými aktivitami kyberprostor vytvářejí a ovládají. Polčák[8] nazývá tyto entity tzv. *definičními autoritami*. Vychází ze závěrů amerického konstitucionalisty Lawrence Lessiga, který se ve své knize Code 2.0[9] zabývá fenoménem kódu a jeho role v regulování světa informačních technologií. Polčák tak shrnuje výchozí bod Lessigovy teorie do výstižné definice, podle níž je kód „*předpisem, na jehož základě funguje informační infrastruktura – kód tedy kauzálně determinuje chování jednotlivých složek dohromady tvořících informační síť*.“ Zároveň varuje před přílišným zúžením chápání kódu pouze jako počítačového programu. Podle něj je pod pojem kódu nutno podřadit i jiné formy kauzálních technických pravidel – např. parametry prostředí, formáty dat, množstevní omezení v podobě kvót, přenosové protokoly apod. [10]

Kód je v Lessigově chápání autoritativně vytvořenou definiční normou, která má schopnost ovlivňovat prostředí kyberprostoru podobně jako přírodní zákon svět fyzický. Na rozdíl od přírodního zákona však může daná autorita svou vůlí předmětný kód modifikovat a aktivně tak ovlivňovat jeho účinky na prostředí. Kód je oproti jiným normám (zde především právním) významný svou vysokou efektivitou a rychlostí, se kterou je schopen vyvolat žádaný účinek. Zatímco právní norma stanovuje určitá pravidla, jejichž efekt musí být mnohdy následně vynucován další aktivitou ze strany státu, kód oproti tomu již přímo ze své podstaty modifikuje regulované chování tak, aby odpovídalo vůli příslušné autority, a umožňuje tak prostředí informačních sítí účinně utvářet. Kódy vytvářené jednotlivými definičními autoritami se vzájemně ovlivňují a funkčně i existenčně na sobě závisí. Vzniká tak komplikovaná rozvrstvená síť tvořená základní fyzickou informační a komunikační infrastrukturou, operačními systémy, datovými formáty apod.[11] Definiční autority, kterými mohou být na základě výše uvedeného *de facto* všichni, kdo jakýmkoli způsobem přicházejí do styku se světem informačních technologií (tj. producenti softwaru, ISP, vlastník e-mailové schránky, provozovatel chatroomu apod.), tak na základě šíře svých kompetencí reálně pozitivně i negativně ovlivňují existenci informací, jejich vlastnosti i jejich fungování.

Význam působení definičních autorit v prostředí informačních technologií je nesmírně důležitý i pro zhodnocení jejich vztahu k právu.[12] Jednotlivé autority jsou ve své existenci i aktivitách podřízeny jurisdikci jednotlivých států, zároveň chce-li stát v jimi ovlivňovaném prostředí cokoli prosadit, neobejde se bez jejich součinnosti. Vyvstává tak problém určení pravomocí orgánů jednotlivých států při prosazování práva ve vztahu k aktivitám jednotlivých entit a jejich vazbám na fyzický svět (tedy jejich sídlo resp. místo pobytu nebo např. protiprávní efekt jejich činnosti apod.). Tímto problémem

6 Více k tomuto článku lze nalézt například v těchto příspěvcích: CANNON, C. M. Free Speech vs. Hate Speech. *Politics Daily* [online]. vyd. 18. 08. 2009 [cit. 2010-24-01]. Dostupné z: <http://www.politicsdaily.com/2009/08/18/free-speech-vs-hate-speech>. nebo BAKER, C. E. Hate Speech [online]. University of Pennsylvania Law School, 2008, vyd. 3.10.2008 [cit. 2010-25-01]. Dostupné z: <http://lsr.nellco.org/cgi/viewcontent.cgi?article=1212&context=upenn_wps>.

7 Rozbor a hodnocení existujících právních nástrojů poskytnou následující kapitoly.

8 Pro podrobnější analýzu nahlédněte do POLČÁK, R. *Právo na internetu: Spam a odpovědnost ISP*. 1. vyd. Brno: Computer Press, a.s. 2007, s. 42 – 46.

9 Viz LESSIG, L. *Code 2.0*. 1. vyd. New York: Basic Books. 2006, 410 s.

10 Viz POLČÁK, R. *Právo na internetu: Spam a odpovědnost ISP*. 1. vyd. Brno: Computer Press, a.s. 2007, s. 43.

11 Viz POLČÁK, R. *Právo na internetu: Spam a odpovědnost ISP*. 1. vyd. Brno: Computer Press, a.s. 2007, s. 43.

12 Lessig ve svém díle zohledňuje i význam dalších faktorů působících na prostředí kyberprostoru, jako jsou například etické normy, sociální pravidla, samoregulační a samoorganizační mechanismy či pravidla ekonomiky. Pro dosažení účelu této kapitoly se autorka zaměří pouze na oblast práva.

se budeme zabývat v kapitole věnované jurisdikci a působnosti práva.

Z Lessigových a Polčákových myšlenek lze vyvodit závěr, že aktivní vliv jednotlivých definičních autorit je esenciální pro samotnou existenci a fungování kyberprostoru. Mají-li zde tedy být prosazeny právní normy resp. právo jako fungující celek, lze tak učinit pouze prostřednictvím působení na tyto definující entity, které zároveň z vlastní iniciativy a ve vlastním zájmu regulují komplexní fungování celého systému. Jednou z variant, jak zabránit určité nežádoucí činnosti, je zajistit, aby vůbec možnost chovat se nežádoucím způsobem nevznikla – neposkytneme-li potenciálnímu pachateli možnost volby, zda se chce a bude chovat protiprávně nebo ne, vyhneme se riziku, že se vydá „cestou mimo zákon". Tato konstrukce může fungovat jako jeden ze základů pro ospravedlnění autoritativních zásahů státu ve formě blokování a odpojování komunikačních linek v globální síti, o kterých bude pojednáno v kapitole páté.

2.3 Definice kyberzločinu a jeho specifika

Nejobecněji lze kyberzločin definovat jako *„počítačové aktivity, které jsou buď protiprávní, nebo za nezákonné považovány určitými stranami a které mohou být vykonávány prostřednictvím globálních elektronických sítí."*[13] V teorii bývá pojem „kyberzločin" (*cybercrime*) někdy zaměňován s pojmem „počítačový trestný čin" (*computer crime*). „Počítačový trestný čin" se používá pro označení všech útoků, jejichž cílem jsou počítačová data obecně. „Kyberzločin" je tedy pojmem o něco širším, neboť umisťuje počítačové trestné činy do prostředí elektronických sítí – charakteristická je pro něj propojenost s globálním kyberprostorem. V praxi však dochází k volnému zaměňování těchto pojmů mezi sebou, vznikají i nová označení jako „*high-tech* zločin" (*high-tech crime*) nebo „trestný čin v oblasti informačních technologií", „IT zločin" (*IT crime*). Definování tedy není jednotné a dokonale odráží globální charakter a složitost celé problematiky. [14]

Trestný čin v kyberprostoru je typickým příkladem tzv. distančního deliktu, kdy mezi jednáním pachatele a jeho následkem nebo účinkem existuje určité rozpětí neboli distance – místní, časová nebo obojí. Od toho jsou tedy odvozeny v teorii používané pojmy distance časová, distance místní a distance místní a časová.[15] Určení charakteru deliktu po této stránce je stěžejní především při řešení jurisdikčních otázek, kterým se bude věnovat následující kapitola.

Kategorizací kyberzločin rozdělujeme do tří resp. 2+1 oblastí. Do první kategorie spadají činy, jejichž cílem je počítač nebo síť jako taková – narušení jejich zabezpečení, integrity a fungování (např. hackerské útoky, šíření virů apod.). Druhá kategorie zahrnuje „klasické" trestné činy, jako jsou třeba podvod, krádež či šíření dětské pornografie, spáchané s pomocí nebo prostřednictvím počítače. Do třetí oblasti pak patří „klasické" trestné činy, při kterých bylo incidentálně použito počítače (např. pro komunikaci mezi pachateli či pro napsání dopisu vyděračem apod.) Rozdíl mezi druhou a třetí kategorií spočívá v roli, jakou hraje použití počítače v celém problému. Zatímco v případě trestných činů spáchaných s pomocí nebo prostřednictvím počítače je využití počítače esenciální součástí procesu, bez něhož by nebyla naplněna daná skutková podstata trestného činu, u kategorie třetí nehraje použití počítače pro naplnění skutkové podstaty roli. Svůj význam však může sehrát při následném hodnocení závažnosti trestného činu a při rozhodování o trestu. Vzhledem k výše uvedenému nebývá často třetí kategorie v teorii zmiňována. Zvyšující se nároky při vyšetřování takových trestných činů a rostoucí význam kyberforenzní praxe však zohlednění této kategorie dostatečně ospravedlňují.[16]

Národní i mezinárodní právní dokumenty poskytují řadu různě přesných a podrobných vyjádření skutkových podstat kybernetických trestných činů. Nehledě na konkrétní definice můžeme určit několik charakteristických okruhů. Brenner[17] nabízí shrnutí do osmi kategorií:

1. Hacking a jemu podobné aktivity – neoprávněný průnik do informačního systému provedený zpravidla ze vzdáleného počítače a následná neautorizovaná činnost prováděná v rámci napadeného systému. V praxi se rozlišují pojmy *hacking* (spojován s jinou nežli zištnou resp. destrukční motivací) a *cracking* (jehož cílem je neoprávněný zisk či spáchaná škoda).[18]

2. Šíření tzv. *malware*, škodlivého *softwaru* – počítačových virů a jiných programů způsobujících poškození systému – zahrnuje *„jakýkoli software, který při svém spuštění zahájí činnost ke škodě systému, ve kterém se nachází. Jeho vnější projevy mohou být časovány, nebo reagují na konkrétní naprogramovanou spouštěcí událost."*[19] (např. *infoware, adware, spyware,* trójský kůň, červ aj.)

3. Podvod a krádež spáchané prostřednictvím nebo s pomocí informačních technologií (např. zcizování digitální identity prostřednictvím *phishingu* a následné využití získaných informací k neoprávněným bankovním transakcím) – omračující úspěšnost podvodníků pramení především z důvěřivosti spotřebitelů, kteří si plně neuvědomují svou odpovědnost za ochranu vlastních osobních dat.

4. Gamblerství, pornografie a jiné činy v rozporu s morálkou a dobrými mravy – rozsah omezení se stát od státu výrazně liší – například zatímco v Ruské Federaci je *online gambling* federálním zákonem o státní regulaci organizování

13 Viz definice použitá v článku: THOMAS, D. – LOADER, B. D. *Cybercrime.* 2. vyd. London: Nakladatelství Routledge, 2000. s. 3.

14 Autorka bude pro zjednodušení i nadále používat pouze pojem „kyberzločin".

15 Podrobněji se tímto tématem zabývá např. KRATOCHVÍL, V. – KUCHTA, J. – MATES, P. *Trestní právo hmotné: Obecná část.* 3. vyd. Brno: Masarykova univerzita, 2003. s. 97.

16 Více viz GOODMAN, M. D. Why the Police Don´t Care About Computer Crime. *Harvard Journal of Law and Technology*. 1997, roč. 10, s. 468 – 469.

17 Viz GOODMAN, M. D. – BRENNER, S. W. The Emerging Consensus on Criminal Conduct in Cyberspace. *International Journal of Law and Information Technology*. 2002, roč. 10, č. 2, s. 146 – 150.

18 Pro podrobnější informace viz např. THOMAS, D. – LOADER, B. D. *Cybercrime*. 2. vyd. London: Nakladatelství Routledge, 2000. s. 36 – 84.

19 Definice byla přejata z článku *Základní definice vztahující se k tématu kybernetické bezpečnosti.* [online]. Ministerstvo vnitra České Republiky, 2009 [cit. 2010-24-01]. Dostupné z: <http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx>.
Někteří autoři řadí mezi kybernetické trestné činy i hromadné šíření nevyžádaných zpráv (*spamu*), které jsou infikovány viry, trojským koněm apod. Mezi škodlivý *spam* je řazen také tzv. *scam nigerijského typu*, jehož prostřednictvím rozesilatel podvodně vyláká na oběti určitou částku pod záminkou dobročinnosti nebo pomoci v nouzi. *Spam* je tedy specifickým prostředkem, prostřednictvím kterého se lze dopustit činů uvedených v bodě 2. a 4., proto často nebývá mezi kyberzločiny zařazován. Více viz: VOLEVECKÝ, P. Kybernetická trestná činnost v mezinárodních dokumentech a v dokumentech ES/EU. *Trestní právo*. 2009, roč. 8, č. 7 – 8, s. 26 – 38.

a provádění hazardních her[20] zakázán, australský *Interactive Gambling Act* staví mimo zákon poskytování takových služeb v Austrálii, samotné hraní online však protiprávní není apod.

5. Dětská pornografie a trestné činy páchané na nezletilých – existuje všeobecný konsenzus, který staví pořizování dětské pornografie a nakládání s ní mimo zákon. Diskutuje se však například o škodlivosti a nebezpečnosti počítačem vytvořených animací, které nezobrazují skutečné žijící osoby a při jejichž vzniku tedy nedošlo ke zneužití nezletilého.

6. Šikana, harašení, projevy hanobící rasu, národ či přesvědčení – společnost je stále více vázána na virtuální komunikaci a tím se stává výrazně zranitelnou i jejím obsahem (tzv. „*hate speech*" viz výše).

7. Jiné trestné činy proti fyzickým osobám – např. „kybervražda" jako úmyslné usmrcení druhého prostřednictvím informačních technologií doposud zaznamenána nebyla, avšak reálné nebezpečí takových útoků stoupá. Jako klasický případ se uvádí průnik do elektronické databáze nemocničního zařízení a pozměnění informací v lékařských záznamech pacienta, které následně způsobí pacientovu smrt (např. úmyslná změna dávkování léků).

8. Kyberterorismus – je jen otázkou času, kdy si teroristé uvědomí, že k vyvolání strachu a ohrožení životů není potřeba náročných příprav, fyzické námahy a pochybného mučednictví. Prostřednictvím počítače bude možné přerušit dodávky elektřiny pro celá města, narušit záchranné telekomunikační sítě, zasahovat do letového provozu apod.[21]

Na základě získávaných poznatků lze jmenovat několik znaků, které jsou pro kyberzločin charakteristické a odlišují jej tak od trestných činů „pozemských":

- Naučit se postup pro spáchání takových trestných činů je v zásadě *snadné*.
- V porovnání se škodami, které tyto trestné činy mohou způsobit, vyžadují nemnoho zdrojů a jsou *levné*.
- Mohou být spáchány v rámci určité jurisdikce, aniž by jí byl pachatel podroben *fyzicky*.
- Jejich protizákonný charakter je často *diskutabilní*.[22]
- Vzhledem k charakteru doby jsou informační technologie velmi mocným nástrojem. Jejich ohrožení kyberzločinem je tedy spojováno s *riziky* doposud nevídaných rozměrů.
- Počítačová data jsou snadno *přenosná* a není snadné jejich tok sledovat. Pro boj s kyberzločinem jsou proto nezbytné technologicky náročné postupy, které se rychle vyvíjejí a přizpůsobují aktuální situaci.
- Kyberzločin je *neosobní*. Pro „pozemský" zločin je charakteristické, že pachatel i oběť jsou součástí jedné společnosti, je snazší vytvořit vzorce deviantního chování a tím lze obě strany snáze definovat. Oddělení virtuální identity od fyzického základu a geografický dosah, který mohou aktivity v kyberprostoru mít, utvoření platných vzorců prakticky znemožňují.

3 Trestněprávní jurisdikce v kyberprostoru

3.1 Pojem působnosti a jurisdikce

Jak již bylo zmíněno výše, globální dopad přeshraniční trestné činnosti na internetu vyžaduje specifická právní řešení. Pachatel, který není v kyberprostoru v zásadě nijak fyzicky limitován, může svou aktivitou vyvolat stejně neomezené výsledky – ať již geograficky nebo jejich množstvím. Zde leží kámen úrazu – kyberprostor je bez hranic, aktivita v něm není fyzicky omezena a její případné škodlivé následky mohou též narůst do globálních rozměrů – moc státu, který má tuto aktivitu regulovat, však fyzicky limitována je. Zatímco problém vzniká a šíří se neovlivněn geografickým uspořádáním světa, je stát jako řešitel tohoto problému tím samým uspořádáním spoután. Území je jedním z prvků, které charakterizují moderní stát,[23] a v rámci tohoto území pak stát uplatňuje svou státní moc, jakožto *„legitimní právem sankcionovanou schopnost státu ovlivňovat subjekty společenských vztahů a jejich chování (a to i proti jejich vůli)."*[24] Svrchovaná státní moc je nezávislá a již ze své podstaty eliminuje moci konkurující působící zvnějšku.

Jurisdikce, čili pravomoc orgánů státu – nositelů státní moci, je realizována v třech rovinách[25] :

- právo vytvářet závazná pravidla chování
- právo rozhodovat spory vznikající v rámci těchto pravidel a
- právo tato pravidla resp. rozhodnutí mocensky prosazovat

Výše zmiňovaná pravomoc, uplatňovaná v rámci území státu, bývá někdy označována jako jurisdikce v užším slova smyslu. Svou pravomoc může totiž stát uplatňovat i na poli mezinárodním – jedná se o pravomoc vstupovat do mezinárodních vztahů, podílet se na vytváření mezinárodně uznávaných pravidel chování a být těmito pravidly vázán. V nejužším slova smyslu je pak pojem „pravomoc" používán ve spojitosti

20 Viz Федеральный закон о государственном регулировании деятельности по организации и проведению азартных игр и о внецении изменений в некоторые законодательные акты Российской Федерации, N 211-Ф3.

21 Více naleznete na *Cyberterrorism*. [online]. NATO [cit. 2010-24-01]. Dostupné z: <http://www.nato.int/STRUCTUR/library/bibref/cyberterrorism.pdf>.

22 Základní čtyři znaky jsou zmíněny v článku GOODMAN, M. D. – BRENNER, S. W. The Emerging Consensus on Criminal Conduct in Cyberspace. *International Journal of Law and Information Technology*. 2002, roč. 10, č. 2, s. 142.

23 Tento princip je vyjádřen v tzv. *Jellinekově tříprvkové teorii státu*, která zavádí tři prvky státnosti – státní území, státní obyvatelstvo a veřejná moc. Mezinárodní právo veřejné pak k tomuto přidává ještě jeden prvek, a tím je mocenské prosazení se na poli mezinárodního práva (především způsobilost státu vstupovat do mezinárodně právních poměrů). Více viz:
MALENOVSKÝ, J. *Mezinárodní právo veřejné: jeho obecná část a poměr k jiným právním systémům, zvláště právu českému*. 5. vyd. Brno: Vydavatelství Masarykovy univerzity a Nakladatelství Doplněk, 2008. s. 107 – 115.
ČEPELKA, Č. – ŠTURMA, P. *Mezinárodní právo veřejné*. 1. vyd. Praha: Nakladatelství C. H. Beck, 2008. s. 54.

24 Viz FILIP, J. – SVATOŇ, J. – ZIMEK, J. *Základy státovědy.* 4. vyd. Brno: Vydavatelství Masarykovy univerzity, 2006. s. 17.

25 Viz KOHL, U. *Jurisdiction and the Internet.* 1. vyd. Cambridge: Cambridge University Press, 2007. s. 16.

s vymezením oblasti právních vztahů, o nichž může rozhodovat konkrétní soud.[26] [27]

Je důležité podotknout, že pojem „jurisdikce", tedy pravomoc, bývá občas používán se značnou volností a objevuje se i s významem „působnost práva". Při uplatnění určujících principů uvedených níže v podkapitole 3.4 to zdánlivě ztrácí význam, protože se tyto principy používají *de facto* zároveň, jak při určení pravomoci tak i působnosti. Je však nezbytné mít stále na paměti rozdíl mezi těmito dvěma pojmy: „pravomoc", tedy soubor práv a povinností, kterými je stát nadán, kontra „působnost", čili vyjádření kdy, kde, v jaké věci a vůči komu tato práva a povinnosti uplatňuje. V podstatě tak dochází k uplatnění pravomoci v rámci působnosti práva dané aplikací jednotlivých principů (např. místní působnost daná na základě principu teritoriality, registrace, aktivní/pasivní personality, ochrany a universality nebo působnost osobní uplatněná použitím kritéria personality).

3.2 Princip „dvojí trestnosti"

Tradičně je jurisdikce/působnost[28] uplatňována na základě principu teritoriality. Právo státu tak působí v rámci jeho území a stát tak má pravomoc určovat zde závazná pravidla jednání a prosazovat je vůči všem, kdo se na jeho teritoriu nacházejí. Uplatňování tohoto principu je charakteristické především právě pro oblast trestněprávní, neboť trestní právo jako součást práva veřejného chrání vitální zájmy státu a společnosti.[29] Technický vývoj a zvyšující se mobilita obyvatel, které jsou charakteristické pro 20. a 21. století, však postupně mění chápání trestněprávní jurisdikce a působnosti trestního práva a uplatňují se i další právní principy, o kterých bude pojednáno níže v této kapitole. Množí se trestná činnost, jejíž důsledky překračují hranice států, pachatelé se mohou velmi rychle přesunovat z místa na místo a v rámci kyberprostoru dokonce nemusí být přítomni fyzicky vůbec.[30] Učebnicovým příkladem je případ rozšíření viru *I Love You* v květnu 2000.

> Během jediného dne 5. května roku 2000 se virus rozšířil přes Hong Kong do Evropy a USA. Ke dni 13. května bylo evidováno kolem 50 milionů napadení počítačového systému tímto virem a škody se vyšplhaly k 5,5 miliardám dolarů. Virus, vytvořený v jazyce *VBScript* napadal počítačový systém *Microsoft Windows*. Poté, co uživatel spustil přílohu infikovaného e-mailu, se virus rozeslal na veškeré kontakty obsažené v aplikaci *Microsoft Outlook*. Virus způsobil především změny v systémových souborech a u některých specifických souborů i jejich odstranění.[31] FBI ve spolupráci s filipínskými vyšetřovacími orgány lokalizovaly místo vzniku do filipínského hlavního města Manily. Jako tvůrce a hlavní šiřitel viru byl identifikován filipínský občan Onel de Guzman. Trestní stíhání de Guzmana však bylo znemožněno tím, že v dané době nebylo šíření *malware* trestným činem dle filipínského práva. USA tak nemohly ani požádat o de Guzmanovo vydání k potrestání dle práva Spojených států amerických.

Ve výše zmíněném případě byl uplatněn tzv. „*princip dvojí trestnosti*" jako výraz zachování suverenity zúčastněných států. Dle tohoto principu může být občan resp. resident ze státu A vydán k trestnímu stíhání do státu B pouze pod podmínkou, že čin je kvalifikován jako trestný v obou dotčených státech. Pokud by tomu tak nebylo, mohl by být občan resp. resident státu A, který jednal v souladu s právním řádem tohoto státu, vydán k trestnímu stíhání do státu B, kde je to samé jednání trestným činem. Pravomoc státu jakožto vykonavatele práva vůči osobám nacházející se v rámci jeho teritoria by tak byla narušena stejně tak jako právní jistota, kterou má stát vůči osobám na svém teritoriu zaručovat.[32]

3.3 Trestněprávní jurisdikce - test přiměřenosti

V kontextu moderní koncepce jurisdikce se hovoří o využití tzv. *testu přiměřenosti*.[33] Jedná se o souhrn hledisek, na základě jejichž posouzení stát rozhoduje o uplatnění své jurisdikce v konkrétním případě. Tato hlediska jsou přehledně sepsána v souhrnném textu pravidel mezinárodního práva s názvem *Restatement (Third) of Foreign Relations Law of the United States.*[34] Ač tento text již ve svém názvu odkazuje na právo platné v USA, je díky své obecnosti a přehlednosti použitelný i při výkladu otázek týkajících se jurisdikce obecně.[35] Jurisdikce státu se vztahuje na:[36]

1. a) jednání, které se zcela nebo z podstatné části odehrává na jeho území

26 Jak je například uvedena v ustanovení §7 zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů.

27 KOHL, U. *Jurisdiction and the Internet.* 1. vyd. Cambridge: Cambridge University Press, 2007. s. 14.

28 Aby se autorka vyhnula nevhodně složitému a komplikovanému výkladu, kdy jeden a ten samý princip aplikuje při určení jurisdikce a zároveň působnosti, rozhodla se pro zjednodušení v dalším výkladu hovořit pouze o jurisdikci. Pojmům „pravomoc", „působnost", „kompetence" a jejich vzájemnému úzkému propojení se ve své kvalifikační práci věnuje i Milan Kvasnička. Zdůrazňuje nejednotnost chápání těchto pojmů v dílech významných právních teoretiků, viz: KVASNIČKA, M. *Rozhodování kompetenčních sporů.* [online]. 2007 [cit. 2010-03-27]. 80 s. Magisterská diplomová práce. Masarykova univerzita, Právnická fakulta. Vedoucí práce Vojtěch Šimíček. Dostupné z www: <http://is.muni.cz/th/74792/pravf_m/?info=1>.

29 Viz POLČÁK, R. Místní působnost trestního práva. *Kolizní otázky internetových právních vztahů* [online]. Brno: Masarykova univerzita, [cit. 2010-02-04].

30 Blíže viz BRENNER, S. W. – KOOPS, B.-J. Approaches to Cybercrime Jurisdiction. *Journal of High Technology Law*. 2004, roč. 4, č. 1, s. 6.

31 Více viz I Love You. *Wikipedia* [online]. Naposledy editováno 15. 12. 2009 [cit. 2010-02-04]. Dostupné z: <http://cs.wikipedia.org/wiki/I_Love_You>.

32 Podrobněji se k této problematice vyjadřuje BRENNER, S. W. – KOOPS, B.-J. Approaches to Cybercrime Jurisdiction. *Journal of High Technology Law*. 2004, roč. 4, č. 1, s. 7.

33 Anglicky označen jako „*reasonability test*", viz BRENNER, S. W. – KOOPS, B.-J. Approaches to Cybercrime Jurisdiction. *Journal of High Technology Law*. 2004, roč. 4, č. 1, s. 8 – 10.

34 Viz *Restatement (Third) of Foregn Relations Law of the United States* [online]. [cit. 2010-02-04]. Dostupný z: <www.macalester.edu/courses/intl114/docs/restatement.pdf>.

35 *Restatements of the Law* – jedná se o právní texty vydávané Americkým právním institutem (*American Legal Institute*, ALI). Renomovaní soudci, právníci a pedagogové vytvářejí na základě judikatury, právních předpisů a poznatků právní praxe jakýsi „destilát" obecných právních poznatků pro řadu odvětví práva, ke kterým jsou připojena i podrobné komentáře. Více viz: Restatements of Law. *Tarlton Law Library* [online]. Last updated 26 January 2010 [cit. 2010-02-04]. Dostupné z: <http://tarlton.law.utexas.edu/vlibrary/outlines/restatements.html>.
K postavení těchto textů v systému pramenů práva viz např. KNAPP, V. *Teorie práva*. 1. vyd. Praha: Nakladatelství C. H. Beck, 1995. s. 138.

36 Přepis textu Restatementu není doslovný, jedná se spíše o převzetí základních myšlenek nežli o překlad.

b) právní vztahy a právní postavení osob v rámci území
c) jednání, které se odehrává mimo území tohoto státu, avšak má nebo mělo mít podstatný účinek na území tohoto státu

2. jednání, zájmy, postavení a právní vztahy příslušníků státu v rámci i mimo jeho území
3. jednání cizinců, které je namířeno proti bezpečnosti státu a/nebo vymezenému okruhu zájmů státu

I když na základě výše uvedených kritérií osoba či právní vztah do jurisdikce státu spadá, neznamená to, že na něj stát bude svou pravomoc aplikovat. Před jejím uplatněním by státní orgán měl celou situaci podrobit testu přiměřenosti zhodnocením těchto faktorů:

- vztah předmětné aktivity k teritoriu hodnotícího státu – tj. v jakém rozsahu se tato aktivita na území státu odehrává a do jaké míry se ho její výsledek dotkne
- právní vztah mezi státem a osobou za tuto aktivitu odpovědnou – občanství, trvalý pobyt, sídlo apod.
- charakter dané aktivity, význam regulace této aktivity pro stát, způsob, jakým je aktivita regulována v zahraničí a způsob, jakým je tento postup státu obecně veřejně přijímán
- existence oprávněných očekávání, která by zásahem státu mohla být poškozena
- důležitost dané regulace v mezinárodním politickém, právním a ekonomickém měřítku
- otázka, do jaké míry je daná činnost státu konzistentní s tradicemi mezinárodního systému
- do jaké míry může mít jiný stát zájem na vlastním regulování dané aktivity
- pravděpodobnost střetu s právně závaznými pravidly jiného státu

I v případě, že je na základě výše uvedených kritérií uplatnění jurisdikce státu nepřiměřené, mohou do ní určité činy přesto spadat. Jedná se o činy, jejichž charakter je natolik závažný, že je jejich stíhání a potrestání prioritou bez ohledu na pravomoci státu či například na splnění předpokladu dvojí trestnosti. Jedná se o trestné činy definované mezinárodním trestním právem[37] – všeobecně uznané jako např. obchodování s otroky, pirátství, válečné zločiny atd. a partikulárně přijímané jako třeba šíření pornografie, terorismus, únos letadla apod. – které vzhledem ke své závažnosti vyžadují striktnější postup ze strany států (více viz „*princip univerzality*“ níže).

Na základě posouzení pravomoci státu pak mohou v zásadě vzniknout tři situace. V prvním případě, všeobecně považovaném za ideální, svědčí test přiměřenosti pouze jednomu státu. V případě kyberkriminality však velmi často dochází k činům, které mají mnohočetné negativní důsledky ve vícero státech. V takovém případě pak dochází ke konfliktu pravomocí. Nejvíce nežádoucím jevem je tzv. *konflikt negativní*, kdy svou pravomoc může uplatnit několik států, avšak ani jeden se pro tuto možnost nerozhodne. Důvody mohou být různé, někdy orgány jednoho státu spoléhají na aktivitu orgánů státu jiného, výkon spravedlnosti bývá také často omezován různými pochybeními ze strany orgánů činných v trestním řízení[38] nebo nedostatky v procesním právu daného státu, které nedokáže dostatečně rychle a pružně reagovat na vývoj tak specifické oblasti jako je kyberprostor. Negativní dopad takovéto situace je nabíledni – pachatel trestného činu zůstane nepotrestán. Třetí situace nastane v případě tzv. *konfliktu pozitivního* – tehdy chce svou pravomoc uplatnit více států najednou.[39] Na řadu pak přichází vzájemný dialog a v ideálním případě je trestný čin stíhán v rámci jedné jurisdikce na základě mezinárodní spolupráce.

> V rámci Evropské Unie byla oficiální diskuze o řešení pozitivního konfliktu pravomocí uvedena *Zelenou knihou o kompetenčních konfliktech a zásadě ne bis in idem v trestním řízení.*[40] Komise zde navrhla třístupňový mechanismus volby příslušnosti, který by umožnil zvolení jednoho tzv. „gestorského“ státu, jehož zájem na stíhání daného trestného činu by byl vzájemnou dohodou určen jako nejsilnější. V prvním stupni by došlo k identifikování a informování zainteresovaných států, což by měl být úkol státu, který jako první zahájil nebo hodlá zahájit trestní stíhání. Informované orgány by pak měly možnost se v dané lhůtě vyjádřit, zdali též mají zájem na stíhání předmětného trestného činu. Ve druhé fázi by pak mělo dojít k diskuzi a volbě nejvhodnějšího členského státu pro stíhání věci. V případě nenalezení shody by pak mohl nastoupit třetí stupeň, ve kterém by za pomoci zprostředkovatele nebo smírčího orgánu zainteresované státy hledaly potřebný konsensus. Toto navrhované řešení přináší řadu otázek, například jak se lze vypořádat s všeobecně uznávanou zásadou zákonnosti, často zakotvenou v pramenech nejvyšší právní síly jednotlivých států, která příslušným státním orgánů přikazuje povinnost bez výjimky stíhat každý trestný čin spadající

37 V rovině teorie je nezbytné rozlišovat pojmy *mezinárodní právo trestní* a *trestní právo mezinárodní*. *Mezinárodní právo trestní* je tvořeno mezinárodními smlouvami, které předepisují smluvním státům povinnost stanovit trestnost určitých činů ve vnitrostátním právu a zároveň také vytvořit předpoklady pro jejich postihování a pro přeshraniční spolupráci se státy ostatními. *Trestní právo mezinárodní* je oproti tomu založeno na vnitrostátních normách trestního práva, které upravují především místní působnost trestních předpisů, popř. i na dalších normách týkajících se postihu trestných činů s mezinárodním prvkem. Více viz:
KRATOCHVÍL, V. – FENYK, J. – KALVODOVÁ et al. *Kurs trestního práva: Trestní právo hmotné, obecná část*. 1. vyd. Praha: Nakladatelství C. H. Beck. 2009. s. 73.

38 Polčák zmiňuje ve svém článku případ, kdy *„český policejní vyšetřovatel dožádal šetření o počítačovém trestném činu v Bulharsku. Tamní orgány nejprve informovaly podezřelého o tom, že je na jeho činnost vedeno vyšetřování a požádaly jej o stanovisko. Podezřelý samozřejmě v reakci na to zastavil své aktivity, zlikvidoval veškeré důkazy, které se nacházely v paměti jeho systému, a vyšetřovatelům pak přišel oznámit, že o žádné trestné činnosti neví.“* Viz: POLČÁK, R. Místní působnost trestního práva. Koliznı́ otázky *internetových právních vztahů* [online] Brno: Masarykova univerzita, [cit. 2010-02-04]. Pozn. č. 2. Dostupné z: <http://is.muni.cz/do/1499/el/estud/praf/js09/kolize/web/pages/trestni-pravo.html>.

39 Jedním z prvních případů pozitivního jurisdikčního konfliktu byl spor, který vznikl v souvislosti s havárií francouzského parníku Lotus roku 1927. Lotus se vinou své posádky srazil v tureckých teritoriálních vodách s plavidlem plujícím pod tureckou vlajkou, při havárii zahynulo několik tureckých námořníků. Spor o to, který stát uplatní svou pravomoc a viníky potrestá, se dostala až před stálý dvůr mezinárodní spravedlnosti v Haagu. Tento soud nakonec přiznal trestněprávní pravomoc Turecku – francouzští námořníci byli sice v době spáchání trestného činu pod francouzskou jurisdikcí (princip teritoriality, viz níže), větší váha však byla přiznána účinku, který trestný čin měl – a ten nastal v Turecku.

40 Zelená kniha o kompetenčních konfliktech a zásadě ne bis in idem v trestním řízení SEK(2005) 1767, KOM(2005) 696 v konečném znění.

do jejich pravomoci. Dalším problémem je, jak se vypořádat s rozdílnými definicemi trestných činů v jednotlivých státech a tudíž co je a co není „to samé" vyjádřené v zásadě *ne bis in idem.*[41]

3.4 Jednotlivé jurisdikční principy

Princip teritoriality

Při posouzení současné právní úpravy lze dojít k závěru, že princip teritoriality je tím nejběžnějším základem pro uplatnění pravomoci státu. Jak již bylo řečeno výše, na základě principu teritoriality se pravomoc státu vztahuje na veškeré osoby resp. činy situované na jeho území. Brenner a Koops[42] však nabízejí podrobnější analýzu, která zohledňuje specifika kyberkriminality a není již striktně založena na fyzické přítomnosti pachatele trestného činu. Dle **místa spáchání činu** bývá jurisdikce založena nejčastěji. Vzhledem k tomu, že elektronická komunikace spočívá v přenosu informace, nelze striktně určit jedno jediné místo, kde se akt přenosu odehrál. Právní řády jednotlivých zemí proto formulují okruh, v rámci kterého uplatňují své pravomoci, široce – jurisdikce může být založena dle místa, kde přenos naplňující skutkovou podstatu trestného činu započal nebo skončil, jinými slovy dle místa, odkud byla informace odeslána a kam byla doručena (taková ustanovení můžeme najít například v právním řádu států Arkansas a Severní Karolina). V různé šíři bývá nastaven i okruh zúčastněných osob a trestnost vývojových stádií trestného činu („spolupachatelství" v právním řádu Německa, „pokus o protiprávní jednání" ve státě Utah). Jak již vyplývá z výše načrtnutého testu přiměřenosti, je nezbytné, aby mezi státem uplatňujícím svou pravomoc a předmětným jednáním existovala tzv. *skutečná (podstatná) spojitost*,[43] čili míra závažnosti, v jaké je předmětný stát danou aktivitou dotčen – dosáhne-li tato míra určité (ryze subjektivní) hranice, může stát uplatnit svou jurisdikci. Z tohoto důvodu je často posuzováno i **místo, kde se projevil efekt trestního jednání**, tj. reálné důsledky tohoto jednání, které se nemusí objevit v místě odeslání ani doručení informace. Klasickým případem je využívání *hostingu* nebo postupný přenos informací prostřednictvím několika často velmi vzdálených serverů. Také například u webových stránek, které jsou dostupné prakticky odkudkoli, *de facto* nelze určit jedno jediné konkrétní místo, kam byla informace doručena, toto je již z povahy veřejného internetu vyloučeno. Doktrína efektu proto umožňuje státu posoudit reálný dopad daného činu na jeho území a na základě tohoto vyvodit příslušné právní důsledky.[44]

Vedle místa spáchání trestného činu může být jurisdikce stanovena i podle **místa, kde se nachází počítač, program nebo data** nějakým způsobem související se spácháním trestného činu. Může tedy jít o umístění napadeného počítače (např. právní úprava státu Connecticut) nebo čistě o „přítomnost" *softwaru*, dat nebo počítače na území daného státu (např. právní řád platný v městském státu Singapore). Zajímavé otázky pak vznikají v souvislosti s využitím satelitů pro trestněprávní aktivity.

Místo, kde se nachází dotčená osoba, může být často totožné s místem spáchání trestného činu, jak bylo popsáno výše. V případě pachatele se nabízí otázka významu státního občanství, která je posuzována i v případě principu personality (viz níže). Vazba na oběť pak umožňuje velmi široké uplatnění státní jurisdikce, obzvláště není-li touto obětí jednotlivec, ale určitá charakteristická skupina (děti v případě dětské pornografie, skupina obyvatel v případě hanobení národa, rasy, etnické nebo jiné skupiny osob). Definování okruhu obětí trestného činu pak úzce souvisí s prokazováním skutečné (podstatné) spojitosti resp. s doktrínou prokázaného efektu na území státu. Jak je vidět, neexistují kritéria pro posuzování pravomoci odděleně. Ve většině případů dochází k jejich vzájemnému zkombinování, které umožňuje účinnější potírání protiprávních aktivit v kyberprostoru.

Geografická teritorialita se doplňuje fikcemi, podle nichž se za území státu považují i další prostory mimo jeho územní katastr. Mezinárodní právo za takové považuje např. paluby plavidel a letadel (zásada registrace) či sídla diplomatických misí jakožto extrateritoriálních území vyňatých z území suverénního státu. Pro osoby činné v rámci těchto misí platí výjimky i v rámci uplatňování principu teritoriality (viz níže), jak je určují mezinárodní dokumenty. [45]

Princip personality

V tomto případě dochází k zohlednění vztahu občan – stát. Ač je výše uvedený princip teritoriality běžně nastaven velmi široce, přece jen dochází čas od času k situacím, kdy se pachatel dokáže vymanit z teritoriální jurisdikce státu. Právě v tomto případě nastupuje jako doplňkový princip personality, který umožňuje státu vztáhnout pravomoc na své občany nezávisle na tom, kde se zrovna fyzicky nacházejí. Jedná se tak o vyjádření vztahu občana vůči státu. V případě uplatnění jurisdikce na základě **občanství pachatele**[46] je teoretickým základem premisa, že *„zájmy a práva chráněná trestním kodexem státu, jehož je pachatel občanem, a je dán proto předpoklad, že tyto zná a je si vědom následků jejich porušení, musí být chráněna kdekoli na světě, bez ohledu, zda jiné státy tak činí nebo nikoliv."*[47] V praxi však většinou nedochází k takto striktnímu širokému výkladu a je vyžadováno splnění podmínky dvojí trestnosti (např. Nizozemí).

Na stejném principu pak funguje uplatnění jurisdikce na základě **občanství oběti** trestného činu.[48] Jde o významný

41 Diskuse k tomuto tématu byla dále rozvinuta v příloze k Zelené knize, která byla vydána pod číslem COM(2005)696 final.
Další komentáře lze nalézt např. ve vyjádření Evropského Institutu University v Leidenu: *Reaction to the Green Paper on conflicts of jurisdiction and the ne bis in idem-principle in criminal proceedings [SEC (2005) 1767].* [online]. Leiden University, European Institute. [cit. 2010-02-04]. Dostupné z: <http://ec.europa.eu/justice_home/news/consulting_public/conflicts_jurisdiction/contributions/university_leiden_en.pdf>.

42 Viz: BRENNER, S. W. – KOOPS, B.-J. Approaches to Cybercrime Jurisdiction. *Journal of High Technology Law*. 2004, roč. 4, č. 1, s. 10 - 29.

43 V angličtině je používán pojem „*substantial link*" nebo také „*substantial connection*".

44 V teorii se v souvislosti s výše popsaným hovoří o tzv. *subjektivní* a *objektivní teritorialitě.* K uplatnění principu *subjektivní teritoriality* dochází v případě, kdy stát stíhá i takové jednání, jehož následky nastanou v jiném státě. Na základě *objektivní teritoriality* je pak pravomoc státu aplikována na jednání, které se sice odehrálo v zahraničí, avšak s následky v daném státě.

45 Jde například o Vídeňskou úmluvu o diplomatických stycích, č. 157/1964 Sb.

46 Tzv. *personalita aktivní*, tj. odvozená od toho, kdo činí něco protiprávného.

47 Viz VRTEK, M. *Evropské trestní právo* [online]. 2008 [cit. 2010-02-04]. 259 s. Disertační diplomová práce. Masarykova universita, Právnická fakulta. Vedoucí práce Vladimír Kratochvíl. Dostupné z: <http://is.muni.cz/th/12443/pravf_d/Souhrnny_text_disertace.pdf>.

48 Tzv. *personalita pasivní*, odvozená od toho, na kom je bezpráví pácháno. Je nezbytné si uvědomit, že personalita aktivní resp. pasivní je vyjádřením vztahu „osoba – území", proto je jako kritérium používána při určování místní působnosti práva, ne působnosti osobní.

doplňkový instrument nejen při ochraně jednotlivce, ale i v případě nutnosti ochrany napadené skupiny obyvatel. Jsou-li v této skupině reprezentováni i občané dotčeného státu, může tento právě díky pasivní personalitě svou pravomoc nad pachatelem uplatnit. Zajímavý je například i způsob, jakým je „oběť" chápána právním řádem Spojených států amerických. „Obětí" dle amerického práva totiž nemusí být pouze fyzická či právnická osoba, v určitých situacích jí může být i stát sám resp. jeho reprezentativní složka. Pravomoci orgánů USA činných v trestním řízení jsou proto podřízeny i například neoprávněné vstupy do systému státních úřadů apod. V tomto pojetí se již projevuje další princip – ochrany, o kterém bude pojednáno v následujícím odstavci.

Pasivní/aktivní personalitu jakožto základ pro určení místní působnosti pak nelze zaměňovat s personalitou založenou na osobním statusu a to bez ohledu na místo spáchání trestného činu. Tato personalita je pak určující pro stanovení osobní působnosti práva státu. Personalita v tomto významu je tak například ve spojení s aktivní personalitou v rámci místní působnosti základem pro formulování extradičních zásad, tedy zdali daný stát vydává resp. nevydává své občany k trestnímu stíhání či k výkonu trestu. Osobní působnost lze pozitivně definovat tak, že zahrnuje množinu osob, jež spadají na základě určitých hledisek pod právní režim daný právem státu. Na základě osobního statusu je pak stanoven okruh hmotněprávních exempcí (beztrestnost, trvalá) a procesněprávních exempcí (nestíhatelnost, přechodná) u určitých osob.

Princip ochrany a univerzality

Princip ochrany přichází ke slovu v závažných případech, kdy není možné pachatele stíhat na základě principu teritoriality a personality, protože se pachatel dopustil svého jednání mimo území dotčeného státu a zároveň není ani jeho občanem. Pochopitelně nelze princip ochrany uplatnit kdykoli. Je to možné, pouze pokud jsou protiprávní aktivitou poškozovány důležité zájmy státu a jeho základní funkce. V poslední době se četnost protiprávních zásahů do systémů státní správy zvyšuje a význam principu ochrany stoupá. Pojem „důležité zájmy státu" lze přitom použít ve značné šíři. Například dodatek s názvem *USA Patriot Act* uvedl do amerického práva pojem „chráněného počítače". Tento pojem je dle tohoto zákona zahrnuje nejen počítače (sloužící k plnění funkcí mezinárodního obchodu a komunikace), které jsou situovány na území USA, ale i počítače mimo toto území, pokud plní funkci se stěžejním významem pro Spojené státy americké. Toto na první pohled odvážné rozšíření pravomocí je ve skutečnosti účinným propojením s doktrínou prokázaného efektu, jak byla již popsána výše. Podpisem *USA Patriot Act* v roce 2001 se tak USA pokusily rozšířit svou jurisdikci, na jejímž základě by bylo možné efektivněji bojovat proti terorismu resp. jeho kybernetické odnoži.

Se zmínkou o všeobecně odsuzované trestné činnosti, kterou terorismus bezpochyby je, se dostáváme k poslednímu jurisdikčnímu principu a tím je princip univerzality. Tento princip stojí jako nadstavba nad jednotlivými principy chránícími partikulární zájmy jednotlivých států a pokrývá trestné činy, které jsou vzhledem ke svému charakteru a závažnosti odmítány mezinárodním společenstvím na základě všeobecného konsenzu. Jedná se o trestné činy, které již byly zmíněny v kapitole věnované testu přiměřenosti. Vzhledem k zaměření tohoto článku však autorka považuje za nezbytné pozastavit se především nad těmi univerzálně stíhatelnými trestnými činy, které jsou páchány prostřednictvím informačních technologií. Jako jediný příklad uplatnění principu univerzality na kyberzločin uvádí Brenner a Koops[49] právní úpravu Belgie a Německa – zde je na základě univerzální jurisdikce stíhatelné šíření dětské pornografie. Zatímco u „klasických pozemských" trestných činů již nalezlo světové společenství konsensus (např. všeobecné odsouzení mořského pirátství), na poli kyberkriminality taková shoda prozatím chybí. Promítá se zde tak nejen různé nastavení právních systémů, ale i disharmonie v chápání významu a závažnosti trestných činů páchaných s pomocí informačních technologií. Rostoucí význam dějů odehrávajících se ve virtuálním světě však nepochybně donutí státy v nejbližší době hledat v postupu proti závažným kyberzločinům jednotu.

4 Relevantní právní úprava

Pro rozdělení dostupných pramenů práva v oblasti přeshraniční trestné činnosti v kyberprostoru se autorka rozhodla pro klasické členění na právo mezinárodní, právo ES/EU[50] a právo národní, především s ohledem na jeho přehlednost. Přesto je však nezbytné podotknout, že si zároveň uvědomuje jeho nedostatky, které právě v této oblasti získávají nový rozměr. Podle obecné teorie totiž pod pojem „právo mezinárodní" fakticky spadá i právo EU, protože Evropská unie je mezinárodní teritoriální organizací. V praxi však bývá právo EU pro svou značnou specifičnost od „čistého" mezinárodního práva oddělováno, autorka se tedy rozhodla tento všeobecně užívaný postup převzít. Pojem „mezinárodní dokumenty" proto zahrnuje mezinárodní dokumenty vyjma dokumentů ES/EU, kterému je věnována vlastní podkapitola.

Druhým problémem je fakt, že kromě obecného pojmového propojení existuje mezi těmito oblastmi velmi úzký vztah i co se týče náplně, v oblasti trestního práva a justiční spolupráce v trestních věcech obzvláště. Trestní právo v rámci EU totiž dlouhou dobu patřilo mezi exkluzivní prerogativy státu. Pevný základ pro justiční spolupráci a celkový rozvoj evropského trestního práva tak tvořily především dokumenty vytvořené v rámci aktivit Rady Evropy, tedy mezinárodní organizace od EU odlišné. Od počátku devadesátých let 20. století dochází k postupné europeizaci trestního práva, nejprve vytvořením třetího pilíře zahrnujícího i oblast justiční spolupráce v trestních věcech na základě Maastrichtské smlouvy, a dále pak na základě závěrů jednání v Tampere z roku 1999, kdy Evropská unie, posílená novými pravomocemi přinesenými Amsterodamskou smlouvou, přijala svůj první pětiletý plán v oblasti spravedlnosti a vnitřních věcí. Nemluvě o faktu, že nová Smlouva o fungování Evropské Unie (tzv. Lisabonská smlouva, v účinnosti od 1. prosince 2009) přináší další zásadní změny v šíři a konkretizaci kompetencí v rámci EU. V každém případě nové právotvorné postupy mají stále

49 Viz BRENNER, S. W. – KOOPS, B.-J. Approaches to Cybercrime Jurisdiction. *Journal of High Technology Law.* 2004, roč. 4, č. 1, s. 28.

50 Tyto zkratky budou nadále používány pro pojmy Evropská společenství (ES) a Evropská unie (EU). Se zavedením Lisabonské smlouvy ztrácí rozdělování na právo ES a právo EU smysl, jedinou existující mezinárodní organizací je Evropská unie. Jelikož však v podstatě všechny zmíněné právní akty vznikly před oním klíčovým datem 1. prosince 2009, rozhodla se autorka zavedené rozlišování na některých místech pro názornost ponechat.

základ v principech obsažených v dokumentech Rady Evropy, obsahové oddělení mezinárodního práva (jak je vymezeno v předchozím odstavci) a práva EU v trestněprávní oblasti proto není úplně možné.[51]

Na základě výše naznačených aktivit tak vznikla předlouhá řada dokumentů, které upravují fungování systému mezinárodního resp. evropského trestního práva po stránce hmotné i procesní. Řada z nich výslovně nepočítá s pojmem a specifiky kyberprostoru, to jim však neubírá na účinnosti v případě, že se informační prvek v dané aktivitě nějak projeví (viz obecný výklad o kyberkriminalitě, Kapitola 1). Autorka se v tomto článku bude zabývat pouze těmi dokumeny, které se přímo zaobírají právem informačních technologií a jejichž význam je pro danou oblast stěžejní.

4.1 Mezinárodní dokumenty

Úmluva Rady Evropy č. 185 o kyberkriminalitě

Rada Evropy se začala věnovat problematice informační kriminality již v druhé polovině osmdesátých let minulého století. Na prvotní dokument Doporučení Výboru ministrů č. 9 z 13. září roku 1989 (angl. *Recommendation No. R (89) 9 On Computer-related Crime*) o trestné činnosti vztahující se k počítačům navázalo Doporučení Výboru ministrů č. 13 z 11. září roku 1995 (angl. *Recommendation No. R (95) 13 Concerning Problems Of Criminal Procedural Law Connected With Information Technology*), které řeší otázky procesněprávní. Na svém 109. zasedání dne 8. listopadu 2001 ve Štrasburku přijal Výbor ministrů Rady Evropy text Úmluvy o kyberkriminalitě (dále jen „Úmluva"). Jednalo se první dohodu mezinárodního charakteru, která se týkala trestné činnosti páchané prostřednictvím informačních technologií. Úmluva byla následně otevřena k podpisu dne 23. listopadu 2001 v Budapešti s tím, že den jejího vstupu v platnost byl stanoven na datum 1. července 2004. Ke dni 4. srpna 2010 byla Úmluva podepsána 46 státy, z nichž ji ratifikovalo pouhých třicet. Česká republika Úmluvu doposud též neratifikovala, i když její podpis se datuje již ke dni 9. února 2005.[52]

S vědomím nezbytnosti nadnárodního postupu při potírání kyberkriminality vznikl text Úmluvy, jehož cílem bylo sjednocení přístupu signatářů k postihování trestných činů páchaných v kyberprostoru, a to prostřednictvím přijetí harmonizované legislativy na národní úrovni a posílení vzájemné spolupráce mezi jednotlivými státy. Po přijetí tohoto textu by již tedy nemělo docházet k situaci, kdy by některý z definovaných kyberzločinů postrádal v některém členském státě trestnost nebo by zdejší orgány činné v trestním řízení nedisponovaly procesními oprávněními nutnými k tomu, aby mohly čin vyšetřit a prokázat. Dodrží-li tedy státy své závazky, měl by zde odpadnout problém existence tzv. bezpečných přístavů (angl. „*safe harbors*") pro pachatele internetové trestné činnosti. [53] Zároveň by tak mělo dojít ke značnému ztížení účelového výběru států s „děravou" právní úpravou ze strany osob s nekalými úmysly (angl. „*territory shopping*").

Úmluvu tvoří kromě preambule čtyři kapitoly dále rozdělené do 48 článků. Kapitola první (*Use of Terms*) poskytuje definice některých technických pojmů, se kterými Úmluva nadále operuje. Druhá kapitola obsahující opatření, která mají být přijata na národní úrovni (*Measures to be taken at the national level*), zahrnuje hmotně a procesně právní instituty. Jejich zavedením do právních řádů jednotlivých signatářských států má být dosaženo sjednocení znaků kyberzločinů a procesních postupů, umožňujících efektivní kooperaci při jejich potírání. Úmluva tak zavádí čtyři kategorie kybernetických trestných činů:

1. Do skupiny **trestných činů proti utajení, celistvosti a dostupnosti počítačových dat a systémů** (*Offences against the confidentiality, integrity and availability of computer data and systems*, články 2 – 6 Úmluvy) patří *nedovolené získání přístupu k systému, nedovolené narušování komunikace, poškozování dat, narušování běhu informačních systémů, zneužití technických prostředků k výše uvedeným činům (včetně jejich držení).*
2. *Padělání za užití počítače a počítačový podvod* jsou souhrnně označeny jako **trestné činy související s počítači** (*Computer-related offence,* články 7 a 8 Úmluvy).
3. Do kategorie **trestných činů související s obsahem** (*Content-related offences*, článek 9 Úmluvy) je zařazena *výroba, distribuce, získávání a držení dětské pornografie na datových nosičích.*
4. **Trestné činy související s porušováním autorských práv a práv souvisejících** *(Offences related to infringements of copyright and related rights)* jsou upraveny v článku 10 Úmluvy.

Signatářské státy nemusí tento katalog přijmout v plné míře, v mnohých případech mají možnost uplatnit výhradu a nestíhat určité typy uvedených jednání. Obecné instituty trestního práva hmotného, jejichž úpravu je nezbytné v souvislosti s kyberzločinem sjednotit, obsahují články 11 – 13 Úmluvy – navádění a napomáhání trestnému činu, odpovědnost právnických osob a obecné ustanovení týkající se sankcí, které mají být dostatečně efektivní, úměrné a odrazující. Vzhledem k řešené problematice je významný čl. 12 Úmluvy, který požaduje zavedení odpovědnosti právnických osob za kybernetické trestné činy (*Corporate liability*). Odst. 3 tohoto článku dává volnost ve výběru typu odpovědnosti podle právních principů uznávaných v signatářským státem – ta tedy může být buď civilně-, správně- nebo trestněprávní. Právnická osoba tak může být odpovědná za některý z výše uvedených trestných činů v případě, že v její prospěch jedná jakákoli fyzická osoba, buďto individuálně nebo jako člen orgánu této právnické osoby ve vedoucí pozici, na základě oprávnění tuto právnickou osobu reprezenzovat, přijímat jejím jménem rozhodnutí nebo provádět v jejím rámci kontrolní činnost. Odpovědnost právnické osoby má nastat též v případě, že je spáchání uvedeného trestného činu umožněno na základě nedostatků v dozoru či kontrole prováděných výše uvedenou fyzickou osobou, přičemž v žádném z uvedených případů není

51 Podrobnější informace k procesu europeizace resp. komunitarizace trestního práva jsou dostupné např. v:
FENYK, J. – SVÁK, J. – KLÍMA, K. *Europeizace trestního práva*. 1. vyd. Bratislava: Bratislavská vysoká škola práva, 2008. 229 s.

52 Aktualizovaný seznam všech států, které podepsaly resp. ratifikovaly Úmluvu o kyberkriminalitě naleznete na stránkách Rady Evropy [online]. Council of Europe, Status as of: 2010-08-04 [cit. 2010-08-04]. Dostupné z: <http://conventions.coe.int/treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG>.

53 Viz POLČÁK, R. Místní působnost trestního práva. *Kolizní otázky internetových právních vztahů* [online]. Brno: Masarykova univerzita, [cit. 2010-02-08]. Dostupné z: <http://is.muni.cz/do/1499/el/estud/praf/js09/kolize/web/pages/trestni-pravo.html>.

odpovědnost právnické osoby vázána na odpovědnost osoby fyzické za tuto právnickou osobu jednající.

Procesněprávní úprava obsažená v kapitole druhé Úmluvy (*Procedural law*) ukládá státům přijmout taková opatření, která jim umožní efektivně postupovat v trestním řízení. Tato opatření se mají vztahovat jednak na trestné činy uvedené v článcích 2 – 11, dále na jiné trestné činy spáchané prostřednictvím počítačového systému a na shromažďování důkazů v elektronické formě. Je zároveň nezbytné zajistit, aby veškerý postup v trestním řízení zůstal v souladu s mezinárodněprávními závazky jednotlivých států, které se týkají ochrany lidských práv a práv občanských a politických.[54] Články 16 – 21 řeší otázky související se zajišťováním, uchováváním a sdílením uchovaných dat. Signatářské státy se tak zavazují vytvořit účinný systém, který jejich pověřeným autoritám umožní rychle a efektivně získat přístup k potřebným informacím. Důležité je, že na základě příkazu pověřené autority (*Production order,* čl. 18) jsou fyzické osoby a poskytovatelé informačních služeb v rámci teritoria státu povinni spolupracovat a předávat požadované informace.

Článek 22 Úmluvy je věnován úpravě jurisdikce. Dochází zde ke kombinaci principu teritoriality a doplňkových principů personality a registrace (jak již byly teoreticky popsány v Kapitole 3. tohoto článku), přičemž některá ustanovení mohou jednotlivé státy aplikovat odlišně na základě učiněné výhrady. Strany se též zavazují přijmout legislativu a další opatření nutná k založení jurisdikce nad činy uvedenými v článku 24 odstavec 1 Úmluvy[55] v případech, kdy se pachatel nachází na jejich území a není na základě žádosti rozhodnuto o jeho vydání ke stíhání jiné Straně z důvodu jeho státní příslušnosti. Zároveň Úmluva nevylučuje v žádném případě stanovení jurisdikce signatářských států dle jejich národního práva. Pro případ, kdy více států nárokuje jurisdikci, zavádí Úmluva hledání řešení prostřednictvím vzájemných konzultací.

Jak je vidět na výše uvedeném, neobsahuje Úmluva ve skutečnosti jednoznačnou delimitaci pravomocí ani pravidla, která by umožnila jejich efektivní prosazení. Vázanost na princip teritoriality resp. personality a opomenutí doktríny efektu trestné činnosti činí tuto úpravu prakticky poněkud „bezzubou" v porovnání s rétorikou zbytku Úmluvy, ze které čiší uvědomění si závažnosti hrozby kyberkriminality a odhodlání se s ní společným a organizovaným postupem vypořádat. Přitom otázka určení jurisdikce je jednou ze stěžejních při stíhání trestných činů, bez jejího vyřešení prakticky nelze celý proces ani zahájit. Úmluva bere ohled na limity diskrece jednotlivých států a tím ztrácí značnou část své efektivity v této oblasti. [56]

Kapitola třetí (*International co-operation*) zavádí ve svých ustanoveních pravidla pro mezinárodní spolupráci, vydávání stíhaných osob a vzájemnou přeshraniční pomoc při získávání důkazů a potřebných informací. Úmluva tak má za cíl doplňovat vícestranná ujednání týkající se mezinárodní justiční spolupráce v trestních věcech, kterými jsou například Evropská úmluva o vydávání z 13. prosince 1957 (ETS No. 24), Evropská úmluva o vzájemné pomoci ve věcech trestních z 20. dubna 1959 (ETS No. 30) a dodatkový protokol k této úmluvě ze dne 17. března 1978 (ETS No. 99).

Dodatkový protokol č. 189 k Úmluvě o kyberkriminalitě, o kriminalizaci činů rasistické a xenofobní povahy

Čtrnáct měsíců po Úmluvě o kyberkriminalitě byl ve Štrasburku dne 28. ledna 2003 otevřen k podpisu dodatkový protokol o kriminalizaci činů rasistické a xenofobní povahy. Tento protokol tak doplňuje skupinu trestných činů souvisejících s obsahem. Nabízí se otázka, proč nebyla tato skutková podstata zahrnuta přímo do Úmluvy již v roce 2001. Důvody byly především politické – cílem Rady Evropy bylo pro novou Úmluvu získat co největší podporu napříč geografickým spektrem. Fakticky nejvýznamnějším hráčem, jehož podpora se stala pro prosazení nové úpravy naprosto nezbytnou, byly USA, přičemž, jak již bylo zmíněno v první kapitole tohoto článku, právní úprava tzv. „*hate speech*" v Prvním dodatku Ústavy Spojených států amerických prakticky znemožňuje stíhání rasistických projevů a projevů xenofobní povahy. Vznikla tak oprávněná obava, že Spojené státy nepodpoří Úmluvu kvůli jejímu nesouladu s federálním ústavním pořádkem v tomto bodu a tím dojde k reálnému ohrožení celého projektu. Pro zakotvení kriminalizace činů rasistické a xenofobní povahy tak byla zvolena forma opčního protokolu, který nevyžaduje ratifikaci všech vysokých smluvních stran.

Ve čtyřech kapitolách tak dodatkový protokol přináší definici „rasistického a xenofobního materiálu", tedy jakéhokoli písemného materiálu, jakéhokoli zobrazení nebo jiného znázornění myšlenek nebo teorií, které obhajují, propagují nebo podněcují nenávist, diskriminaci nebo násilí proti jednotlivci nebo proti skupině osob, založenou na rasové příslušnosti, barvě pleti, národním nebo etnickém původu či náboženství. Protokol tak požaduje kriminalizaci šíření těchto materiálů, rasisticky a xenofobně motivovaného vyhrožování a útoků a popírání, snižování, schvalování či ospravedlňování genocidy nebo zločinů proti lidskosti. Podle kapitoly třetí mohou být na tento Protokol aplikována *mutatis mutandis* vybraná ustanovení Úmluvy o kyberkriminalitě.

4.2 Dokumenty ES/EU

Do dne 1. prosince 2009 byly oblasti působnosti Evropské Unie vymezeny především v Hlavě VI. Smlouvy o Evropské unii (dále jen „SEU"), především v čl. 29 – 34 SEU. Na základě vymezení společných cílů a jim odpovídajících základních kompetencí dával čl. 34 SEU Radě[57] možnost přijímat opatření v podobě společných postojů vymezujících postoj Unie k určité otázce, rámcových rozhodnutí, která sloužila ke

54 Jde například o závazky vyplývající z dokumentů:
Mezinárodní pakt o občanských a politických právech. [online]. [cit. 2010-02-08]. Dostupné z: <http://www.osn.cz/dokumenty-osn/soubory/mezinar.pakt-obc.a.polit.prava.pdf>.
Úmluva o ochraně lidských práv a základních svobod. [online]. [cit. 2010-02-08]. Dostupné z: <http://www.echr.coe.int/NR/rdonlyres/82E3CE7F-5D3D-46EB-8C13-4F-3262F9E20B/0/CzechTch%C3%A8que.pdf>.

55 Jedná se o trestné činy podle čl. 2 – 11, pokud je čin uznán v obou dotčených státech za trestný čin postižitelný trestem odnětí svobody s horní sazbou alespoň jeden rok nebo trestem přísnějším. Výše trestní sazby může být odlišně upravena vzájemnou dohodou.

56 Nutno však podotknout, že autorka nepouští ze zřetele citlivost otázek souvisejících se státní suverenitou, jak je popsala již v předchozích kapitolách, a s tím související komplikovanost hledání odpovídající právní úpravy.

57 Jedná se o Radu Evropské unie, jeden z hlavních rozhodovacích orgánů EU. Zastupuje členské státy a jejích schůzek se účastní jeden ministr z každé vnitrostátní vlády EU. Jednotliví ministři se střídají podle toho, do kterého resortu spadá předmět jednání. Více informací naleznete zde: *Orgány a ostatní instituce Evropské unie: Rada Evropské unie* [online]. Europa[cit. 2010-03-30]. Dostupné z: <http://europa.eu/institutions/index_cs.htm>.

sbližování práva členských států, a rozhodnutí týkajících se čehokoliv jiného kromě sbližování práva.

Strukturovanější a specifičtější výčet pravomocí přinesla až Lisabonská smlouva, na jejímž základě byly vytvořeny dva současné stěžejní dokumenty – Smlouva o fungování Evropské unie (dále jen „SFEU") a konsolidovaná Smlouva o Evropské Unii (zkráceně „SEU"). Zaniklo tak původní rozdělení agendy do tří pilířů a Evropská unie v pozici mezinárodní organizace využívá pro výkon svých pravomocí „tradiční" právní nástroje, jak je vymezuje čl. 288 SFEU.[58] Specifikace a prohloubení pravomocí EU se odráží ve strukturovaném rozdělení na kompetence v oblasti justiční spolupráce v trestních věcech v užším slova smyslu (čl. 82 odst. 1 SFEU) a na kompetence k aproximaci právních předpisů v oblasti trestního práva procesního (čl. 82 odst. 2 SFEU) a trestního práva hmotného (čl. 83 odst. 1 a 2 SFEU).[59]

Rozhodnutí Rady 92/242/EHS ze dne 31. března 1992, o bezpečnosti informačních systémů

Rapidní rozšíření elektronického zpracování informací a rostoucí význam globálních komunikací v hospodářské a sociální sféře na počátku devadesátých let přiměly orgány ES zaujmout odpovědný postoj vůči zabezpečení informačních systému a zajištění spolupráce na mezinárodní úrovni. Toto rozhodnutí je jedním z prvních, které otevřeně uznává zranitelnost informační společnosti a tudíž i nezbytnost společného postupu při její ochraně. Rada jím stanovila globální strategii pro zajištění bezpečnosti informačních systémů v podobě akčního plánu a za tímto účelem rozhodla o vytvoření pověřené skupiny odborníků, která do budoucna měla sloužit jako konzultační orgán Komise[60] při řešení úkolů spojených se zajišťováním bezpečnosti v informační společnosti.

Dvouletý akční plán zahrnoval přípravné práce na následující témata:

I. vývoj strategického rámce pro bezpečnost informačních systémů

II. zjištění potřeb uživatelů a poskytovatelů služeb v oblasti bezpečnosti informačních systémů

III. vypracování řešení pro některé krátkodobé a střednědobé potřeby uživatelů, dodavatelů a poskytovatelů služeb

IV. vypracování specifikací, normalizace, hodnocení a osvědčování ve vztahu k bezpečnosti informačních systémů

V. technologický a funkční vývoj v oblasti bezpečnosti informačních systémů

VI. zavedení bezpečnosti informačních systémů

Vytvoření této strategie mělo za cíl nalezení rovnováhy mezi hospodářskými, politickými a sociálními zájmy společnosti a vytvoření rámce pro efektivní mezinárodní spolupráci a harmonizaci postupu jednotlivých států. Pro další vývoj bylo významné také uznání role jednotlivých poskytovatelů informačních služeb v procesu zabezpečování informačních systémů. Text tohoto rozhodnutí je na první pohled velmi obecný a budí spíše dojem jakéhosi hrubého nástinu vize nežli stanovení konkrétního postupu. Jeho význam je tak nezbytné spatřovat v samotné verbalizaci narůstajícího nebezpečí a ve vyjádření jasného postoje společenství vůči nově vznikajícímu fenoménu. Kyberkriminalita již nebyla pouhou šedou nedefinovanou zónou potenciální hrozby, byla uznána za vážný rizikový fenomén, kterému je nutno organizovaně a systematicky čelit.

Rozhodnutí Rady 2000/375/SVV ze dne 29. května 2000, o boji proti dětské pornografii na internetu

Toto rozhodnutí navazuje na dlouhou řadu dokumentů, které se zabývají opatřeními k ochraně dětí před vykořisťováním a sexuálním zneužíváním. Nepřináší konkrétní opatření pro boj s šířením dětské pornografie, má spíše deklaratorní a apelační charakter, jehož cílem je zdůraznit fakt, že internet je vhodným prostředím pro nárůst této nebezpečné trestné činnosti a že státy musí zaujmout odpovídající opatření pro její potlačení. Rada tak členské státy vyzývá k systematické spolupráci při vyšetřování, k vytvoření kontaktních center a výměně informací, která tak orgánům činným v trestním řízení zajistí rychlý a efektivní postup.

Důležitý je též apel na zahájení dialogu mezi státy a průmyslovým odvětvím pro vzájemnou výměnu zkušeností. Cílem této spolupráce by mělo být vyvíjení účinných technických prostředků a postupů pro zamezení a zjišťování šíření dětského pornografického materiálu. Rada tak implicitně uznává fakt, že bez podpory soukromého sektoru nelze v oblasti kyberprostoru účinně prosadit zájmy státu, a vyzývá k jeho respektování jako partnera při autoritativní regulaci informační společnosti.

Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000, o některých aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („směrnice o elektronickém obchodu")

Tato směrnice představuje v podstatě jediný dokument, který se zčásti zabývá otázkami odpovědnosti poskytovatelů služeb informační společnosti za protiprávní jednání spáchaná v souvislosti s výkonem jejich činnosti. Cílem tohoto dokumentu byla především harmonizace vnitřního trhu v rámci volného pohybu služeb, ustanovení oddílu 4 kapitoly II. týkající se odpovědnosti ISP však mají veliký význam i pro oblast trestního práva a pro potírání nezákonného obsahu na internetu. Celá tato konstrukce je založena na faktu, že není možné efektivně prosazovat zájmy společnosti a státu v kyberprostoru bez podpory a spolupráce se soukromým sektorem. Závažnost situace již zároveň neumožňuje spoléhat pouze na opatření přijatá ze strany ISP dobrovolně na základě

58 Jde konkrétně o nařízení, směrnice, rozhodnutí, doporučení a stanoviska. Někdy bývají do tohoto výčtu zahrnovány i specifické akty *sui genesis*, které jsou právně závazné, i když nenaplňují charakteristické rysy „základních" právních nástrojů, jak je uvádí čl. 288 SFEU.

59 Blíže viz BŘÍZA, P. – ŠVARC, M. Komunitarizace trestního práva v Lisabonské smlouvě a její (případná) reflexe v právním řádu České republiky. *Trestněprávní revue.* 2009, roč. 8, č. 6, s. 161 – 170.

60 Jedná se o Evropskou komisi, zákonodárný a výkonný orgán Evropské unie. Komise je složena ze zástupců jednotlivých členských států, sestavuje návrhy nových evropských právních předpisů a odpovídá za provádění rozhodnutí Evropského parlamentu a Rady Evropské unie. Více viz: *Orgány a ostatní instituce Evropské unie: Evropská komise* [online]. Europa [cit. 2010-03-30]. Dostupné z: <http://europa.eu/institutions/index_cs.htm>.

právně nezávazných kodexů chování, bylo proto nezbytné přijmout odpovědnostní pravidla ve formě právně závazného aktu – směrnice.

Pro určení odpovědnosti ISP jsou stěžejní články 12 – 15 směrnice. V ustanovení článku 12 nalezneme vysvětlení pojmu, který je úhelným kamenem celé odpovědnostní konstrukce obsažené v této směrnici – je jím pojem „prostý přenos" (často používán v anglickém znění „*mere conduit*"). Podle tohoto článku není ISP v případě poskytování služby spočívající v přenosu informací nebo ve zprostředkování přístupu ke komunikační síti odpovědný za přenášené informace, pokud není původcem přenosu, nevolí příjemce přenášené informace a z hlediska obsahového předmětnou informaci nevybírá ani nemění. Ustanovení článku 13 pak zbavuje ISP odpovědnosti i za tzv. „*caching*", čili za dočasné přechodné ukládání informací do vyrovnávací paměti, které slouží pouze pro co možná nejúčinnější následný přenos informace na žádost jiných příjemců služby. ISP přitom nesmí předmětnou informaci změnit a musí vyhovět podmínkám přístupu k informaci a dodržovat obecně uznávané postupy pro aktualizaci informací a získávání údajů o užívání těchto informací. Dále má povinnost informaci odstranit či zablokovat její přístupnost, byla-li na výchozím místě přenosu odstraněna, nebo byl-li k ní znemožněn přístup resp. bylo-li toto zamezení přikázáno soudem či jiným správním orgánem. Státní orgány mohou poskytovateli též uložit, aby ukončil porušování práv nebo mu předešel.

V případě služby spočívající v ukládání informací na žádost příjemce není poskytovatel dle článku 14 odpovědný, pokud si nebyl vědom protiprávnosti informace resp. činnosti nebo pokud učinil opatření s cílem tyto informace odstranit ihned, jak se o jejich protiprávnosti dozvěděl. V souvislosti s tímto ustanovením pak vzniká otázka, zda jsou ISP povinni kontrolovat soulad přenášených resp. ukládaných informací se zákonem. Odpověď nabízí ihned následující článek č. 15, který deklaruje neexistenci obecné povinnosti dohledu za strany poskytovatelů služeb. Zároveň však umožňuje členským státům autoritativně nařídit poskytovatelům povinnost informovat příslušné orgány veřejné moci, pokud přijdou do styku se závadným materiálem, a poskytnout také informace, na jejichž základě lze zjistit totožnost příjemců jejich služeb.

Výše popsaná ustanovení hrají velmi důležitou roli v procesu potírání trestné činnosti na internetu. V praxi totiž dochází k situacím, kdy je předmětná aktivita zjištěna a definována jako protiprávní, chybí však právní nástroj, kterým by bylo možno autoritativně nařídit její zastavení, nemluvě o samotné identifikaci odpovědné osoby. O tomto problému bude ještě podrobně pojednáno v následujících kapitolách.

Rámcové rozhodnutí Rady 2001/413/SVV ze dne 28. května 2001, o potírání podvodů a padělání bezhotovostních platebních prostředků

V tomto rámcovém rozhodnutí se již jasně projevuje pozvolné „drobení" třetího pilíře a tendence ke komunitarizaci trestního práva, jak ji odstartovala Amsterodamská smlouva. Rada vyslovila závěr, že mezinárodní rozměr trestných činů v rámci bezhotovostního platebního styku znemožňuje jejich efektivní potírání na národní úrovni, a proto je nezbytné vyvinout společnou nadstátní aktivitu. Navázala tak na řadu dokumentů s touto tématikou, která byla vydávána na konci devadesátých let 20. století.[61] Toto rámcové rozhodnutí již nenese jen vágní deklarace, zavádí povinnost přijmout opatření nezbytná ke kriminalizaci krádeže, podvodu a neoprávněného nakládání s elektronickým platebním nástrojem prostřednictvím manipulace s počítačovými daty nebo zásahu do počítačového programu. Trestným má být i úmyslné nakládání s prostředky, které takovou nežádoucí činnost umožňují, tj. např. výroba či šíření *softwaru* apod., přičemž udělované tresty mají být přiměřené a odrazující.

I toto rozhodnutí zavazuje v článku 7 členské státy k zavedení odpovědnosti právnických osob, přičemž konstrukce tohoto ustanovení je v zásadě totožná s ustanovením článku 12 Úmluvy o kyberkriminalitě, jak bylo zmíněno již výše. Novum přináší až text navazujícího článku číslo 8, které kromě pokut trestního či správního charakteru přináší členským státům i návrh jiných sankcí, konkrétně vyloučení ze způsobilosti k veřejným výhodám nebo pomoci, dočasný nebo trvalý zákaz výkonu obchodní činnosti, ustavení soudního dohledu nebo soudní příkaz k likvidaci.

Jurisdikční otázky řeší následující článek číslo 9, který členské státy vybízí k založení soudní pravomoci na základě zásady teritoriality a zásady aktivní a pasivní personality, přičemž umožňuje i modifikaci uplatňování těchto principů ve spojení s extradiční výhradou učiněnou vůči ustanovením článku 10 tohoto rozhodnutí.

Rámcové rozhodnutí Rady 2004/68/SVV ze dne 22. prosince 2003, o boji proti pohlavnímu vykořisťování dětí a dětské pornografii

Oproti deklaratornímu dokumentu z května roku 2000, který o aktivitě států hovořil spíše v obecné rovině, přináší již toto rámcové rozhodnutí členským státům povinnost přijmout opatření k zajištění trestnosti konkrétně daných činů – jednak trestných činů týkajících se pohlavního vykořisťování dětí (donucování dítěte k prostituci nebo k účasti na pornografických dílech nebo kořistění prostřednictvím dítěte nebo jiné vykořisťování dítěte k takovým účelům, najímání dítěte k prostituci nebo k účasti na pornografických dílech, provádění sexuálních praktik s dítětem) a dále trestných činů týkajících se dětské pornografie (výroba, prodej, rozšiřování nebo další předávání dětské pornografie, její nabízení a zpřístupňování stejně jako její pořizování a držení). Rámcové rozhodnutí vyzdvihuje nebezpečí páchání této činnosti s využitím nových informačních technologií a internetu a vyzývá členské státy k zohlednění tohoto fenoménu v národních právních úpravách. Závažnost situace naznačuje i fakt, že se Rada neomezuje pouze na doporučení „přiměřených a odstrašujících trestů", ale vyjadřuje již požadavek stanovení trestů odnětí svobody v konkrétně stanoveném rozmezí.

Odpovědnostní a sankční mechanismus ve vztahu k právnickým osobám je v zásadě stejný jako u předchozího dokumentu. K trestům však ještě kromě zbavení oprávnění pobírat veřejné výhody nebo podpory, dočasnému nebo trvalému zákazu provozování obchodní činnosti, uložení soudního dohledu a zrušení rozhodnutím soudu přibylo ještě jedno opatření – dočasné nebo trvalé uzavření provozoven, jichž bylo užito ke spáchání protiprávního jednání. Tato

61 Jednalo se například o akci vytvářející Evropskou soudní síť, rozšiřování činnosti Europolu nebo kriminalizaci některých nežádoucích aktivit v rámci nakládání s platebními prostředky.

sankce získává nový rozměr právě ve vztahu k trestné činnosti páchané prostřednictvím informačních technologií. Postih je vázán na místo spáchání trestného činu, přičemž dle tohoto rámcového rozhodnutí (článek 8 odst. 5 ve vazbě na založení pravomoci) již tímto místem není pouze místo, kde se závadný počítačový systém nachází, ale i místo, odkud bylo do tohoto systému vstoupeno.

Rámcové rozhodnutí Rady 2005/222/SVV ze dne 24. února 2005, o útocích proti informačním systémům

Dle úvodních slov dokumentu je *„cílem tohoto rámcového rozhodnutí … zlepšit spolupráci mezi justičními a jinými příslušnými orgány, včetně policie a dalších donucovacích orgánů členských států, prostřednictvím sbližování* (jejich) *trestněprávních předpisů…"* Rada v něm otevřeně přiznává rostoucí obavy z možných teroristických útoků proti informačním systémům a z rozšiřování organizované trestné činnosti v této oblasti, čímž má být ohrožen prostor svobody, bezpečnosti a práva, který si Společenství bere za úkol chránit. Aby bylo tohoto cíle dosaženo, má rámcové rozhodnutí doplnit jiné nástroje, které existují jak na úrovni EU, tak i na úrovni mezinárodní, a vycházet z nich (zejména Úmluva Rady Evropy o kyberkriminalitě).

Rozhodnutí stanovuje pro členské státy povinnost kriminalizovat protiprávní přístup k informačním systémům a dále protiprávní zásah do systému a protiprávní zásah do dat (neoprávněným vložením, přenosem, poškozením, vymazáním, znehodnocením, pozměněním, potlačením nebo znepřístupněním počítačových dat), na což navazuje i povinnost stanovit za tato provinění přiměřené a odrazující tresty včetně trestu odnětí svobody. Členské státy mohou kriminalizaci uvedených činností omezit, v textu dokumentu jde o formulaci, že je nezbytné přijmout *„opatření k zajištění toho, aby* (jmenovaná činnost) *byla trestným činem, a to alespoň pokud se nejedná o případy menšího významu."* Výklad a chápání pojmu „případ menšího významu" se ukázaly poněkud problematickými, jak vyplývá ze zprávy Komise ze dne 14. 7. 2008.

> Ustanovením článku 12 rámcového rozhodnutí bylo členským státům uloženo, aby sdělily Radě a Komisi do 16. března 2007 znění předpisů, kterými ve vnitrostátním právu provádějí povinnosti z rozhodnutí vyplývající. Zhodnocením celé situace se následně zabývala Komise ve své zprávě pod číslem KOM(2008) 448. Zpráva rozhodně není dobrým vysvědčením pro jednotlivé státy už proto, že k zadanému datu splnilo předepsanou povinnost pouze Švédsko a to ještě neúplně. Po rozeslání upomínek splnilo svou oznamovací povinnost 20 států z celkového počtu 27, přičemž řada poskytnutých informací byla neúplných. Problém nastal především s výkladem pojmu „případ menšího významu". Dle původně zamýšleného pojetí měl tento pojem odkazovat na protiprávní postup menší důležitosti nebo případ, kdy porušení důvěrnosti informačního systému je menšího stupně. Cílem bylo přimět státy formálně upravit alespoň základní oblast trestnosti a poskytnout jim manévrovací prostor pro úpravu přísnosti jednotlivých ustanovení. Některé státy (konkrétně Finsko, Česká republika, Lotyšsko a Rakousko) však ve své právní úpravě svázaly v rozhodnutí předepsané skutkové podstaty ještě s dalšími okolnostmi (např. se zvláštním úmyslem spáchat trestný čin, se způsobením závažné újmy či závažným ohrožením protiprávně získaných dat apod.), které nelze považovat za soudržné s výše uvedeným chápáním. V uvedených případech se proto nejedná o „případy menšího významu", jak je zavádí předmětné rámcové rozhodnutí.

Pojetí odpovědnosti právnických osob je nastaveno obdobně jako u rámcového rozhodnutí Rady 2001/413/SVV, o potírání podvodů a padělání bezhotovostních platebních prostředků. Jurisdikce má být založena opět dle zásady teritoriality a personality, přičemž článek 10 odst. 2 výslovně stanoví, že pravomoc má zahrnovat jak případy, kdy pachatel spáchal trestný čin v době své fyzické přítomnosti na státním území, bez ohledu na umístění napadeného počítačového systému, tak situace, kdy pachatel provedl útok na počítačový systém lokalizovaný na území státu ze zahraničí. V případě, že je ke stíhání trestného činu příslušných více členských států, apeluje Rada na jejich vzájemnou spolupráci při rozhodování, kdo z nich bude pachatele přednostně stíhat (viz proces popsaný v Kapitole 3.3).

Sdělení Komise Evropskému parlamentu, Radě, Hospodářskému a sociálnímu výboru a výboru regionů KOM(2006) 688 ze dne 15. listopadu 2006, boj proti spamu a špionážnímu („spyware") a škodlivému softwaru („malicious software")

V tomto dokumentu Komise upozorňuje na rostoucí nebezpečí šíření *spamu*,[62] škodlivého *spamu* a *malware* jako takového. Rostoucí miliardové náklady spojené se *spamem*, které vznikají hlavním evropským ekonomikám, mají značný hospodářský dopad. Komise kladně hodnotí opatření pro potírání šíření tohoto nežádoucího fenoménu – zvyšování informovanosti uživatelů, budování mezinárodní kontaktní sítě orgánů bojujících proti *spamu* (CNSA, LAP a jiné mezinárodní iniciativy) i opatření aplikovaná ze strany soukromého sektoru, který přijal svůj díl odpovědnosti a účinně se na potírání *spamu* podílí vlastními prostředky (technická opatření, smluvní vyloučení nekalých praktik apod.)

Komise však zároveň varuje, že se *„stále propojenější trestní a správní hlediska spamu a dalších hrozeb doposud dostatečně nepromítla do odpovídajícího zintenzivnění postupů spolupráce v členských státech, jež by spojily technické a vyšetřovací dovednosti jednotlivých subjektů."*[63] Komise tak vyzývá orgány členských

62 *Spamming* jako takový není trestným činem, jedná se však o nežádoucí obtěžující aktivitu a jeho propojení s trestnou činností je velmi úzké. Nejde jen o situace, kdy je rozesílám infikovaný *spam*, samotné získávání osobních údajů, na základě kterých je *spam* rozesílán, je velmi často prováděno nezákonným způsobem. Všechny tyto faktory činí ze *spammingu* velmi nebezpečný fenomén, jehož negativní potenciál stále narůstá.

63 Sdělení Komise Evropskému parlamentu, Radě, Hospodářskému a sociálnímu výboru a výboru regionů KOM(2006) 688 ze dne 15. listopadu 2006, boj proti *spamu* a špionážnímu („*spyware*") a škodlivému *softwaru* („*malicious software*"), s. 7.

států ke stanovení jasných hranic odpovědnosti v rámci boje proti *spamu* a také k větší míře spolupráce a zdokonalení koordinace mezi jednotlivými orgány v rámci státu i mezi státy navzájem. Dále apeluje na soukromý průmyslový sektor, aby posílil svou iniciativu a využíval svých možností, které mu dává jeho přímý kontakt s uživatelem (odpovědný postup při dodávání a instalaci *softwaru*, zvýšení informovanosti spotřebitele, zvýšení bezpečnostních opatření apod.). Ze strany orgánů ES/EU přislíbila Komise intenzivní práce na smlouvách se třetími zeměmi a nových legislativních návrzích, které posílí politiku boje proti kybernetické trestné činnosti.

Dalšími dokumenty z poslední doby, které neoddiskutovatelně stojí za zmínku jsou:

- **Sdělení Komise Evropskému parlamentu, Radě a Evropskému výboru regionů KOM(2007) 267 ze dne 22. května 2007, k obecné politice v boji proti počítačové kriminalitě**

- ***Závěry* Rady 2009/C 62/05 ze dne 27. listopadu 2008, o společné pracovní strategii a konkrétních opatřeních v oblasti boje proti počítačové trestné činnosti**

- **Sdělení Komise Evropskému parlamentu, Radě, Hospodářskému a sociálnímu výboru a výboru regionů KOM(2009) 149 ze dne 30. března 2009, o ochraně kritické informační infrastruktury**

Důvod, proč zde nebudou popsány podrobněji, je prostý – znamenalo by to v zásadě opakovat stále dokola prohlášení již obsažená výše, čemuž se autorka chce pokud možno vyhnout. Dokumenty přinášejí obecné zhodnocení dosavadního vývoje pro danou oblast společně s varováním, že nebezpečí stále narůstá a prohlubuje se. Zároveň je konstatován fakt, že vzhledem k povaze kyberprostoru a počítačové trestné činnosti není možné účinně bojovat pouze prostředky na národní úrovni – mezinárodní spolupráce je proto nutná. Kromě zákonodárných aktivit, které mají za úkol harmonizovat právní rámec pro potlačování kyberkriminality, je nezbytné spolupracovat i na zakládání a fungování speciálních projektů a akcí, které koordinují a usnadňují společný postup (např. kontaktní síť orgánů bojujících proti spamu CNSA, Londýnský akční plán LAP nebo Evropská agentura pro bezpečnost sítí a informací ENISA). Evropské orgány zároveň zdůrazňují roli, jakou hraje soukromý sektor při regulování chování v kyberprostoru a apelují na prohloubení spolupráce s poskytovateli informačních služeb či jinými zainteresovanými právnickými osobami, které by měly přijmout svůj díl odpovědnosti za vývoj situace. Otázkou zůstává, jaký je skutečný význam podobných prohlášení Rady a Komise – zda jde o pouhý komentář signalizující „bdělost Unie" bez výraznějšího dopadu na vývoj situace v Evropě, nebo mají podobné deklaratorní texty skutečný význam při řešení konkrétních problémů.

Pro druhou možnost hovoří i řada projektů na mezinárodní úrovni, jejichž počet poslední dobou rychle stoupá. Pod záštitou významných světových organizací a institucí dochází k rozvoji spolupráce v boji proti počítačové kriminalitě, přičemž se nyní mezinárodní společenství zaměřuje především na tyto tři oblasti – potírání dětské pornografie, omezování projevů rasistické a xenofobní povahy a na boj proti terorismu. Zvláště poslední oblasti je v poslední době věnována výrazná pozornost, neboť je již jen otázkou času, kdy k prvnímu pokusu o kybernetický teroristický útok dojde. K rozvíjení preventivních opatření a zvýšení pozornosti tak vyzývá Organizace spojených národů, [64] Organizace pro bezpečnost a spolupráci v Evropě,[65] Organizace pro hospodářskou spolupráci a rozvoj,[66] Severoatlantická aliance,[67] Skupina vyspělých států světa G8[68] a v neposlední řadě pochopitelně Evropská unie.[69] [70]

4.3 Česká právní úprava

Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

Modernizovaná náhrada více než 40 let starého zákona č. 140/1961 Sb., trestního zákona, ve znění pozdějších předpisů, vstoupila v účinnost dne 1. ledna roku 2010. Příprava zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů (dále jen „trestní zákoník" nebo „NTZ" [71]), trvala skoro 15 let, parlament konečné znění schválil po více než rok trvajícím jednání a prezident republiky jej podepsal dne 27. ledna 2009. Tento zákon přinesl do oblasti trestního práva změny bez nadsázky řečeno revoluční v podobě nových zásad i právních institutů. Ve vztahu k našemu tématu je podstatné především uznání významné role užívání informačních technologií ve společnosti (a tedy i ve světě zločinu), dále plné zohlednění specifik moderní trestné činnosti, tedy faktu, že tato činnost již není fixně vázána na fyzickou stránku pachatele a tudíž je jeho akční rádius resp. okruh dotčených osob mnohem širší. Zákon tak počítá s nezbytností mezinárodní spolupráce na vysoké úrovni a na jeho obsahu je výrazně znát vliv mezinárodních dokumentů, které se Česká republika zavázala respektovat.

Místní působnost zákona (a tedy odvozeně i pravomoc českých orgánů) je upravena v úvodních ustanoveních §§4 – 9, přičemž jednotlivé paragrafy jsou označeny podle zásad, které aplikují. Rozborem předmětných ustanovení lze dojít k závěru, že nový trestní zákoník aplikuje většinu jurisdikčních principů, jak byly rozebrány v Kapitole 3. Postrádat snad lze pouze uplatnění doktríny efektu, jejíž význam pro potírání přeshraniční počítačové kriminality byl vyzdvižen již výše.

Trestní zákoník dělí trestné činy podle závažnosti na přečiny a zločiny. Skupina přečinů zahrnuje všechny nedbalostní trestné činy a činy, za které lze stanovit trest odnětí svobody

64 Viz např. Rezoluce Rady bezpečnosti OSN č. 1624 ze dne 14. září 2005, S/RES/1624 (2005).

65 Viz rozhodnutí Rady ministrů č. 3/2004, o boji proti používání Internetu pro účely terorismu, MC.DEC/3/04.

66 K vytvoření a posílení nových opatření pro posílení bezpečnosti vybízí Výbor pro informační, počítačovou a komunikační techniku *(Committee for Information, Computer and Communication Policy)* ve svých *Pokynech pro bezpečnost informačních systémů a sítí: Směrem ke kultuře bezpečnosti (OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security).*

67 Vyvrcholením řady akcí ze strany NATO je kupříkladu studie vypracovaná Pracovní skupinou pro telekomunikace (*Working Group for Telecommunications, Civil Communication Planning Committee NATO*), která se věnuje obraně sítí elektronických komunikací a informačních systémů proti kybernetickému útoku.

68 Svůj zájem o tuto problematiku projevily vyspělé státy již v roce 1996 podporou založení specializované Skupiny zaměřené na „*high-tech*" zločin.

69 Viz např. Akční plán Evropské unie pro boj s terorismem apod.

70 Do podrobností se touto problematikou zabývá Ministerstvo vnitra České republiky ve svém dokumentu *Mezinárodní spolupráce v boji proti informační kriminalitě* [online]. [cit. 2010-02-22]. Dostupné z:
<www.mvcr.cz/soubor/cyber-vyzkum-studie-mezinarodni-pdf.aspx>.

71 „NTZ" podle obecně užívaného označení „nový trestní zákoník", které umožňuje odlišení od předchozího předpisu, běžně označovaného jako „TZ".

s horní sazbou do pěti let. Za zločiny jsou pak označovány všechny trestné činy, které nespadají mezi přečiny. Trestně odpovědné jsou dle NTZ pouze příčetné osoby fyzické, a to od patnácti let věku. Zavedení institutu trestní odpovědnosti právnických osob (resp. institutu, který by umožnil trestání právnických osob za vážná provinění jinak ošetřená trestním právem) je v současnosti odbornou veřejností široce diskutováno a ačkoliv k řešení tohoto problému vyzývají i mezinárodní dokumenty, kterými je ČR vázána, nebylo doposud nalezeno jednotné řešení. Diskuze k tomuto tématu proběhne v následujících kapitolách.

Skutkové podstaty trestných činů spočívajících v protiprávním zásahu do počítačového systému jsou nově upraveny a zařazeny na základě Úmluvy Rady Evropy o kyberkriminalitě, především jejích článků číslo 2 – 11. Dalším podkladem pro novou úpravu je Rámcové rozhodnutí Rady 2005/222/SVV ze dne 24. února 2005, o útocích proti počítačovým systémům. Převzetím těchto mezinárodních dokumentů došlo k rozšíření a konkretizaci úpravy nových forem počítačové kriminality (§§230 – 232 NTZ), přičemž její tradiční formy jsou i nadále postižitelné podle obecnějších skutkových podstat, jak jsou zavedeny například v rámci trestných činů proti majetku, trest ných činů proti lidské důstojnosti v sexuální oblasti nebo činů narušujících soužití lidí.

Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů

Zatímco trestní právo hmotné bylo modernizováno zcela novým zákonem, v právu procesním dochází prozatím pouze k novelizacím již téměř padesát let starého zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů (dále jen „trestní řád" nebo „TŘ"). Trestní řád je tou nejzákladnější trestněprocesní normou a ač ve svém názvu odkazuje na trestní řízení soudní, tvoří ve skutečnosti úprava řízení před soudem jakožto jednoho ze stadií trestního řízení pouze část tohoto rozsáhlého kodexu.

Pro stíhání počítačové kriminality je stěžejní především postup před zahájením trestního stíhání, přípravné řízení a fáze vyšetřování upravené v ustanoveních §§ 157 – 179h TŘ, kdy dochází ke shromažďování materiálů, které se následně mají stát podkladem pro obžalobu v řízení před soudem. Jak již vyplývá z povahy počítačové kriminality, vyžadují tyto přípravné fáze vysoce odborný postup, který je v porovnání s obecnými kriminalistickými postupy značně specifický vzhledem ke své technické náročnosti. Obecně lze konstatovat, že čím je procesní úkon důležitější a čím více zasahuje do práv a integrity dotčené osoby, tím přísněji je trestním řádem předepsána obsahová a formální náležitost takového úkonu. Orgány činné v trestním řízení[72] totiž velmi často balancují na hranici mezi veřejným zájmem a ústavně zaručenými právy, kdy je velmi snadné a mnohdy i do jisté míry nezbytné tuto mez překročit. Trestní řád se proto svou přesnou dikcí snaží podobné konflikty a pohyb „v šedé zóně mezi využitím a zneužitím práva" eliminovat. Za účelem odhalování počítačové kriminality a dopadení pachatele jsou prováděny zejména prohlídky domovní a jiných prostor, ohledání místa činu, zajištění a šetření obsahu výpočetní techniky a výslech obviněného.[73] Praxe bohužel často naráží na fakt, že zobecnělé trestněprocesní normy, které, ač průběžně novelizované, nejsou s to sledovat rychlost vývoje v oboru, brzdí a omezují činnost orgánů činných v trestním řízení při vyšetřování počítačové kriminality. Postupy jsou často značně zdlouhavé a mnohdy chybí vhodná procedura úplně, o čemž se přesvědčíme v následujících kapitolách.

Zákon č. 480/2004 Sb., o některých službách informační společnosti, ve znění pozdějších předpisů

Tento právní předpis[74] vznikl za účelem harmonizování českého práva s právem ES, jak k němu vyzývá Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000, o některých aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (dále jen „směrnice o elektronickém obchodu"). Co se týče stanovení odpovědnosti ISP, zákon v zásadě kopíruje předmětné články směrnice a rozděluje ISP do tří skupin:

- poskytovatelé služeb spočívajících v přenosu informací poskytnutých uživatelem (angl. *mere conduit* nebo také *access provider*)
- poskytovatelé služeb spočívajících v automatickém meziukládání informací poskytnutých uživatelem (tzv. *caching*)
- poskytovatelé služeb spočívajících v ukládání informací poskytnutých uživatelem (tzv. *storage* nebo také *hosting*).

Obecně se tedy dá říci, že český právní řád přijímá zásadu, že je ISP odpovědnosti ze zákona zbaven, pokud neměl ani povědomosti o vzniku nebo komunikaci informace protiprávního charakteru. Pro účely tohoto článku je důležité, že zákon č. 480/2004 Sb. nevyužil možnosti stanovit oprávnění soudu resp. správního orgánu požadovat po poskytovateli služeb informační společnosti omezení nebo zastavení služby, pokud dochází k porušování práv, jak to umožňuje čl. 12 odst. 3, čl. 13 odst. 2 a čl. 14 odst. 3 směrnice. Že však lze s takovým autoritativním zásahem v českém právním řádu přece jen počítat naznačuje již hned nejbližší ustanovení §4 písm. e) zákona č. 480/2004 Sb., které implementuje pravidla obsažená v čl. 13 odst. 1 písm. e) Směrnice. Dle české právní úpravy je totiž ISP druhého typu odpovědný za obsah informací, *„pokud … ihned nepřijme opatření vedoucí k odstranění jím uložené informace nebo k znemožnění přístupu k ní, jakmile zjistí, že … soud nařídil stažení či znemožnění přístupu k této informaci."* Zákon tedy počítá s možností, že soud autoritativně zasáhne, pouze se k tomu explicitně nevyjadřuje a bohužel také nedává procesní návod pro konkrétní postup pověřeného orgánu. Důležité je též upozornit na fakt, že český zákonodárce toto rozhodnutí vložil pouze do rukou soudu, směrnice oproti tomu dává státům možnost, předat tuto nařizovací pravomoc kromě soudů i *„jinému správnímu orgánu"*. Význam tohoto faktu bude okomentován v následujících kapitolách.

72 Postavení a další pravomoci jednoho z orgánů činných v trestním řízení, konkrétně Policie ČR, jsou upraveny v zákoně č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů. Pro tento článek důležitá ustanovení tohoto předpisu budou společně s vybranými paragrafy trestního řádu analyzována v Kapitole 6.

73 Více viz GŘIVNA, T. – POLČÁK, R. – HERCZEG, J. et al. *Kyberkriminalita a právo.* 1. vyd. Praha: Nakladatelství Auditorium, 2008. s. 89 – 97.

74 Vybraná ustanovení zákona č. 480/2004 Sb. naleznete v příloze č. 2.

Co se týče odpovědnosti ISP za obsah informací uložených na pokyn uživatele, dává směrnice 2000/31/ES členským státům dvojí možnost přístupu k jejímu založení. Český zákonodárce zvolil přísnější kritérium a založil odpovědnost na podmínce nevědomé nedbalosti ISP ve vztahu k protiprávnímu obsahu informace. Dle tohoto přístupu pak ISP za protiprávní charakter informace odpovídá, i když o něm nevěděl, ačkoli vzhledem k okolnostem vědět mohl. Druhou možností by pak bylo použití podmínky vědomé nedbalosti, která je vázána na fakt, že ISP o protiprávním charakteru informace věděl.[75]

5 Odpovědnost ISP

V předchozích kapitolách bylo pojednáno o problémech boje s počítačovou kriminalitou především z teoretického hlediska. Nyní tedy lze v zásadě velmi zjednodušeně říci, že máme konkrétně definovaný zločin a dle obecně daných zásad a platné právní úpravy jsme schopni určit, který stát resp. státy mohou na základě své pravomoci tento zločin stíhat. Nalezena byla tedy odpověď na otázku *„Co?"* a následně *„Kdo?"*, zbývá tedy odpovědět na otázku *„Jak?"* a ve spojitosti s ní na často opomíjené *„Jestli vůbec?"*. Význam definičních autorit v kyberprostoru, jak je popsali Lessig a Polčák, byl již zdůrazněn v kapitole první. Jak bylo již řečeno, právo může být v této oblasti prosazeno pouze prostřednictvím působení na tyto entity, které regulují komplexní fungování celého systému. Je proto nezbytné, aby předmětné definiční autority nesly i odpovídající právní odpovědnost za svá jednání a způsob, jakým tento vliv uplatňují.

5.1 Trestněprávní odpovědnost fyzických a právnických osob

Na základě předchozích úvah lze dojít k závěru, že vzhledem k výraznému vlivu definičních autorit na fungování v oblasti informačních technologií je nezbytné, aby tyto byly za své aktivity právně odpovědné. Rozsah této odpovědnosti je však nutno stanovit velmi citlivě a brát při tom ohledy na jednotlivá specifika, která s sebou aktivita ve světě kyberprostoru nese. Před započetím diskuze na téma šíře odpovědnosti jednotlivých aktérů však zbývá najít odpověď na základní otázku, zda mohou být vůbec tyto definiční autority odpovědné. Tento článek se zaměřuje na veřejnoprávní ochranu kyberprostoru, pozornost tedy bude primárně věnována odpovědnosti trestněprávní v rámci českého právního řádu.

Fyzické osoby jsou dle obecně přijímaných pravidel trestněprávně odpovědné, naplní-li skutkovou podstatu trestného činu. Skutková podstata je strukturována do čtyř složek – subjekt, subjektivní stránka, objekt a objektivní stránka – přičemž všechny tyto složky musí být posouzeny a jejich znaky naplněny, jinak nelze trestněprávní odpovědnost založit. Kategorie subjektu se zabývá osobností pachatele – odpovědnou tedy může být jen osoba dospělá (resp. ve věku mladistvého, §25 NTZ, §2 odst. 1 písm. c) zákona č. 218/2003 Sb., o soudnictví ve věcech mládeže, ve znění pozdějších předpisů (dále jen „ZSM") *per argumentum a contrario*) a příčetná (§26 NTZ, u mladistvého navíc posuzována rozumová a mravní vyspělost - §5 odst. 1 ZSM), přičemž někdy může zákon navíc vyžadovat, aby se tato osoba vyznačovala nějakou zvláštní způsobilostí či postavením (§114 NTZ). Subjektivní stránka skutkové podstaty trestného činu jej charakterizuje z vnitřního hlediska pachatele, tj. z hlediska jeho vnitřního postoje a psychiky, jeho zavinění. Ustanovení §13 odst. 2 NTZ vyžaduje k trestnosti činu úmyslného zavinění, nestanoví-li zákon výslovně, že postačí zavinění z nedbalosti. Fakultativními znaky subjektivní stránky jsou potom motiv (pohnutka), cíl (účel) a záměr. Při posuzování trestněprávní odpovědnosti musí být vždy zohledněno zavinění subjektu, bez tohoto by nebyla naplněna skutková podstata a trestný čin by *de facto* nevznikl. Proto je v trestním právu posuzována pouze subjektivní odpovědnost pachatele a nikdy odpovědnost objektivní, která na subjektivní stránku nebere zřetel. Tato skutečnost je v novém trestním zákoníku ještě posílena výkladovým posunem od zaměření na odpovědnost za následek směrem k posuzování odpovědnosti za vinu jako takovou.

Objektem v rámci skutkové podstaty je určitý právem chráněný zájem, který je činem narušen či ohrožen. Objektivní stránka trestného činu pak charakterizuje trestný čin z pohledu vnějšího. Jejími obligatorními znaky jsou jednání, následek a příčinná souvislost (*kauzální nexus*) mezi jednáním a následkem. Fakultativně ji doplňuje místo, čas a způsob spáchání trestného činu doplněny o zhodnocení účinku jednání.[76]

Naprosto odlišná je situace při posuzování trestněprávní odpovědnosti osob právnických. Český právní řád totiž se zavedením tohoto druhu odpovědnosti nepočítá. Za trestné činy připsatelné na vrub právnické osobě byly vždy trestně odpovědné osoby, které tuto právnickou osobu zastupovaly, resp. jednaly jejím jménem. Příčinu fixace trestní odpovědnosti na konkrétní fyzickou osobu lze spatřovat v chápání samotného smyslu trestu, které se vyvinulo v průběhu historie. Kromě funkce represivní má trest fungovat i jako prevence budoucího závadného jednání. Podle Nietzscheho má trest působit jako prostředek, kterým bylo možno vštípit konkrétní osobě do paměti fakt, že daná činnost je nežádoucí a není ve společnosti tolerována, přičemž nejúčinnější mnemotechnickou pomůckou je bolest.[77] Vytvoří-li se tedy v lidské mysli určitý vzorec, dle kterého určitá činnost rovná se bolestivý vjem (tedy jakýkoli zásah do fyzické či psychické integrity jedince, který ho nějakým způsobem citlivě zraňuje), je pravděpodobné, že tato silná vzpomínka trestem postiženého jedince do budoucna od takové činnosti odradí. Při aplikaci tohoto závěru na právnickou osobu pak vzniká nesnáz v tom, že právnická osoba je nehmotná fiktivní entita, nemá tělo, nemá osobnost ani fyzický základ, kterému by bylo možno trestem vštípit žádoucí vzpomínku v podobě odrazujícího vzorce. Právnickou osobu také už z její podstaty nelze oddělit od fyzických osob, které v jejím rámci působí, a autoritativně udělený trest je ve skutečnosti druhotně přenesen na tyto fyzické osoby. Jeho účinnost také *de facto* ovlivňují jednotlivé aktivity těchto osob, což není vzhledem k účelu institutu trestání žádoucí. Vzniká tak otázka, zda aplikací trestněprávní odpovědnosti na právnickou osobu může být dostatečně účinně naplněna pre-

75 Více se k této problematice rozepisuje Polčák v knize POLČÁK, R. *Právo na internetu: Spam a odpovědnost ISP*. 1. vyd. Brno: Computer Press, a.s. 2007, s. 59 – 60.

76 Pro účely této práce toto stručné shrnutí postačí. Velmi podrobný rozbor nabízí např. Kratochvíl, viz:
KRATOCHVÍL, V. a kol. *Kurs trestního práva: Trestní právo hmotné, Obecná část.* 1. vyd. Praha: C. H. Beck, 2009, s. 188 – 258.

77 Bolest pochopitelně nemusí být pouze fyzického rázu, jde obecně o jakýkoli zásah či deprivaci, která negativně zasáhne trestaného jedince (tj. i trest odnětí svobody, zabavení určité ceněné hodnoty apod.).

ventivní funkce trestu, a jaký trest tedy v tomto specifickém případě zvolit.

Současná praxe odpovídá na tuto otázku kladně a k zavedení odpovědnosti právnických osob, ať už přímo trestněprávní nebo jiné s obdobným charakterem, přímo vyzývají i mezinárodní dokumenty (viz předchozí kapitola). Co se týče nového trestního zákoníku, rozhodl se český zákonodárce setrvat ve svém předchozím postoji a nadále institut trestní odpovědnosti právnických osob nezavádět. Podle současných plánů má být v budoucnu úprava odpovědnosti těchto osob včetně účinných a přiměřených sankcí ponechána v oblasti správního trestání. Český zákonodárce se tak inspiroval v četných pokročilejších zahraničních úpravách a v současnosti operuje s katalogem sankcí, které jsou svou povahou již přímo přizpůsobeny právnickým osobám:

- zrušení právnické osoby, pokud její činnost spočívala zcela nebo převážně v páchání trestného činu
- propadnutí majetku v případě, že se právnická osoba získala nebo se snažila získat závažným zločinem majetkový prospěch
- propadnutí věci případně náhradní hodnoty
- peněžitý trest, pokud se právnická osoba získala nebo se snažila získat majetkový prospěch prostřednictvím trestného činu
- zákaz činnosti (1 rok až 20 let)
- zákaz účasti v zadávacím řízení o veřejných zakázkách a ve veřejné soutěži, pokud trestný čin souvisel s touto činností (1 rok až 20 let)
- zákaz přijímat dotace a subvence, pokud byl trestný čin spáchán v souvislosti s procesem přijímání těchto podpor (1 rok až 20 let)
- zveřejnění pravomocného odsuzujícího rozsudku nebo jeho části v obchodním věstníku nebo v jiném veřejném sdělovacím prostředku na náklady odsouzené právnické osoby.

Tyto sankce jsou voleny tak, aby primárně zasáhly právnickou osobu na citlivém místě a splnily tak požadovanou funkci trestu. Při stanovení druhu trestu a jeho výměry je s ohledem na odlišnosti právnické osoby od osob fyzických nezbytné přihlížet ke specifickým okolnostem – vedle povahy a závažnosti jsou to například vnitřní a vnější poměry právnické osoby, její majetkové poměry, její jednání po činu apod.[78]

5.2 Trestněprávní odpovědnost ISP

Pro následující rozbor je nejprve nutné definovat pojem „poskytovatel informačních služeb." Polčák[79] ISP vymezuje jako definiční autoritu, která poskytuje, typicky za úplatu, ostatním své služby, *„jejichž prostřednictvím mohou … vstupovat do informační sítě, resp. jejichž prostřednictvím zde probíhá tvorba, zpracování nebo výměna informací."* Česká právní úprava, konkrétně zákon č. 480/2004 Sb., o některých službách informační společnosti, ve znění pozdějších předpisů, v sobě koncentruje ustanovení dvou evropských směrnic – Směrnice Evropského parlamentu a Rady č. 98/34/ES ze dne 22. června 1998, o postupu při poskytování informací v oblasti norem a technických předpisů, ve znění Směrnice 98/48/ES, která definuje službu informační společnosti, a Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000, o některých aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („směrnice o elektronickém obchodu"). Zákon tak poskytuje relevantní definice služby informační společnosti (§2 písm. a), elektronické pošty (§2 písm. b), elektronických prostředků (§2 písm. c), poskytovatele služby (§2 písm. d) a uživatele (§2 písm. e).

Při snaze označit konkrétní aktivity za služby informační společnosti je vždy nezbytné zohlednit postoj dotčeného uživatele. Tento musí vždy spočívat v aktivním jednání, v impulzech, které jsou způsobilé vyvolat interakci mezi poskytovatelem a uživatelem, jejíž podstata leží v elektronicky komunikované informaci. Na základě shrnutí článku 18 Preambule k směrnici č. 2000/31/ES formuluje Polčák[80] tři základní kritéria, při jejichž naplnění je možno určitý subjekt označit za ISP:

1. služba je poskytována pro jiného (vyloučen je tady např. služby poskytované v rámci zaměstnavatelského poměru),
2. podstata služby leží v elektronicky komunikované informaci (elektronická výměna informací není pouhým prostředkem, kterým je realizována služba mající podstatu v něčem jiném) a
3. služba je poskytována individuálně za přímého přičinění uživatele při její konzumaci (odpadá tak např. rozhlasové vysílání),

přičemž u každého jednotlivého případu je nezbytné zohlednit jeho individuální charakter a zvláštnosti. S pomocí zákona č. 480/2004 Sb. tak můžeme ISP rozdělit na poskytovatele služeb spočívajících v přenosu informací poskytnutých uživatelem, poskytovatele služeb spočívajících v jejich automatickém meziukládání a dále na ty, jejichž činnost spočívá v ukládání takových informací (jak již bylo ostatně konstatováno v kapitole věnované právní úpravě).

Trestněprávní odpovědnost ISP - teorie a postupný vývoj

Z prosté teorie i z praktických poznatků jasně vyplývá, že poskytovatelé informačních služeb jsou skupinou natolik specifickou, že je naprosto nevyhnutelné zohlednit tento fakt i v rámci právní úpravy. Oproti očekávání však tento proces, zvláště ve vztahu k právu trestnímu, trval velmi dlouho a v mnoha aspektech není doposud ukončen. Odpovědnost ISP byla totiž po značnou dobu posuzována ve světle tehdejší právní úpravy a právotvůrci až postupně a jakoby váhavě začali uznávat fakt, že stávající pravidla tolik vázaná na fyzický svět zkrátka nelze vhodně „napasovat" na nově fungující fenomén. Při sledování vývoje především v období devadesátých let 20. století tak můžeme vypozorovat různé způsoby, jakými byla hodnocena trestněprávní odpovědnost ISP.

První možností bylo podřazení trestněprávní odpovědnosti ISP normám tradičního trestního práva bez specifického

78 Více se k tomuto problému vyjadřuje KRATOCHVÍL, V. a kol. Kurs trestního práva: *Trestní právo hmotné, Obecná část.* 1. vyd. Praha: C. H. Beck, 2009, s. 731 – 732. Z tohoto zdroje byl taktéž převzat katalog sankcí vyjmenovaných výše.

79 Pro bližší informace nahlédněte do knihy POLČÁK, R. *Právo na internetu: Spam a odpovědnost ISP.* 1. vyd. Brno: Computer Press, a.s. 2007, s. 46.

80 Ibid, s. 49.

omezení odpovědnosti.[81] Problematickým se toto řešení jeví už při zkoumání samotné povahy jednání, které aspiruje na označení za trestné. V modelové situaci stojí na jedné straně poskytovatel, tedy původce obsahu – informace (angl. *„content provider"*), která se následně ukáže závadnou. Tento původce obsahu vědomě a cíleně umístí závadnou informaci prostřednictvím služby poskytované ISP na internet – tím naplní skutkovou podstatu trestného činu a je trestněprávně odpovědným. Otázkou však zůstává, v jaké pozici zde stojí poskytovatel dané služby (angl *„service provider"*). Jak bylo již napsáno v předchozích odstavcích, musí být pro založení odpovědnosti naplněna skutková podstata trestného činu, jejíž nedílnou součástí je i subjektivní stránka hodnotící zavinění. Ptáme se tedy, v čem v tomto případě vězí ona subjektivní vina ISP, který poskytl svoje služby, jichž bylo následně zneužito.

Možná odpověď se nalézá ve zhodnocení samotného charakteru trestného činu – zdali se jedná o delikt komisivní či omisivní. Komisivní delikt spočívá v aktivním cíleném jednání, které má za následek navození závadného stavu. Budování technické infrastruktury určené k sociálnímu užívání, které je *de facto* náplní činnosti ISP, však přece není samo o sobě ze zákona trestné. Zbývá tedy delikt omisivní, spočívající v opomenutí konat – v našem případě nepřijetí kontrolních a preventivních opatření, případně absence snahy zakročit proti závadnému stavu. ISP je zde stavěn do pozice garanta resp. ingerenta, který nesplnil svou povinnost. Garantem je zjednodušeně řečeno osoba, která přijetím určité pozice či povinnosti (ta jí není nijak autoritativně vnucena) na sebe bere i povinnost, že bude v nebezpečí, které vzniklo v souvislosti s předmětnou povinností, konat a snažit se závadný stav napravit. Nesplněním této povinnosti v nebezpečí zasáhnout pak garantující osoba naplňuje skutkovou podstatu omisivního deliktu. Klasickým modelovým příkladem je skupina horolezců chystajících se zdolat nebezpečnou horu – každý jednotlivec si je vědom rizika a své odpovědnosti vůči skupině, zahájením společného výstupu bere na sebe povinnost v případě nebezpečí zasáhnout a pokusit se jej odvrátit. Pokud bychom tuto konstrukci aplikovali na ISP, v pozici garanta na sebe bere zahájením své činnosti povinnost bránit páchání trestných činů prostřednictvím zneužívání svých služeb. Pokud tuto povinnost nesplní a trestnému činu nezabrání, je trestně odpovědná.

Garant specifického typu, tzv. ingerent svým nebezpečným jednáním, které je v rozporu s jeho právní povinností, sám působí navození závadného stavu. Z toho mu plyne povinnost sám se aktivně podílet na odstranění tohoto závadného stavu. Pokud tak neučiní, je odpovědný z omisivního deliktu. Za příklad je dávána povinnost osoby, která nedopalkem založí požár, pokusit se oheň uhasit a aktivně se podílet na odvrácení škody. V případě ISP je tato konstrukce poněkud krkolomná – otázkou je, v čem lze označit činnost ISP za nebezpečnou, zda v poskytování služeb veřejnosti, v jejíchž řadách se nacházejí i potenciální pachatelé trestných činů. Nebezpečná činnost je totiž obecně chápána jako aktivita již od počátku negativní, jako něco, „co se dělat nemá" a co může vyvolat, resp. vyvolá škodlivý následek. To by tedy znamenalo, že činnost ISP je a priori brána jako nebezpečná a hazardní. Nemluvě o faktu, že mezi nebezpečnou činností a škodlivým následkem, který je pak nutno odvracet, musí být příčinná souvislost. Zde se však musíme ptát, jaká je souvislost mezi budováním technické infrastruktury určené k sociálnímu užívání a poskytováním služeb v jejím rámci na straně jedné a ukájením potřeby deviantního chování naprosto odlišnou osobou na straně druhé.

Ve specifickém případě ISP se může výše zmíněná konstrukce zdát přímo absurdní. Přesto je tato právní argumentace, uplatňovaná například koncem devadesátých let v Německu, velmi významná pro další výklad už proto, že německé právo trestní značnou měrou ovlivnilo i českou právní úpravu. Postupný vývoj totiž sice odstranil nedostatky a přinesl tolik požadovanou regulaci omezení obecné odpovědnosti ISP, trestní právo však žádnou specifickou konstrukci pro postih ISP doposud nemá a ani pravděpodobně mít nebude.

Použití tradiční (a pro ISP značně tvrdé a omezující) argumentace dokumentuje významný případ společnosti CompuServe GmbH z roku 1998:

> *CompuServe Deutschland GmbH* se svými 170 zaměstnanci a ředitelem Felixem Sommem fungovala v 90. letech jako dceřinná společnost americké společnosti *CompuServe, Inc.* Jejím úkolem bylo poskytovat a utvářet mateřské společnosti v Německu zázemí pro poskytování služeb informační společnosti a kromě marketingové a servisní činnosti také zprostředkovávat německým zákazníkům k těmto službám přístup prostřednictvím přímého telekomunikačního kanálu na principu *dial-in* service. Smluvní vztah byl tak uzavírán přímo mezi zákazníkem a mateřskou společností *Compu Serve, Inc.* V té době se opakovaně začaly objevovat na diskusních fórech spravovaných *CompuServe, Inc.* dětské pornografické fotografie a další obrázky věnované brutální pornografii a sexu se zvířaty. Ač byly tyto závadné fotografie na žádost německé společnosti průběžně blokovány a ačkoliv se *CompuServe GmbH* podílela i na šíření *softwaru* schopného odfiltrovávat závadný obsah, ocitl se v roce 1997 ředitel Felix Somm před trestním soudem v Mnichově pro spolupodílnictví na protiprávním šíření třinácti závadných snímků.[82]
>
> V té době již byl v Německu účinný zákon o telekomunikačních službách (něm. *Teledienstgesetz*), který částečně zbavoval poskytovatele služeb v pozici *access providera* na základě v zásadě stejných podmínek, jak činí současná směrnice 2000/31/ES. Soud však v tomto případě odmítl uznat *CompuServe GmbH* za *access providera* s tím, že pouze zprostředkovává spojení mezi zákazníkem a mateřskou společností, která následně poskytuje přístupové a *hostingové* služby, jak je definuje německé právo. Následně soud rozhodl, že se americká společnost provinila šířením dětské pornografie (protože o závadném obsahu věděla) a že je

81 Německá trestněprávní teorie je pro svůj český protějšek velmi významná, protože poskytuje řadu myšlenek a závěrů, ze kterých pak české právo vychází. Následující výklad týkající se garance v trestním právu tak osvětluje některé z významných institutů německého práva, které jsou aplikovány i u nás.

82 Rozsudek číslo 8340 Ds 465 Js 173158/95.

společnosti *CompuServe GmbH* možno přičítat jednání její mateřské společnosti. Dceřinná společnost se tedy ocitla v pozici spolupachatele tohoto trestného činu (vzhledem k neexistenci trestněprávní odpovědnosti právnických osob v německém právu je osobou odpovědnou osoba společnost zastupující – tedy výkonný ředitel Felix Somm). *CompuServe GmbH* byla dle soudu v tomto případě v pozici garanta, který měl provádět fyzickou kontrolu zdroje rizika a předcházet poškození právních zájmů třetích osob. Felix Somm byl tedy za spolupachatelství na trestném činu šíření dětské pornografie odsouzen soudem prvního stupně na 2 roky nepodmíněně.[83]

Odvolací soud následně rozhodnutí prvoinstančního soudu zrušil vyvrácením předchozí argumentace a vyloučením Sommovy odpovědnosti za předmětný delikt. Oprávněné pobouření a pachuť v ústech odborné veřejnosti však již smýt nedokázal.

Další možností jak vyřešit problém trestněprávní odpovědnosti ISP, která již na rozdíl od předchozí konstrukce aplikována nebývá, byla úprava těchto služeb v rámci již existujících předpisů na základě podobnosti regulovaných aktivit. V řadě evropských států tak byly hlavně koncem devadesátých let služby informačních společností připodobňovány k činnosti vydavatelů tiskovin resp. mediálních producentů, kteří také poskytovali jednotlivým osobám prostor pro vyjádření a jejichž odpovědnost za publikovaný obsah byla z tohoto titulu omezena. Šíře trestněprávní odpovědnosti vydavatele byla stát od státu upraveny odlišně, od naprostého zproštění odpovědnosti v případě, že je jméno autora článku – pachatele – předáno odpovědným autoritám a že se pachatel nachází na území státu (Belgie), až po plnou spoluodpovědnost vydavatele, jak byla upravena například ve Francii. Jednotícím prvkem pro právní úpravy jednotlivých států byla specifikace zvláštních povinností vydavatele, tedy i poskytovatele služeb informační společnosti, který byl takto posuzován. Jednak šlo o povinnost kontrolní, kdy byl ISP povinen aktivně monitorovat činnost spotřebitele a hodnotit soulad poskytnutého obsahu se zákonem. Dále to byla povinnost identifikovat případného delikventa a veškeré údaje předat pověřeným autoritám k šetření. Je jasné, že už první podmínka znamenala pro ISP často neřešitelný problém – vzhledem k rozsahu služeb a objemu informací běžně zpracovávaných v jejich rámci zkrátka není fyzicky ani technicky možné odpovědně monitorovat veškerý obsah, nemluvě o odlišnostech v posuzování trestnosti obsahu, jak ji upravují právní úpravy jednotlivých států, na jejichž území jsou služby poskytovány. Je poměrně snadné uhlídat obsah informací, které jsou publikovány běžnými médii, např. nakladatel (resp. odpovědný redaktor) má možnost celkem účinně revidovat novinové články předtím, než půjdou do tisku. Proces je přehledně strukturovaný a masa zpracovávaných informací omezená. Otázkou však zůstává, jak aplikovat takový postup na služby ISP, kdy je objem zpracovávaných informací mnohonásobně vyšší a komplikovaná rozvětvená struktura internetových stránek často ani neumožňuje sledovat jednotlivé detaily prováděné komunikace. Nemluvě o faktu, že jednotlivé příspěvky jsou povětšinou vkládány bez aktivního přispění poskytovatele služeb, *content provideři* sami publikují své informace v prostoru, který jim ISP poskytuje. Tento způsob posuzování odpovědnosti tedy neodpovídal charakteru služeb ISP, naopak znamenal pro dotčené subjekty nespravedlivou zátěž.

Ke konci devadesátých let bylo již nad slunce jasné, že bez specifické právní úpravy se nelze obejít. Jednotlivé státy se tak soustředily na vytváření právních předpisů zaměřených již konkrétně na poskytování služeb prostřednictvím informačních technologií se zohledněním všech jejich charakteristických rysů. Trestněprávní odpovědnost ISP byla postupně omezena tak, jak ji konstruujeme dnes. Právní úprava se buď věnovala úpravě těchto služeb komplexně jako celku (např. Německo, Švédsko, Rakousko – zákony věnované poskytování telekomunikačních služeb), nebo upravovala odděleně jednotlivé oblasti, ve kterých se tyto aktivity mohly projevovat (kupříkladu USA – zákony na ochranu dětí na internetu, ochranu autorských práv na internetu apod.). Vnímání trestněprávní odpovědnosti ISP zvláště ze strany evropských států se následně promítlo v nám již dobře známé směrnici 2000/31/ES, kterou se řídíme v současnosti.[84]

Rozbor trestněprávní odpovědnosti dle české právní úpravy

Na základě získaných informací lze nyní přistoupit k vytvoření teoretické konstrukce, podle které bude možné odvozovat trestněprávní odpovědnost ISP v rámci českého právního řádu. Při posuzování naplnění skutkové podstaty trestného činu je nejprve nutno zhodnotit, zda vůbec máme způsobilý subjekt (viz náležitosti subjektu uvedené výše). Odpovíme-li si na první otázku kladně, můžeme se posunout k další složce skutkové podstaty a tou je objektivní stránka, tj. v čem spočívá závadné jednání onoho subjektu.[85] Vodítko nám poskytuje výklad klíčových paragrafů zákona č. 480/2004 Sb. ve spojení s ustanoveními trestního zákoníku. V případě ISP prvního typu tak z §3 zákona č. 480/2004 Sb. jasně vyplývá, že trestněprávní odpovědnost může založit pouze fakt, že se ISP v souvislosti s předmětnou informací nějakým způsobem aktivně angažuje.[86] Šlo by tedy o závadné konání komisivní a na základě jeho charakteru by bylo následně hodnoceno postavení ISP vůči hlavnímu pachateli, *content providerovi* (podrobně bude rozebráno v následujících odstavcích).

83 Anglickou verzi tohoto rozsudku s komentářem Christophera Kunera naleznete zde: KUNER, C. *Judgment of the Munich Court in the "CompuServe Case" (Somm Case)* [online]. vyd. 15. 07. 2010 [cit. 2010-03-05] Dostupné z: <http://www.kuner.com/data/reg/somm.html>.

84 Více k problematice historického vývoje lze nalézt v tomto článku: SIEBER, U. Responsibility of Internet Providers – a Comparative Legal Study with Recommendations for Future Legal Policy. *Computer Law & Security Report.* 1999, roč. 15, č. 5, s. 291 – 310.

85 Tento na první pohled zmateně zpřeházený postup je ve skutečnosti logický a časově úsporný. Nejprve je nutno říci zdali vůbec mohla osoba čin spáchat. Následuje zhodnocení, zda je předmětná aktivita označitelná za trestnou, zda vůbec jde o závadné jednání. Pokud máme způsobilý subjekt, který jednal protiprávně, musíme určit, zda vůbec byl resp. mohl být určitý právní zájem narušen (tedy objekt). Až jako na poslední nahlížíme na osobní postoj subjektu k dané situaci, tedy stránku subjektivní. V každém bodě může být proces přerušen zápornou odpovědí, čímž k naplnění skutkové podstaty trestného činu nedojde.

86 Ustanovení §3 z. č. 480/2004 Sb.: *„Poskytovatel služby ... odpovídá za obsah přenášených informací, jen pokud přenos sám iniciuje, zvolí uživatele přenášené informace, nebo zvolí nebo změní obsah přenášené informace."*

Právní úprava *cachingu* již uvádí situaci složitější. Zatímco u ustanovení §4 písm. a) předmětného zákona se jedná opět o komisivní konání (změna obsahu přenášené informace), v následujících případech jde již o nekonání, tedy o omisi upravenou v §112 NTZ.[87] K tomu, aby tedy vůbec mohlo k omisivnímu konání dojít, musí existovat nějaká primární povinnost subjektu nějak jednat. Podmínky přístupu k informacím (§4 písm. b) zákona č. 480/2004 Sb.) jsou ve většině případů upraveny smluvně v rámci vztahu poskytovatele služeb a spotřebitele. Složitější argumentaci by již bylo nutno použít u písmen c) a d) předmětného paragrafu, která odkazují na *„pravidla používaná v příslušném odvětví,* "která nelze přímo označit za právní předpis resp. úřední rozhodnutí. Přesto na ně zákon č. 480/2004 Sb. přímo odkazuje, čímž zdůrazňuje jejich význam pro dané odvětví i pro právo samotné. Autorka se tedy osobně domnívá, že ač povaha těchto pravidel neodpovídá zákonnému požadavku §112 NTZ, lze jejich respektování ze strany zákona o některých službách informačních společností přijmout za pádný důvod pro zařazení mezi právní normy, které by mohly založit povinnost zmiňovanou v §112 NTZ. Druhou otázkou však zůstává zhodnocení zásady subsidiarity v trestním právu (§12 odst. 2 NTZ). Dle této zásady lze trestní odpovědnost pachatele a trestněprávní důsledky s ní spojené uplatňovat jen v případech společensky škodlivých, ve kterých nepostačuje uplatnění odpovědnosti podle jiného právního předpisu. Dalo by se tedy diskutovat o tom, zda porušení výše uvedených pravidel skutečně musí vyvolat trestněprávní důsledky, nebo zda by postačil postih např. v rámci správního trestání apod.

Právní úprava *hostingu* je pak z hlediska trestního práva tou nejkomplikovanější. V §5 zákona č. 480/2004 Sb. je totiž zohledněna nejen objektivní stránka trestného činu, ale i stránka subjektivní. Ustanovení odstavce 1 písm. b) opět umožňuje vyvodit trestněprávní odpovědnost za omisivní jednání – v tomto případě přímo stanovuje povinnost zasáhnout proti závadnému obsahu, pokud se ISP o něm prokazatelně dozvěděl (jde tedy o právní předpis dle §112 NTZ). Pokud tedy poskytovatel služeb tuto povinnost nesplní, naplní objektivní stránku skutkové podstaty trestného činu. V ustanovení §5 písm. a) pak nalezneme odkaz na subjektivní stránku trestného činu, čili na fakt, zda ISP věděl resp. mohl vědět, že je obsah ukládaných informací protiprávní. Zde pak přichází na řadu zhodnocení, jestli lze předmětné jednání označit za úmyslné či nedbalostní. Pochopitelně ve většině případů nedochází ze strany ISP k tolerování trestné činnosti s vyloženým úmyslem tuto činnost podpořit (jak upravuje ustanovení §15 odst. 1 NTZ). Nová právní úprava trestního zákoníku však přinesla v tomto kontextu významnou změnu, kdy jako úmysl hodnotí i smíření pachatele s tím, že způsobem uvedeným v trestním zákoně může porušit nebo ohrozit zájem chráněný takovým zákonem (viz §15 odst. 2 NTZ). Z toho tedy vyplývá fakt, že i situace, kdy ISP „něco tuší" a z nějakého (byť i ve své podstatě nevinného) důvodu nezasáhne, je dle NTZ chápána jako úmyslné zavinění, což může mít dalekosáhlé následky.[88]

Pokud je ISP shledán trestně odpovědným, vyvstává otázka, v jaké pozici vůči pachateli by se mohl ocitnout. Trestní zákoník dává buďto možnost přiznat mu roli spolupachatele nebo roli účastníka na trestném činu. Podle ustanovení §23 NTZ se spolupachatelství vyznačuje úmyslným společným jednáním více osob. Taková konstrukce je však založena na komisivním cíleném jednání těchto osob, kde je nezbytná určitá intenzita vůle spáchat trestný čin, což nekoresponduje s předmětným chováním ISP, které spíše spočívá v tolerování nepravostí páchaných *content providerem*. Pravděpodobnější tedy je, že by ISP byl postaven do pozice účastníka na trestném činu, konkrétně pomocníka, jak jej upravuje ustanovení §24 odst. 1 písm. c) NTZ, za to, že pachateli umožnil nebo usnadnil spáchání trestného činu zajištěním prostoru na internetu nebo zprostředkováním přístupu k němu. Ať tak či tak, na stanovení rozhraní trestní sazby by určení postavení ISP nemělo vliv – pro obě dvě situace užívá trestní zákoník ustanovení o trestní odpovědnosti a trestnosti pachatele samotného. Vzhledem ke specifické povaze aktivit ISP by však soud pravděpodobně využil svého moderačního práva a po zhodnocení materiální stránky trestného činu by volil pro poskytovatele služeb sazbu poněkud nižší.[89] Jak ale bylo již několikrát zdůrazněno výše, závisí velmi na posouzení individuálních okolností každého případu stejně jako na osobnosti soudce – jeho vybavenost nejen právnickými ale i technickými znalostmi problematiky sehrává mnohdy určující roli v celém případu.[90]

Na základě získaných poznatků lze obecně shrnout, že ISP není ze zákona odpovědný, pokud obsah informací nijak nemodifikuje, neovlivňuje proces komunikace těchto informací a dodržuje předepsané technické postupy (ISP prvního a druhého typu) a dále pokud nemohl mít povědomosti o jejich protiprávním charakteru (ISP třetího typu). Právě pro služby typu *hostingu* je tedy z hlediska založení odpovědnosti důležitý onen moment získání povědomosti o protiprávním charakteru dané informace. Od tohoto bodu se již nelze ze strany ISP třetího typu zaštiťovat vyloučením odpovědnosti, a pokud ISP nepodnikne ihned kroky směřující k odstranění nebo znepřístupnění vadného obsahu, stává se trestněprávně odpovědnou v pozici pomocníka při trestného činu.[91] Tento důležitý moment je úzce spojen s anglickými pojmy *„notice"*, neboli oznámením o protiprávnosti, a *„takedown"*, tedy omezením nebo ukončením poskytování služeb. Polčák[92] poskytuje ve svém rozboru poměrně podrobnou analýzu, kdo a v jaké formě může *notice* poskytovateli služeb podat, aby mohl ISP adekvátně reagovat. Dle jeho závěrů může *notice* podat *de facto* kdokoli, přičemž nezáleží na tom, zdali jde přímo o po-

87 § 112 NTZ: *„Jednáním se rozumí i opomenutí takového konání, k němuž byl pachatel povinen podle jiného právního předpisu, úředního rozhodnutí nebo smlouvy, v důsledku dobrovolného převzetí povinnosti konat nebo vyplývala-li taková jeho zvláštní povinnost z jeho předchozího ohrožujícího jednání anebo k němuž byl z jiného důvodu podle okolností a svých poměrů povinen."*

88 Komentovaná úprava, konkrétně zákon 480/2004 Sb., působí při rozboru z pohledu trestního práva poněkud neúplně a neuměle. Je to především z toho důvodu, že nebyla primárně vytvořena k regulaci trestněprávní odpovědnosti. Má sloužit k úpravě odpovědnosti ISP jako celku, což nevyhnutelně znamená, že neodpovídá specifickým požadavkům z odvětví trestního práva, a její výklad je v mnohých částech složitý a „kostrbatý".

89 Autorka záměrně ve větě volí podmiňovací způsob. Řešení daného problému je totiž záležitostí výkladu platného práva, ve kterém se názory odborníků liší. Neexistuje ani relevantní česká judikatura, která by daný problém jednoznačně osvětlila, pohybujeme se tedy na poli teoretických úvah inspirovaných teorií a judikaturou zahraniční.

90 Jak ostatně dokazuje nám již známé rozhodnutí ve věci *CompuServe Deutschalnd GmbH.*

91 Tento závěr vzniká na základě následující konstrukce: od chvíle, kdy se subjekt dozví, že je jeho služeb využíváno k páchání trestné činnosti, a nic proti tomuto neučiní, svou pasivitou čin *de facto* podporuje a brání ukončení závadného stavu. To, že se na udržování tohoto protiprávního stavu svým postojem podílel, jej staví do role pomocníka.

92 Více viz POLČÁK, R. *Právo na internetu: Spam a odpovědnost ISP.* 1. vyd. Brno: Computer Press, a.s. 2007, s. 68 – 75.

škozeného či o osobu třetí.[93] Není ani předepsána konkrétní forma oznámení. Důležité je, aby se dalo říct, že se ISP o situaci skutečně dozvěděl, aby obdržel takovou sumu informací, na základě které by následně mohl podniknout příslušné kroky a která by tudíž zakládala i jeho trestněprávní odpovědnost. K protiprávní činnosti může docházet a také často dochází opakovaně. Další zásadní otázka tedy zní, zdali je nezbytné při opakujícím se deliktním jednání na tuto skutečnost znovu a znovu upozorňovat, nebo má ISP na základě prvního upozornění další protiprávní aktivitu monitorovat. Odpověď zčásti poskytuje již zákonné ustanovení vylučující povinnost ISP dohlížet na obsah jimi přenášených nebo ukládaných informací a aktivně vyhledávat skutečnosti a okolnosti poukazující na protiprávní obsah informace (§6 zákona č. 480/2004 Sb.). Na druhou stranu tento zákon v ustanovení §5 odst. 1 přímo uvádí, že ISP jsou odpovědni nejen v situaci, že jsou o závadném obsahu přímo zpraveni, ale i v případě, že o protiprávnosti dané informace vzhledem k okolnostem a povaze své činnosti vědět mohli. Pokud je tedy vzhledem okolnostem jasné, že daný subjekt bude v protiprávní činnosti pokračovat, může to založit povinnost ISP jeho aktivity monitorovat, pokud se chce vyhnout odpovědnosti. Záleží pochopitelně na individuálním posouzení celého případu a subjektivních možnostech poskytovatele služeb, i když, jak je jasně vidět, jde mnohdy o tanec na velmi tenkém ledě. Teoreticky není v této konstrukci žádný háček, praxe však přináší další problém. Tím je otázka, jak lze v konkrétním případě před soudem prokázat, že ISP ono předmětné upozornění skutečně obdržela. Pokud totiž zasílá *notice* běžný uživatel, prakticky neexistuje způsob, jak věrohodně prokázat poskytovateli služeb obdržení zprávy a tudíž i získání povědomosti o závadném obsahu, na který *notice* upozorňuje. V o mnoho lepším postavení není ani úřední orgán. Může sice zvolit obecně nejsnadněji prokazatelné doručení formou poštovní zásilky, musíme si však uvědomit, že takové upozornění není ze své podstaty úřední zásilkou, kterou by bylo nutno doručit do vlastních rukou. Proto se lze vždy účinně ohrazovat argumentem, že zásilka nebyla doručena do rukou odpovědné osoby a tato se tak nemohla dozvědět o závadném obsahu, na který byla upozorňována. Zde tedy opět nesmíme zapomínat, že i když teorie praví jedno, konečné slovo mívá ve většině případů soud, kde hrají roli skutečně a nevyvratitelně prokázané skutečnosti, takže výsledek může být značně odlišný od teoreticky předpokládaného.

> Nejčerstvějším případem, který doslova zdvihl ze židle odbornou veřejnost, je necelé čtyři měsíce staré rozhodnutí prvoinstančního soudu v Miláně týkající se světoznámé společnosti *Google, Inc.*[94] Dne 24. února 2010 rozhodl milánský soudce Oscar Magi o vině čtyř vedoucích pracovníků společnosti *Google* – Davida Drummonda, George Reyese, Arvina Desikana a Petera Fleischera, kteří se podle něj dopustili trestného činu narušení soukromí, a odsoudil je tak k šesti měsícům trestu odnětí svobody s podmíněným odkladem. V roce 2006 umístila skupinka mladíků na portál *Google Video* záznam, na kterém týrají postiženého spolužáka. Chlapci se již zpovídali ze svého provinění před soudem pro mladistvé, otec týraného však společně s organizací zastupující postižené lidi podal trestní oznámení i na společnost *Google, Inc*. pro narušení soukromí jeho syna tím, že závadný obsah včas neodhalili a nezabránili jeho zveřejnění.
> Video bylo na *Google* umístěno dne 8. září 2006 a zůstalo volně přístupné až do 7. listopadu 2006, tedy plné dva měsíce. Podle tvrzení obžaloby vedené státním zástupcem Alfredem Robledem společnost *Google, Inc.* nezareagovala dostatečně rychle, protože tato doba je dostatečně dlouhá na to, aby ISP sám zjistil závadný obsah, což by měla být jeho povinnost. Obvinění se pochopitelně hájili tím, že není jejich zákonnou povinností vyhledávat závadný obsah a že jednali naprosto zodpovědně, jelikož jakmile obdrželi upozornění od italské policie, předmětné video odstranili. Splnili prý tak povinnost uloženou zákonem. Toto tvrzení však vyvrátila obžaloba pádným argumentem, že upozornění ze strany policie bylo až několikáté v pořadí – jako první zaslalo svou notice několik běžných uživatelů *Google Video*, kteří předmětný materiál shlédli na internetu. *Google, Inc.* na tyto *notice* neregovala, čímž se stala odpovědnou, a její reakce na výzvu policie o měsíc později již nemohla změnit nic na faktu, že video bylo na internetu umístěno s jejím vědomím. Soud dal nakonec obžalobě za pravdu, a protože italské právo nezná trestněprávní odpovědnost právnických osob, označil za odpovědné výše uvedené vrcholné managery. Tito jsou rozhodnuti podat odvolání, postupný vývoj kauzy tedy můžeme sledovat v nejbližších letech.[95]

Předmětný rozsudek rozvířil živou diskusi o skutečné svobodě internetu a odpovědnosti ISP za obsah informací, jejichž šíření umožňují. Úplné znění rozsudku stále ještě nebylo publikováno, jeho odůvodnění tak můžeme pouze dovozovat z doposud zveřejněných vyjádření Alfreda Robleda, která argumentují především ochranou lidských práv, která svým významem přesahuje obchodní zájmy ISP. Odborná diskuse směrovaná podobnými argumenty se tak

93 Vztah oznamovatele k vadnému obsahu je tedy irelevantní. U trestné činnosti ani mnohdy není možné jej posuzovat, protože je často poškozován právní zájem neohraničeného okruhu osob (např. u šířením dětské pornografie apod.).

94 Oficiální znění rozsudku nebyklo bohužel doposud publikováno, není proto prozatím možné zjistit jeho číslo.

95 Více informací včetně komentářů odpůrců rozhodnutí lze nalézt např. zde:
PISA, N. *Google Italy ruling 'threat to internet freedom'* [online]. vyd. 24. 02. 2010 [cit. 2010-03-05]. Dostupné z: <http://www.telegraph.co.uk/technology/google/7308384/Google-Italy-ruling-threat-to-internet-freedom.html>.
DHAVA, D. *Google Execs Convicted In Italian Abusive Video Case* [online]. vyd. 25. 02. 2010 [cit. 2010-03-05]. Dostupné z: <http://news.ebrandz.com/google/2010/3155-google-execs-convicted-in-italian-abusive-video-case.html>.
VŠETEČKA, R. *Průlomový verdikt. Šéfové Googlu nesou vinu za video na internetu* [online]. vyd. 24. 02. 2010 [cit. 2010-03-05]. Dostupné z: <http://technet.idnes.cz/prulomovy-verdikt-sefove-googlu-nesou-vinu-za-video-na-internetu-1cj-/sw_internet.asp?c=A100224_135248_sw_internet_vse>.

přesouvá k řešení otázek, zdali je či není svoboda internetu ohrožena, jestli došlo či nedošlo ze strany *Google* k neoprávněnému zásahu do lidských práv, které hodnoty stojí obecně v hierarchii nejvýše a zasluhují tak přednost před ostatními a podobně. Obecně se však jedná o otázky, na které nelze najít jednoznačnou odpověď a které vždy budou tvořit živnou půdu pro spory a kontroverze. Tyto otázky však odvádějí pozornost poněkud stranou od těžiště celého případu, které se dle názoru autorky nachází jinde. Nelze přeci s jednoznačnou platností říct, kdo a jak porušil či neporušil lidská práva a do jaké míry je tak povinen nést odpovědnost. Vždy bude možné vytvořit jinou teorii, která první tvrzení vyvrátí, přičemž ani o jedné nelze říct, že je stoprocentně správná. Oproti tomu naprosto nevyvratitelné je založení odpovědnosti na základě faktu, že daná ISP získala povědomí o tom, že umožňuje sdílení informací s nežádoucím obsahem, a to dokonce několikrát, přesto nereagovala a vědomě tak porušování zákona podpořila. Dle názoru autorky je toto stěžejním argumentem pro uznání spoluodpovědnosti společnosti *Google, Inc.* za škody, které předmětné video napáchalo, přičemž diskuze o ochraně lidských práv a významu jednotlivých hodnot v rámci obecné hierarchie tuto argumentaci spíše dokresluje. Rozhodnutí ve věci *Google, Inc.* ve skutečnosti nijak výrazně kontroverzní není. Jeho výjimečnost spočívá spíše v tom, že je nové a zabývá se skutečnostmi, které až doposud nebyly otevřeně diskutovány. Ukazuje však na nově nastupující trend zvyšování nároků kladených na poskytovatele služeb informačních společností, podobných kauz tak v budoucnosti bude přibývat.

6 Realizace pravomocí státních orgánů blokovat či odpojovat komunikační linky

Nyní bychom na základě předchozího rozboru měli být schopni definovat počítačový trestný čin, nalézt autoritu, která má pravomoc tento čin stíhat a označit osobu, jež bude za delikt zodpovědná. Otázkou zůstává, jak co nejúčinněji odstranit nebo zmírnit následky protiprávního jednání pachatele. Předem je třeba říci, v čem vlastně tyto následky, jak s nimi bude nadále kalkulováno, spočívají. V řadě případů pochopitelně ono porušení (či ohrožení) chráněného zájmu vzniká již momentem vzniku předmětné informace (např. u pořizování dětské pornografie), pokud se ale bavíme o šíření závadných informací prostřednictvím informačních technologií, nachází se jádro problému v aktu zveřejnění této informace, tj. ve faktu, že tato informace svou přístupností může nějakým způsobem působit na třetí osoby a tím narušovat buď obecně veřejný zájem, nebo zájem jednotlivce resp. skupiny osob. V následujících odstavcích tedy půjde konkrétně o to, jak efektivně zajistit, aby závadná informace svou existencí a všeobecnou přístupností nadále nepoškozovala právní zájmy třetích osob a veřejný zájem jako celek – tudíž o to, jak ji zablokovat. Autorce v tomto případě nejde o rozbor problému z technického hlediska, cílem je nastínit základní otázky procesního charakteru a pokusit se nalézt adekvátní řešení.

Pro zjednodušení lze vytvořit tři pracovní modelové situace. V prvním případě půjde o zablokování přístupu *ad hoc.* Existuje zde tedy konkrétní *content provider*, konkrétní závadná informace navozující negativní stav a z ní vyplývající nutnost tento stav ukončit a zajistit předmětné informace pro účely trestního řízení. Nejde zde tedy ani tak o potrestání pachatele, jako o rychlý a účinný zákrok směřující k odstranění nebo zmírnění následků jeho protiprávního jednání.[96] Ve druhé situaci již má blokování kromě funkce preventivní (ve vztahu k eventuálnímu dalšímu protiprávnímu jednání pachatele) i povahu sankce. Jde o celkové omezení přístupu směřované vůči osobě pachatele. Konkrétní subjekt, vůči kterému je akt zablokování přístupu uplatněn, tedy zůstává, nejde již však o jeden konkrétní závadný soubor informací, který je zablokován, ale o částečné či úplné odpojení od přístupu ke všem informacím, nehledě na jejich charakter a obsah. Ve třetí situaci je to obráceně – okruh omezovaných osob není určitý a přístup je zablokován ke konkrétně definovaným informacím.

6.1 Blokování ad hoc

Jak bylo již uvedeno v předchozím odstavci, spočívá první modelová situace v uskutečnění rychlého a účinného zákroku směřujícího k odstranění nebo zmírnění následků protiprávního jednání pachatele, přičemž tento zákrok míří vůči konkrétnímu souboru informací a konkrétnímu *content providerovi*, který tento soubor zveřejňuje. Nejedná se tedy již o pouhé upozornění, které může založit spoluodpovědnost ISP (viz *notice&takedown* postup výše), ale o přímý příkaz orgánu, který je vynutitelný sám o sobě. Tuto problematiku se autorka rozhodla řešit speciálně z pohledu českého práva, protože právě zde v současnosti přetrvává řada palčivých otázek bez adekvátních odpovědí.

Pro začátek je nezbytné si uvědomit, s jakým typem úředního postupu se vlastně chystáme pracovat a jaké právní předpisy jsou pro něj závazné. Akt autoritativního zablokování nezákonného obsahu na internetu spadá svým charakterem mezi tzv. zajišťovací úkony v trestním řízení. Provádění těchto úkonů má za úkol zajistit přítomnost osob, věcí či jiných hodnot důležitých pro trestní řízení a tím umožňovat jeho hladký průběh. V našem případě je zajišťovanou hodnotou určitá suma informací. Jelikož jde v případě zajišťovacích úkonů o poměrně výrazný autoritativní zásah do osobních práv jedince, je naprosto nezbytné, aby byl takový postup odpovídajícím způsobem podpořen zákonem. V České republice je trestní řízení upraveno trestním řádem,[97] jak jsme jej již zmiňovali v předchozí kapitole věnované právní úpravě.

Zajišťovací úkony jsou upraveny v Hlavě čtvrté trestního řádu. Studiem předmětných ustanovení §§ 67 – 88a TŘ však docházíme k poměrně alarmujícímu závěru, a totiž že institut autoritativního zásahu proti nelegálnímu obsahu na internetu

96 Mohli bychom tedy říct, že blokování dané informace má zde funkci reparační a do jisté míry i preventivní.

97 Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád) ve znění pozdějších předpisů.

není doposud českým právem upraven. Hlava čtvrtá zahrnuje, jak již ostatně sám její název napovídá, zajištění osob, věcí a jiných majetkových hodnot, zajištění dat, jak o nich hovoříme v našem případě, však mezi těmito výslovně upraveno není. Jisté řešení bychom se mohli pokusit najít v uplatnění *analogie legis*, kterou, na rozdíl od trestního práva hmotného, trestní právo procesní v zásadě připouští. Konstrukčně nejlépe našemu požadavku odpovídá institut zajištění peněžních prostředků na účtu u banky, jak je upravuje ustanovení §79a TŘ. Podle tohoto ustanovení provede banka zajištění peněžních prostředků, u kterých je podezření, že jsou nebo byly určeny ke spáchání trestného činu nebo jsou jeho výnosem. Toto zajištění je banka povinna provést na základě rozhodnutí soudce resp. státního zástupce či policejního orgánu v přípravném řízení. Podobnost lze tedy nalézt v onom trojúhelníku rozhodující orgán – subjekt spravující určité hodnoty pro pachatele resp. podezřelého – pachatel resp. podezřelý sám. Při uplatňování analogie v trestním řízení však musíme zohlednit ještě jednu velice zásadní skutečnost, tou je charakter práv subjektu, do kterých je trestním řízením zasahováno. A právě u zajišťovacích úkonů dochází k zasahování do práv základních, zaručených Listinou základních práv a svobod i mezinárodními smlouvami, kterými je náš stát vázán. Do těchto práv je možné autoritativně zasahovat pouze a jedině v zákonem konkrétně taxativně stanovených případech a žádný alternativní výklad není možný. Přímo z povahy předmětných ustanovení tedy vyplývá výjimka z použití *analogie legis*, která tuto bezvýhradně vylučuje. Cestou analogie tak nelze využívat předmětná ustanovení trestního řádu na případy, které v nich nejsou výslovně uvedené.

Tímto rozborem docházíme k velmi zásadnímu závěru, a totiž že v našem právním řádu existuje „legislativní díra", která významně znesnadňuje orgánům činným v trestním řízení jejich postup proti páchání trestného činu. Neexistence odpovídajících ustanovení v trestním řádu nutí proto tyto orgány hledat často vysloveně neudržitelná řešení a pomáhat si širokým výkladem dostupných ustanovení. V současnosti tak orgány činné v trestním řízení vyžadují spolupráci ISP na základě ustanovení §8 odst. 1 TŘ, podle kterého jsou právnické a fyzické osoby povinny vyhovovat dožádáním orgánů činných v trestním řízení.

Použití tohoto ustanovení je však extrémně problematické. Jednak jej lze obecně užít pouze v rámci již započatého trestního řízení, musí již tedy být minimálně sepsán záznam o zahájení úkonů trestního řízení, jak to vyžaduje §158 odst. 3 TŘ. Další problém tkví v samotném charakteru institutu součinnosti poskytované na základě dožádání. Pro výklad chápání pojmu součinnosti se obraťme do dalšího právního předpisu používaného v rámci trestního řízení – do vyhlášky č. 37/1992 Sb. Ministerstva spravedlnosti České republiky, o jednacím řádu pro okresní a krajské soudy, ve znění pozdějších předpisů. Z jednotlivých odstavců ustanovení §28 předmětné vyhlášky získáme demonstrativní výčet činností, které jsou chápány jako poskytování součinnosti. Jedná se např. o *„sdělování skutečností, které mají význam pro soudní řízení a rozhodování* (zde dokonce nalezneme přímý odkaz na §8 TŘ) … *zprávy o chování, majetkových a sociálních poměrech obviněného a účastníků řízení, zprávy o tom, zda odsouzený řádně vykonává trest obecně prospěšných prací, a zprávy o poměrech mladistvého, které mají podklad ve vlastních poznatcích těchto orgánů … zprávy o chování obviněného a účastníků řízení, o chování podmíněně odsouzeného a podmíněně propuštěného z výkonu trestu odnětí svobody ve stanovené zkušební době a o chování odsouzeného pro účely rozhodnutí o zahlazení odsouzení a o pobytu a zaměstnání osob apod.* Z tohoto výčtu jasně vyplývá, že dožádání se běžně používá, pokud chceme získat jistou informaci či vyjádření k dané problematice. Pokud s tímto porovnáme náš požadavek – aby určitá osoba zasáhla do výkonu cizích práv – zjistíme, že je toto ustanovení pro nás absolutně nevhodné a jeho využití je možné pouze na základě účelového výkladu, který v trestním právu nemá své místo.

Dalším předpisem, o který se lze *de lege lata* opřít, je zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů. V Hlavě IV věnované spolupráci nalezneme ustanovení §18, dle kterého je policista v rozsahu potřebném pro splnění konkrétního úkolu oprávněn požadovat od fyzických a právnických osob věcnou a osobní pomoc, zejména potřebné podklady a informace včetně osobních údajů. Tyto orgány a osoby jsou až na výjimky povinny požadovanou pomoc poskytnout. Zde opět musíme objektivně zhodnotit, jaké povinnosti jsou zahrnuty pod pojmy „spolupráce" resp. „pomoc". Již demonstrativní výčet v ustanovení §18 nám napovídá, že „pomoc" ve smyslu tohoto zákona fakticky odpovídá pojmu „součinnost" probíranému o odstavec výše. Pochopitelně je zde možný mnohem širší výklad, který zahrnuje i aktivní fyzické přispění policistovi při plnění jeho úkolů, autorka je ale přesvědčena, že rozšíření až směrem k ukládání povinnosti zasahovat do cizích ústavně zaručených práv je absolutně neudržitelné. Tento zásah do subjektivních práv je sám o sobě natolik závažný, že jeho přikázání pouze z rozhodnutí výkonného orgánu a bez přispění soudu může být dokonce shledáno jako protiústavní. Právě proto je u všech zajišťovacích institutů v trestním řádu jasně stanoven požadavek, aby o předmětném zásahu rozhodl soud, a ne výkonný orgán činný v trestním řízení samostatně.

Z výše uvedeného je jasně vidět, že *de lege lata* nemáme adekvátní prostředky, jak vzniklou mezeru v zákoně zaplnit. Problém nám tak vyvstává i při vymezení institutů navazujících. Klademe si tak otázku, jak lze výše popsanou součinnost resp. pomoc vymáhat, a zdalipak pokud orgány činné v trestním řízení vyzvou dotčenou ISP k blokování závadného obsahu na základě výše uvedených ustanovení a ona jim odmítne vyhovět, ji mohou za toto nějakým způsobem sankcionovat.

Ač je tento výraz obecně používán s velkou oblibou, český právní řád nezná pojem „maření vyšetřování" či „maření trestního řízení" apod. Trestní zákoník sice v ustanovení §337 upravuje maření výkonu úředního rozhodnutí, pro naplnění skutkové podstaty však požaduje jednak komisivní jednání (přičemž při nezablokování nezákonného obsahu jde o omisi) a jednak podklad v podobě úředního rozhodnutí (dožádání za takové rozhodnutí považovat nelze). Náš právní řád tedy nezná odpovídající způsob, jak donutit dožádané osoby, aby s orgány činnými v trestním řízení spolupracovaly. V našem případě je tak jediným použitelným nátlakovým prostředkem uplatnění obecného principu odpovědnosti ISP, jak o něm bylo pojednáno v předchozích kapitolách. Pokud by tak ISP odmítla na výzvu policie zareagovat, mohla by být stíhána pro napomáhání trestnému činu. Odvrátíme-li se však od teorie směrem k realitě, zjistíme, že v praxi na řešení těchto otázek ani nedochází. Policie si je totiž vědoma nebezpečí zákonného nebo dokonce ústavního konfliktu, který by mohl v souvislosti s použitím výše uvedených ustanovení vzniknout, a proto

sahá k tomuto typu příkazu jen velmi obezřetně. To ovšem znamená, že jsou její možnosti v tomto směru značně oklestěny a tento stav je vzhledem k současnému vývoji kyberkriminality prakticky neudržitelný.[98]

Na základě závěrů uvedených v předchozích odstavcích se autorka domnívá, že ve vztahu k této problematice neexistuje jiné adekvátní řešení, nežli urychlená změna současné legislativy, která bude zohledňovat jak věcný záměr nového trestního zákoníku, tak poznatky ze současné vyšetřovací praxe. Není žádoucí, aby možnost autoritativně nařídit blokování závadného obsahu zůstávala nadále upravena pouze v rovině obecného oprávnění, protože tento úkon svým charakterem odpovídá úkonům zajišťovacím, při kterých je nezbytné postupovat dle zákonem přesně stanovených pravidel tak, aby nebyly ohroženy zákonem a Listinou chráněná práva a svobody dotčených subjektů. Otázkou pro odbornou diskusi zůstává, o jak vážný zásah do práv subjektu se ze strany orgánů činných v trestním řízení jedná, a tudíž i které orgány činné v trestním řízení se na tomto procesu musí svým souhlasem resp. dozorem podílet.[99] Zohledníme-li věcný záměr nového trestního zákoníku a i rostoucí podíl kyberkriminality na celkové sumě trestných činů, stojí též za úvahu, zda by nebylo možné předmětná ustanovení naformulovat do obecnější roviny tak, aby byla použitelná na veškeré zajišťovací úkony v rámci kyberprostoru jako celek. Vyhnuli bychom se tak vytváření dalších „legislativních děr", jejichž vznik prudký rozmach informačních technologií nepochybně zapříčiní. Na druhou stranu je nutné podotknout, že vytvoření takového ustanovení by vyžadovalo naprosto precizní formulaci, která by v sobě dokázala obsáhnout všechny aspekty spojené s tímto typem kriminality, což nemusí být reálně dosažitelné.

V návaznosti na změny zavedené prostřednictvím NTZ v současné době vzniká návrh nového kodexu trestního práva procesního. Autorka měla možnost nahlédnout do pracovní paragrafové osnovy tohoto dokumentu. Ačkoli návrh přináší do oblasti trestního práva procesního řadu velmi zásadních změn, v řešení otázek sledovaných touto prací bohužel k žádnému výraznému posunu nedochází. Zajištění se v novém návrhu týká pouze osob, věcí, jiných majetkových hodnot a nově i majetku. Data v podobě informací se závadným obsahem nejsou do této skupiny zahrnuta a jejich zajištění tak zůstává opět neupraveno. Bohužel to tedy vypadá, že ani do budoucna se zákonodárce nehodlá touto poměrně zásadní mezerou v právní úpravě zabývat a že orgány činné v trestním řízení tak budou nadále ponechány v současné nejisté pozici.

6.2 Blokování na základě principu stupňovité odezvy

Stěžejním pojmem objevujícím se ve druhém případě je tzv. stupňovitá odezva,[100] česky někdy vyjadřovaná spojením „třikrát a dost". Na základě uplatnění tohoto principu je osoba dopouštějící se opakovaně závadného jednání dvakrát za sebou na protiprávní charakter své činnosti upozorněna. Pokud v porušování práva pokračuje, dojde na základě autoritativního rozhodnutí k odstřižení této osoby od internetového připojení. Podle předmětného rozhodnutí nesmí být této osobě poskytnuto připojení ani od jiného poskytovatele služeb informační společnosti, a to až na dobu jednoho roku. Tento postup je prozatím uplatňován výhradně ve spojení s ochranou před porušováním autorských práv, kdy umožňuje poškozenému autorovi domáhat se svých práv účinněji nežli prostřednictvím zdlouhavého procesu v rámci civilního soudnictví. Autor sám je většinou zastupován konkrétní státem pověřenou institucí, která komunikuje s osobou porušující autorská práva prostřednictvím výše zmíněných upozornění. Tato instituce je zároveň hlavním iniciátorem procesu odpojení porušitele od informačních služeb (i když, jak si vysvětlíme níže, nemůže být tím orgánem, který o zásahu práv ve formě odpojení závazně rozhodne). Tento správní postup zdánlivě s trestním právem nesouvisí, nesmíme však zapomínat na jeho faktické důsledky – porušování práva je tímto způsobem efektivně ukončeno a do budoucna je poměrně účinně omezeno. Nic tak nebrání tomu, aby tento proces probíhal souběžně s trestním řízením pro trestný čin porušování autorských práv, nebo aby toto řízení účinně navazovalo.

V současnosti bezkonkurenčně nejznámější a nejkontroverznější případ aplikace principu stupňovité odezvy je v rámci francouzského Aktu na podporu šíření a ochranu tvorby na internetu (fr. *Loi favoisant la diffusion et la protection de la création sur Internet*), který vešel v účinnost s novým rokem 2010. Tento zákon je obecně znám pod označením HADOPI resp. HADOPI2, a to podle nově založeného úřadu, který ochranou autorských práv pověřuje – podle Vysokého úřadu pro šíření děl a ochranu práv na internetu (fr. *Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet*, dále jen „Vysoký úřad"). Původní zákon označovaný prostě jako *HADOPI* byl dokončen na jaře roku 2009. Ve svých

98 Zde považuje autorka za nezbytné zdůraznit ještě jeden důležitý fakt, který z předchozího výkladu nemusí být zřejmý. Právo může vytvořit řadu různě účinných nástrojů, kterými lze donutit poskytovatele služeb k součinnosti, přesto musíme na základě poznatků z praxe konstatovat, že nejvýznamnější roli stále hraje dobrá vůle ISP a jejich ochota s orgány činnými v trestním řízení spolupracovat. Nesmíme proto podceňovat vlastní etické kodexy dotčených společností a význam, jaký hraje jejich vstřícnost a odhodlání bojovat se zločinem vlastními prostředky. Praktické zkušenosti bohužel dokazují fakt, že pokud tento pozitivní přístup ze strany ISP schází, může být řízení velice vážně zkomplikováno a v mnoha případech docela zmařeno.

Skutečný případ z policejní praxe:

Je poměrně běžné, že ISP pronajímá své IP adresy jiným subjektům. Následně dojde k situaci, kdy se nájemce IP adresy rozhodne poskytovat prostor jiným subjektům ve formě *hostingu*, přičemž jeden z jeho klientů vytvoří *phishingové* stránky a jejich prostřednictvím se dopouští závažné trestné činnosti.

Orgány činné v trestním řízení se obrátí na pronajímatele IP adresy s požadavkem, aby poskytla osobní údaje svého nájemce a předmětnou IP adresu zablokovala. V této situaci jde především o čas, protože s každou vteřinou může pachatel pomocí *phishingu* získávat citlivé osobní údaje svých obětí a dostat se tak k jejich finančním účtům. Dožádaná ISP je pochopitelně v nepříjemné pozici, protože zablokováním předmětné adresy znemožní fungování nejen pachateli, ale i svému nájemci, který s trestnou činností nemá v zásadě nic společného. Dožádaná ISP tak může jednat dvěma způsoby – v tom lepším policejnímu orgánu vyhoví a problematické stránky zablokuje ihned. Pokud se však rozhodne nespolupracovat (a ve skutečnosti se tak bohužel stává), může celý proces pozdržet až na dva dny. Zhruba tak dlouho totiž trvá vydání soudního nařízení dle §88a odst. 1 TŘ, na základě kterého je ISP povinna vydat informace o uskutečněném telekomunikačním hovoru. ISP pochopitelně může spolupracovat i bez tohoto nařízení, ale ze zákona je k tomu povinná až „s papírem v ruce". Kolik důvěřivých lidí se během těchto dvou dnů může stát a také stane obětí podvodníka si dokážeme snadno představit.

99 Například zadržet obviněného podle §75 TŘ může policejní orgán sám na základě pouze svého rozhodnutí. Je však povinen o provedeném zadržení ihned informovat státního zástupce. Oproti tomu o vzetí osoby, proti které bylo zahájeno trestní stíhání, do vazby může rozhodnout pouze soud a v přípravném řízení na návrh státního zástupce soudce. Při zadržení osoby jde o zbavení osobní svobody pouze na krátké přechodné období max. 48 hodin, není tedy nutné schválení soudu. Vazba oproti tomu může trvat nepoměrně déle, proto je pro tento případ nezbytný souhlas orgánu v hierarchii orgánů činných v trestním řízení rozhodujícího.

100 V angličtině tento pojem zní *„graduate response"*.

ustanoveních uděloval Vysokému úřadu pravomoc řídit proces uplatňování stupňovité odezvy a následně i rozhodnout o odpojení provinilce od přístupu k internetu. Tento zákon vyvolal bouřlivou vlnu nevole, protože *de facto* dával správnímu orgánu pravomoc rozhodovat o základních lidských právech,[101] což bylo až doposud vždy doménou soudů. Kontroverzní předpis se dostal až před francouzskou Ústavní radu a ta ve svém rozhodnutí č. 2009-580 DC ze dne 10. června 2010 označila svěření předmětné pravomoci Vysokému úřadu za protiústavní. Ústavní rada uznala internet jako jeden v současnosti nejvýznamnějších prostředků mezilidské komunikace a není tedy možné, aby omezení výkonu tak významného práva, jako je právo svobodně se vyjadřovat a komunikovat, spočívalo v rukou správního orgánu.

Na základě tohoto rozhodnutí byl návrh zákona přepracován a tato nová verze je nyní známa pod označení *HADOPI2*. Zákon nadále svěřuje Vysokému úřadu významné pravomoci, které lze v některých aspektech srovnávat s pravomocemi samotné policie. Snaží se tak dosáhnout usnadnění a zrychlení celého procesu a zajistit efektivní shromáždění důkazů potřebných v dalších zákonem předpokládaných krocích. První upozornění osobě porušující autorská práva má být zasíláno prostřednictvím e-mailu, druhé již ve formě úředního dopisu. Samotného rozhodnutí o odpojení má být dosaženo ve zkráceném řízení před samosoudcem, který bude vycházet z podkladů dodaných mu Vysokým úřadem.[102] Soudce bude rozhodovat na principu presumpce viny, to znamená, že důkazy předložené Vysokým úřadem resp. agenty velkých vydavatelských a distribučních společností jsou považovány za dostatečné, pokud se neprokáže opak.[103] Porušitel tak může být odpojen od přístupu k internetu na dobu 2 až 12 měsíců, přičemž má udělen zákaz pokoušet se dosáhnout připojení prostřednictvím jiného ISP. Z dikce tohoto předpisu jednoznačně vyplývá, že předpokládané odpojení je pouhou součástí celého trestního řízení s pachatelem trestného činu porušování autorských práv, ve kterém mohou být uděleny tresty buď peněžitého charakteru, nebo spočívající v různých dalších omezeních, včetně trestu odnětí svobody. Z toho se odvíjejí i předpokládané sankce za porušení zákazu připojení, které svým charakterem mají odpovídat sankcím za porušení soudního příkazu v „běžném" trestním řízení. Pokud není možné identifikovat osobu, která se porušování autorského práva dopustila, může soud stíhat i zřizovatele přípojky, jejímž prostřednictvím k takovému porušení došlo. Tento nemůže být pochopitelně obviněn z porušování autorských práv, za nedostatečné zabezpečení přípojky mu však hrozí odpojení až na jeden měsíc a peněžitý trest do výše 1500 €.[104] Důležité jsou také nároky kladené na osobu ISP. Poskytovatel je během řízení povinen nejen plně spolupracovat, ale provést i okamžité odpojení na základě rozhodnutí soudu. V případě, že by tuto povinnost nesplnil, hrozí mu sankce až do výše 3 750 €. Ústavní rada novou verzi zákona dne 22. října 2009 schválila a ten byl vyhlášen dne 29. října pod číslem 2009-1311.[105]

Stejně jako jeho předchůdce, i zákon *HADOPI2* vyvolal vlnu ostré kritiky. Odpůrci se především ohrazují proti, dle jejich názoru naprosto neadekvátním, zásahům do osobních práv jednotlivců i celých skupin osob, které mohou být předmětným odpojením postiženy. Argumentují mimo jiné i samotným charakterem internetu jako „prostředí pro novou formu bytí", jak jsme se jím ostatně zabývali již na začátku tohoto článku, přičemž dané rozhodnutí má toto „virtuální bytí" *de facto* zmařit. Právě kvůli významu komunikace prostřednictvím informačních technologií přináší značné obavy i zkrácení celého řízení před soudem, kdy je odpůrci namítáno ohrožení práva obviněného na řádnou obhajobu a spravedlivý proces jako celek. Proponenti nové právní úpravy naopak argumentují tím, že míra porušování autorských práv na internetu dosáhla již takové úrovně, že je nezbytné zaujmout specifická opatření, která zajistí alespoň částečnou paralyzaci rušivých elementů, což odpojení bezpochyby učiní. Otázkou však zůstává, zda nová právní úprava může obstát i při zohlednění principu proporcionality a tedy zda je takto výrazný zásah do lidských práv skutečně odpovídajícím řešením – to ukáže až čas a zkušenosti z budoucí praxe.

Obdobný systém se ve své zemi rozhodli zavést i britští zákonodárci prostřednictvím návrhu aktu s názvem *Digital Economy Bill.* Tento zákon byl schválen 8. dubna roku 2010 a po udělení královského souhlasu se stal součástí právního pořádku Velké Británie pod názvem *Digital Economy Act 2010* (dále jen „DEA"). Schvalování tohoto zákona provázela řada kontroverzí, už proto, že byl přijat poměrně narychlo v tzv. *wash-up period*, tedy v posledních dnech funkčního období britského parlamentu, kdy se odcházející politici snaží „uklidit stůl" a dokončit rozpracované projekty, včetně urychleného schvalování doposud otevřených návrhů zákonů. Ve zkratce lze říci, že tento akt výrazně posiluje pravomoci britského Komunikačního úřadu (angl. *Office of Communication*, dále jen „OFCOM") – nezávislé instituce mající za úkol regulovat telekomunikační trh a hospodářskou soutěž v jeho rámci. Zároveň však také přináší nové povinnosti pro ISP, které mohou způsobit velkou změnu v charakteru poskytování těchto služeb.

Na základě ustanovení článku 124A DEA je povinnost zaslat upozornění porušiteli práv svěřena ISP, který danému subjektu poskytuje předmětné služby. Toto upozornění je formulováno podle oficiální zprávy zaslané ISP samotným autorem, jehož práva byla porušena. Tato zpráva (angl. *copyright infringement report*) musí splňovat předepsané náležitosti, aby mohla být dále předána porušiteli společně s přesně formulovaným upozorněním (opět předepsáno zákonem). ISP má zároveň povinnost vytvořit a vést speciální seznam porušení autorských práv (angl. *copyright infringement list*) a v něm veškeré záznamy umožňující identifikaci porušitele a podrobnosti týkající se jeho protiprávních aktivit. Poškozený autor

101 Jde především o práva uvedená v článku 27 Všeobecné deklarace lidských práv z roku 1948:

1. Každý má právo svobodně se účastnit kulturního života společnosti, užívat plodů umění a podílet se na vědeckém pokroku a jeho výtěžcích.
2. Každý má právo na ochranu morálních a mediálních zájmů, které vyplývají z jeho vědecké, literární a umělecké tvorby.

102 V reálu půjde o informace dodané úřadu agenty velkých vydavatelských a distribučních společností, na jejichž základě začne úřad jednat.

103 Uplatnění tohoto principu je značně kontroverzní. Znamená totiž, že pokud obviněný s obviněním nesouhlasí, musí sám prokázat svou nevinu. Prvoinstanční řízení však probíhá za nepřítomnosti obviněného, prokázání neviny je tak možné až v rámci odvolacího řízení. Oponenti zákona tak argumentují závažným porušováním práva na spravedlivý soudní proces, jemuž tento postup skutečně může odporovat.

104 Ve svém článku se k tomuto tématu vyjadřují i autoři Gřivna a Herczeg. Viz HERCZEG, J. – GŘIVNA, T. Právo na přístup k Internetu, blokace stránek a digitální gilotina. *Trestněprávní revue.* 2010, roč. 9, č. 4, s. 2 – 3.

105 Celé oficiální znění zákona ve francouzském jazyce lze najít na těchto stránkách: Loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet [online]. [cit. 2010-03-05]. Dostupné z: <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021208046&dateTexte>.

si může relevantní údaje z tohoto seznamu kdykoli vyžádat a použít je k prosazení svých práv.

Návrh zákona následně dává odpovědnému ministrovi pravomoc, kdykoli ve spolupráci s OFCOMem vytvořit soubor technických pravidel, na základě kterých by poskytovatelům služeb informačních technologií mohla být uložena povinnost omezit přístup určitých subjektů k službám v návaznosti na jejich protiprávní činnost. Toto omezení přitom může zahrnovat jak částečnou blokaci přístupu k internetu, tak úplné přerušení připojení. Nesplnění těchto povinností může být sankcionováno velmi vysokými pokutami (hovoří se až o částce 250 000 £).

Krok popsaný v předchozím odstavci je obecně chápán jako nejkrajnější řešení situace. Oficiálně se předpokládá, že dostatečným odstrašujícím prvkem bude fakt, že porušitel bude nucen zpětně uhradit svému poskytovateli služeb informační společnosti náklady, které mu vznikly v souvislosti s „vyřizováním předmětné kauzy". OFCOM však bude průběžně sledovat procentní pokles porušení autorských práv. Pokud se ukáže, že proces zasílání varovných dopisů neplní svůj účel a procentuelní vyjádření autorskoprávních deliktů se nesníží alespoň o 70 bodů, dojde i na toto krajní řešení. Pro účely tohoto článku je důležité zdůraznit, že celý výše popsaný proces nemá, na rozdíl od francouzské úpravy, probíhat v rámci trestního řízení. Primárním cílem této iniciativy tedy zřejmě nemá být stíhání či postih viníků, ač tato pochopitelně nevylučuje, aby se autor domáhal svých práv před civilním soudem.

Rozdílnost názorů na řešení problému porušování autorských práv na internetu prostřednictvím stupňovité odezvy se odrazila i v rámci legislativního procesu na evropské úrovni. Zde mají totiž výše zmíněné dva státy (Francie především) značný vliv, a proto se poměrně napjatě očekávalo, jak se k tomuto problému orgány EU postaví. Nakonec princip stupňovité odezvy v Evropském parlamentu podporu nezískal a zákonodárci vyjádřili jasně své stanovisko v rámci stěžejního dokumentu posledních let pro oblast informačních technologií – ve Směrnici Evropského parlamentu a Rady 2009/140/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/21/ES, o společném předpisovém rámci pro sítě a služby elektronických komunikací, směrnice 2002/19/ES, o přístupu k sítím elektronických komunikací a přiřazeným zařízením a o jejich vzájemném propojení a směrnice 2002/20/ES, o oprávnění pro sítě a služby.[106] Tento komplikovaný a poněkud těžko čitelný text obsahuje pro nás důležité ustanovení článku 1 odst. 1, které mění článek 1 Směrnice 2002/21/ES vložením odstavce 3a. Na základě tohoto ustanovení musí opatření přijatá členskými státy, která se týkají přístupu koncových uživatelů ke službám a aplikacím nebo jejich využívání prostřednictvím sítí elektronických komunikací, respektovat základní práva a svobody jednotlivců zaručená Evropskou úmluvou o ochraně lidských práv a základních svobod a obecnými zásadami práva EU. Při aplikaci jakýchkoli omezení musí být bezpodmínečně zachován princip proporcionality a zajištěno uplatňování přiměřených procesních záruk, včetně účinné soudní ochrany a řádného procesu. Tato opatření tak mohou být přijata pouze při náležitém zohlednění zásady presumpce neviny a práva na soukromí. Právo na řádný proces dle tohoto článku zahrnuje mimo jiné i právo na slyšení dotyčné osoby a právo na včasný a účinný soudní přezkum. Co se týče právní argumentace, toto ustanovení v zásadě koresponduje s výše zmíněným rozhodnutím francouzské Ústavní rady ve věci *HADOPI*, explicitně však nepožaduje soudní rozhodnutí jako podklad pro omezení přístupu na internet – řešení tak zůstává v kompetenci jednotlivých členských států. Ty nám své postupy představí již poměrně brzy – Směrnice o společném předpisovém rámci má být do vnitrostátního práva států implementována do 24. května roku 2011.

106 Obecně je tato směrnice známá jako „telekomunikační balíček".

6.3 Internetové filtrování a digitální cenzura

Jak bylo již uvedeno výše, pro třetí modelovou situaci je charakteristické, že okruh omezovaných osob není určitý a přístup je zablokován ke konkrétně definovaným informacím. Ač to na první pohled nemusí být zřejmé, jedná se o všeobecně nejrozšířenější formu blokování informací na internetu – o tzv. *internet filtering*, česky filtrování, často také označované výrazem s negativní konotací – digitální cenzura. Akt cenzury je většinou chápán jako činnost záporná, jako zásah, který útočí na základní hodnoty demokratické společnosti. Nesmíme však zapomínat, že pojmem „cenzura" je označován jakýkoli autoritativně využívaný mocenský nástroj určený ke kontrole informací určených k veřejnému šíření, případně rovněž ke kontrole informačních toků. Může tak jít jak o činnost, která společnost ohrožuje, tak o proces, který ji svým způsobem chrání.[107] [108]

Dle autorů Farise a Villeneuva[109] se státy uchylují k filtrování informací pro jejich politické, náboženské nebo sociální konotace. Zatímco v sociální oblasti (např. v odsuzování dětské pornografie apod.) nacházejí jednotlivé státy alespoň základní míru konsensu, výklad náboženských a politických otázek se mnohdy stát od státu výrazně liší. Obecně můžeme říci, že regulovat přístupnost informací lze prostřednictvím kombinace zákonů věnovaných médiím, telekomunikacím, národní bezpečnosti a internetu jako takovému, přičemž světový trend ovlivňování obsahu a dostupnosti informací stále stoupá (především v závislosti na stoupajícím významu internetu a informačních technologií, který pro celosvětovou výměnu informací mají). Nejširším spektrem regulovaných oblastí se již tradičně vyznačuje oblast Středního a Dálného Východu a severní Afriky, kdy cenzura

107 Pro pochopení významu a smyslu takových aktivit je nejprve nezbytné znovu si uvědomit charakter informace a moc, jakou v sobě skrývá. Definic informace lze nalézt nepřeberné množství, přičemž jedna formulace se liší od druhé. V zásadě se z nich však dá odvodit pro nás důležitý závěr, že existuje určitá suma dat s různou pravdivostní hodnotou, která svým šířením prostřednictvím komunikace vytváří určitou vědomost resp. znalost určitého faktu. Kdo je schopen uplatnit nějakým způsobem v tomto procesu svůj vliv (tedy jakkoli do něj autoritativně zasahovat), může dát podobu konečné vědomosti a *de facto* tak utvářet podobu světa jako takového.

Ošemetné je i samo označení „pozitivní" a „negativní". Vždyť i autoritářské režimy zdůvodňují uplatňování cenzury jako způsob ochrany společnosti před nežádoucími rozkladnými vlivy, z jejich pohledu by se tedy tyto zásahy daly označit za pozitivní, i když je například naše kultura, založená na odlišných hodnotách, odmítá. Autorka zde pochopitelně nezpochybňuje význam základních hodnot uznávaných v demokratické společnosti, pouze upozorňuje na fakt, že ono „harmonické fungování společnosti" může být v různých kulturách chápáno různě, a proto se chce vyhnout jednoznačně odsuzujícímu tónu, který by mohl v následujícím rozboru zaznít.

108 Více o digitální cenzuře včetně případových studií lze nalézt např. na stránkách iniciativy Digital Cooperative:
Report: *Global Censorship in the Digital Age* [online]. [cit. 2010-03-09]. Dostupné z: < http://library.thinkquest.org/07aug/02035/notebook.html#rep_ov>.

109 Viz DEIBERT, R. – PALFREY, J – ROHOZINSKY, R. a kol. *Access denied. The Practice and Policy of Global Internet Filtering*. 1. vyd. Cambridge: The MIT Press, 2008. s. 5 – 28.

slouží k podpoře a udržení stability autoritářských režimů.[110] Výrazně omezenější je pak filtrování informací v zemích s demokratickým režimem, kdy funguje jako jeden z účinných způsobů, jak bojovat s trestnou činností (např. omezení přístupnosti určitého druhu informací v knihovnách a školách v USA nebo potírání materiálů s nacistickou tématikou v Německu apod.).[111]

> Americký Zákon pro ochranu dětí na internetu z roku 2000 (angl. *The Children´s Internet Protection Act*, zkráceně CIPA) v sekci 3601 výslovně stanoví, že pokud školní zařízení a knihovny nepřijmou odpovídající technická opatření, aby zabránily přístupu dětí ke stránkám s určitým obsahem (konkr. jde o dětskou pornografii a obsah obscénní a obecně pro dítě škodlivý), nemohou získat finanční příspěvky z tzv. *E-rate* fondu. Tento fond poskytuje veřejným institucím prostředky pro zlepšení kvality poskytovaných služeb především v oblasti technického vybavení a přístupu na internet.[112]

> V rámci Spolkové republiky Německo pak mohou ISP hlásit svá podezření na protiprávní aktivity probíhající v rámci jejich služeb a přispívat tak k vytvoření oficiálního seznamu stránek s extrémistickým obsahem. Na základě získaných informací pak může centrální doménový registrační úřad (DENIC) odmítnout registraci adres, které jsou v souvislosti s takto získanými informacemi identifikovány jako nežádoucí. Seznamy nebezpečných adres mohou být dále využívány například iniciativami zabývajícími se ochranou mládeže na internetu (např. iniciativa *Jugendschutz.net*), nebo třeba výrobci filtrovacího *softwaru* jako podklad pro konfiguraci svých výrobků. Podobný postup jako v Německu je v různých podobách aplikován i v řadě jiných států EU například ve vztahu ke stránkám s dětskou pornografií, materiálům popírajícím holocaust apod.

> V České republice funguje filtrování závadného obsahu prozatím pouze v rámci dobrovolných aktivit jednotlivých ISP. Blokován je především obsah podporující a propagující hnutí směřující k potlačení práv a svobod občanů a dětská pornografie. Hodnocení jednotlivých stránek přejímají čeští *provideři* například od britské organizace *Internet Watch Foundation* (IWF), která z pozice soukromého subjektu bojuje proti ilegálnímu obsahu na internetu. Herczeg a Gřivna ve svém článku[113] upozorňují na kontroverzní návrh novely zákona č. 202/1990 Sb., loterijní zákon, ve znění pozdějších předpisů, do které bylo „propašováno" i ustanovení novelizující zákon č. 480/2004 Sb.[114] Dle této novely měl být za §2 vložen §2a, ve kterém byl zaveden požadavek, že provozovatel elektronických prostředků má povinnost zajišťovat nemožnost připojení uživatele ke stránkám s pornografickým obsahem, ke stránkám nabízejícím a umožňujícím účast v loteriích a podobných hrách v rámci sítě internet a k těm stránkám, které podporují jiné zakázané služby a činnosti. Tento návrh byl dosti absurdní, nový §2a by totiž zavedením objektivní odpovědnosti ISP odporoval ostatním ustanovením zákona, které ji vylučují. V přímém rozporu by byl i s ustanovením §6 tohoto zákona, který garantuje vyloučení povinnosti monitorovat přenášené informace a aktivně vyhledávat skutečnosti poukazující na protiprávní obsah těchto informací – pokud má ISP zajistit nemožnost připojení k určitému obsahu, musí tento obsah nejprve vyhledat a toto lze učinit pouze v rámci monitorování všech zpracovávaných informací. Nebylo ani stanoveno, jak by mělo být „zajištění nemožnosti připojení" realizováno. Další problém tkvěl v tom, že návrh zákona zahrnoval mezi nežádoucí informace i materiál „s pornografickým obsahem" obecně - *de facto* tak stavěl mimo zákon pornografii jako celek, tedy i tu, která není kriminalizována trestním zákoníkem a je tudíž legální (tzn. nejde o dětskou pornografii a/nebo pornografická díla, v nichž se projevuje neúcta k člověku a násilí, nebo která znázorňují pohlavní styk se zvířetem). Návrh novely loterijního zákona v této podobě naštěstí neprošel, jde však o zajímavou ukázku z české legislativní praxe.

Vytvoření seznamu zdrojů, jejichž zpřístupnění veřejnosti není žádoucí, je základem pro následný proces filtrace a zároveň je jeho velkou slabinou. Vzhledem k obrovskému objemu zpracovávaných dat na internetu a rychlosti, s jakou se obsah informací mění, je mnohdy nemožné udržet krok s vývojem a adekvátně na něj reagovat. V současnosti existuje řada postupů, jak lze zabránit šíření nežádoucích informací, přičemž každý z nich je účinný v jiném prostředí a za jiných okolností. Využívány jsou nejrůznější technické prostředky, které svým působením v klíčových bodech transportního řetězce[115] způsobí jeho přerušení a znemožní tak, aby došlo

110 Stále častěji se však hovoří i o podobném typu cenzury v rámci států SNS, které bychom tak mohli označit jako „meziskupinu" nacházející se někde na pomezí mezi dvěma popsanými protipóly.

111 DEIBERT, R. – PALFREY, J – ROHOZINSKY, R. a kol. *Access denied. The Practice and Policy of Global Internet Filtering*. 1. vyd. Cambridge: The MIT Press, 2008. s. 41.

112 Podrobně viz: The Children´s Internet Protection Act [online]. [cit. 2010-03-12]. Dostupné z: <http://ifea.net/cipa.pdf>.

113 Viz HERCZEG, J. – GŘIVNA, T. Právo na přístup k Internetu, blokace stránek a digitální gilotina. *Trestněprávní revue.* 2010, roč. 9, č. 4, s. 4.

114 Celý text návrhu lze nalézt na oficiálních stránkách Poslanecké sněmovny, viz: Sněmovní tisk 722/0, část č. 1/2: Novela zákona o loteriích a jiných podobných hrách [online]. [cit. 2010-03-25]. Dostupné z: <http://www.psp.cz/sqw/historie.sqw?o=5&t=722>.

115 Anglicky jsou tyto body označovány jako *„choke points"*, což je výraz přejatý z vojenské terminologie. Původně se jednalo o označení určitého bodu v terénu, kterým jednotky protivníka musí nevyhnutelně projít, a ve kterém se tyto jednotky ocitnou vzhledem ke geografickým podmínkám v nevýhodě. Je tedy žádoucí využít poskytnuté geografické výhody a zaútočit právě v těchto bodech, kdy je postup snazší a šance na úspěch tudíž mnohem vyšší.

k nežádoucímu spojení (např. blokování na základě IP adres, doménových jmen, klíčových slov apod.). V rámci autoritativních režimů, kdy stát pro prosazení svých zájmů neváhá použít i prostředky oficiálně postavené mimo zákon, dochází k využívání nezákonných praktik v podobě šíření *malware*, infikování zpracovávaných informací nepravdivými daty a údaji (tzv. *cache poisoning*) nebo tzv. *Denial-of-Service* útoků.[116] Nesmíme však zapomínat, že cenzuru lze provádět i jinými nežli ryze technickými prostředky. Svou (spíše doplňkovou) roli hraje i vyvíjení specifického sociálního tlaku na jednotlivé aktéry v rámci procesu sdílení informací. Může jít třeba o monitorování jejich aktivit prostřednictvím kamer v internetových kavárnách nebo například o způsob, jakým jsou umístěny počítače v knihovnách – tak, aby monitor počítače byl pro okolí viditelný a bylo možno rozpoznat prohlížený obsah apod.[117]

Státy samotné ve většině případů nejsou schopny přímo fakticky ovlivnit obsah a dostupnost informací na internetu, stěžejní roli proto opět hrají soukromé subjekty, které zákonem uložené požadavky realizují (zde nejde již pouze o poskytovatele služeb informační společnosti, svou významnou roli hrají i poskytovatelé *hardware* a *software* a jiné subjekty, jejichž aktivity zrovna nespadají do rámce definovaných činností ISP). A mnohem častěji, nežli v jiných případech blokování závadného obsahu na internetu, jsou v souvislosti s problematikou cenzurování kladeny otázky týkající se hranic etiky obchodních společností nebo morální ceny za ekonomický úspěch, kterou je nutno zaplatit. Ekonomický rozměr cenzury informací získává stále na významu – otevírají se nové specifické trhy s perspektivou obrovských zisků pro soukromé subjekty, s nimi však zároveň přicházejí i nová chápání pojmů jako je demokracie, boj za národní bezpečnost nebo svoboda projevu či náboženského vyznání. Každý z aktérů se tedy musí nevyhnutelně sám sebe ptát, jak moc je ochoten slevit ze zásad obecně přijímaných ve společnosti, odkud pochází, a kde leží onen mezník za kterým již peníze a úspěch ztrácejí svou skutečnou hodnotu. Typickým příkladem takového střetu zájmů, etických hodnot a tradic je problematické fungování společnosti *Google, Inc.* v rámci Čínské lidové republiky:

> Hegemon ve světě internetových vyhledávačů vstoupil na přísně regulovaný čínský trh v roce 2005. Ihned od začátku *Google* aplikoval v rámci poskytování svých služeb cenzuru v souladu s požadavky čínského autoritativního režimu, za což sklízel značnou kritiku především ve Spojených státech amerických, kde má centrála společnosti své sídlo. *Google* se tak aktivně podílel na tzv. Projektu Zlatého štítu (angl. *Golden Shield Project*, označovaný též jako „Velká informační čínská zeď", angl. „*Great Firewall of China*"), spočívajícím v budování propracované dozorové a cenzurní sítě pod záštitou čínského ministerstva lidové bezpečnosti.[118] Získání výrazného podílu na čínském trhu tak bylo vykoupeno řadou neetických aktivit, které společnosti *Google* vynesly ve světě mnoho nelichotivých kritik.
>
> V poslední době se však situace radikálně změnila – *Google* se v rámci svého působení v Číně již dlouhodobě potýká s nedostatkem ochrany ze strany čínského práva a s opakovanými hackerskými útoky, které citlivě zasahují do již tak okleštěného procesu poskytování služeb veřejnosti. Vrcholem pak bylo odhalení rozsáhlého hackerského útoku z konce roku 2009, který měl za cíl získání citlivých informací z Gmailových účtů. Ač zástupci společnosti *Google* čínskou vládu z podpory nebo dokonce organizování těchto útoků otevřeně neosočili, ve svém prohlášení z počátku ledna 2010 jasně naznačili, že *Google* již nadále nehodlá cenzurovat informace na internetu, jak to požaduje čínské právo, a že existuje reálná možnost odchodu společnosti z čínského trhu. Zatím zůstává pouze u těchto prohlášení a až nadcházející dny ukáží, zda *Google* svoje sliby splní a odstartuje tak nový trend na poli poskytování služeb na internetu.

Odlišné názory na problematiku filtrování závadného obsahu a otázky s ním spojené rozdělují odbornou veřejnost již od počátku vzniku tohoto fenoménu. Zatímco proponenti argumentují tím, že se jedná o nejúčinnější způsob, jak zabránit páchání trestné činnosti, poskytnout ochranu právem garantovaným zájmům a zajistit národní bezpečnost a obranu proti terorismu, odpůrci poukazují na porušování základních lidských práv a možnost zneužití cenzury k potlačování demokracie. Nevyvratitelnou skutečností je fakt, že filtrování na internetu není dokonalý prostředek boje proti bezpráví. Nikdy zřejmě nebude možné dosáhnout toho, aby přijatá opatření odpovídala přesně potřebám dané situace, vždy budou do jisté míry přehnaná nebo naopak nedostatečná. Cenzura, v pozitivním či negativním slova smyslu, je nástrojem velmi mocným, který v rukou nepovolaných osob může napáchat veliké škody a tohoto nástroje by tedy mělo užíváno s rozmyslem a uváženě. Alarmující nárůst využívání internetového filtrování proto nutí k zamyšlení, kde je ona pomyslná hranice nutné ochrany, za kterou se společnost stává otrokem sebe samé.

Na základě zjištěných skutečností lze konstatovat, že autoritativní zásahy státu do fungování prostředí počítačových sítí jsou skutečně nezbytné. Praktické skutečnosti dostatečně prokázaly, že kyberprostor není schopen fungovat na principu samoregulace a stát musí mocensky přispívat k jeho ochraně a řádnému fungování. Na závěr můžeme formulovat několik obecných znaků, které by takovéto autoritativní zásahy měly vždy splňovat:

116 *Denial-of-Service attack*, česky překládaný jako odmítnutí služby, spočívá v cíleném přehlcení systému požadavky, které způsobí pád tohoto systému nebo přinejmenším zablokování jeho fungování.

117 Podrobněji se k tomuto tématu rozepisují autoři Murdoch a Anderson v knize: DEIBERT, R. – PALFREY, J – ROHOZINSKY, R. a kol. *Access denied. The Practice and Policy of Global Internet Filtering*. 1. vyd. Cambridge: The MIT Press, 2008. s. 57 – 72.

118 Čínský cenzurní systém je v současnosti jedním z nejpropracovanějších a nejpřísnějších na světě. Existuje zde například státem spravovaný seznam zakázaných serverů, jehož obsah se podle politické situace průběžně mění. Připojení na blokovanou adresu je automaticky znemožňováno, přičemž se systém odvolává na technickou chybu resp. na neexistenci hledaného serveru. Cenzura probíhá i v rámci diskusních fór či messengerů, a to na základě klíčových slov – při zadání zakázaných slov (např. „demokracie" či „Tiananmen") se objeví upozornění, že zpráva obsahuje zakázaný text, přičemž je ihned zablokována. Kontrolována je i e-mailová komunikace, jednotliví ISP jsou nuceni aktivně spolupracovat se státními orgány a předávat jim citlivé osobní údaje svých uživatelů, které pak umožňují „provinilce" identifikovat a stíhat.

- Jakákoli intervence ze strany státu se vždy musí řídit zásadou proporcionality, musí být *přiměřená* a odpovídat specifikům regulované aktivity. V rámci autoritativní regulace musí být vždy rozsah práv chráněných a práv omezovaných v rovnováze.
- Způsob, jakým má být takový mocenský zásah proveden, musí být naprosto přesně popsán v rámci *kvalitní a jasné procesní úpravy.* Jednotlivé postupy musí přesně odpovídat charakteru situace a té má pak také odpovídat rozsah pravomoci pověřených orgánů.
- Procesní úprava je v zásadě doménou vnitrostátního práva. Ve specifickém prostředí kyberprostoru však ve většině případů není možné zájmy státu a společnosti účinně prosadit bez efektivní *spolupráce na mezinárodní úrovni.*
- Stát by měl svou moc vždy uplatňovat s *respektem k lidským právům a svobodám* a směřovat k harmonickému rozvoji společnosti.

Jistě by bylo možné vytvořit dlouhý seznam dalších požadavků, které by měla autoritativní regulace v prostředí kyberprostoru v ideálním případě naplňovat. Tyto čtyři však můžeme označit jako základní – při absenci kteréhokoli z nich nemůže systém účinně fungovat.

7 Závěr

Jak bylo již řečeno v úvodu tohoto článku, vývoj kyberkriminality je nerozlučně spjat s vývojem informační společnosti a díky technologickému pokroku se tento fenomén stále výrazněji vzdaluje od tradičního pojetí trestného jednání. Nevyhnutelně tak vzniká nutnost revidovat zažité instituty „pozemského" trestního práva a znovu definovat oblasti, ve kterých může resp. musí toto právo působit. Názory na vytváření nových skutkových podstat a vymezení regulovaných oblastí chování v kyberprostoru se ve vazbě na geografické rozdělení světa poměrně výrazně liší, což znesnadňuje nalezení tolik potřebného konsenzu na mezinárodní úrovni.

V úvodní kapitole tohoto článku se autorka pokusila nastínit některé z problémů souvisejících s trestněprávní regulací kyberprostoru, světa bez fyzických vazeb, bez hranic a zdánlivě i bez omezení. Ztotožnila se s názory amerického konstitucionalisty Lawrence Lessiga, jehož myšlenky o významu kódu jakožto autoritativně vytvořitelné a modifikovatelné definiční normy, která má schopnost působit na prostředí kyberprostoru, výrazně ovlivnily i analýzu problémů v následujících kapitolách. První kapitola tak měla za cíl poskytnout alespoň základní definice jednotlivých počítačových trestných činů, kategorizovat je a shrnout jejich charakteristické rysy tak, aby s nimi bylo možné v dalším výkladu pracovat. Vzhledem k zaměření článku se již autorka nezabývala ekonomickými, sociálními a psychologickými aspekty kyberkriminality jako celku.

Přeshraniční charakter aktivit v prostředí informačních technologií má veliký význam i při určování působnosti práva státu a jurisdikce jeho orgánů. Kapitola druhá měla za cíl shrnout základní obecné principy, kterými se tento proces řídí, důraz byl přitom kladen na specifika kyberzločinu a jejich vliv na finální výsledek rozhodování. Na základě pravomoci určené podle předmětných principů pak mohou orgány státu aktivně působit na chování subjektů v kyberprostoru, což je výchozím bodem pro analýzu obsaženou ve zvláštní části článku.

V kapitole třetí se autorka pokusila zmapovat nepřeberné množství právních dokumentů dotýkajících se problematiky trestné činnosti v kyberprostoru. Stěžejním předpisem je mezi těmito Úmluva Rady Evropy o kyberkriminalitě a na ni navazující opční protokol. Doplňuje ji řada dokumentů vytvořených v rámci práva EU, které jsou výsledkem postupné europeizace trestního práva. Tyto předpisy s rostoucím důrazem upozorňují na význam fenoménu kyberkriminality a vybízejí ke koordinovanému postupu a zpřísnění pravidel v rámci prostředí informačních technologií. Do českého právního řádu jsou pak implementovány s různou mírou úspěšnosti, velkým krokem kupředu bylo vytvoření nového kodexu trestního práva hmotného, na druhou stranu základní trestněprocesní předpis zůstává stále velmi konzervativní a řada nových institutů v něm není vůbec zohledněna. Pro další výklad jsou důležité také předpisy, které upravují odpovědnost poskytovatelů služeb informační společnosti.

Ve zvláštní části se autorka rozhodla zaměřit na specifickou skupinu definičních autorit, kterými jsou poskytovatelé informačních služeb. Položila si otázku, zda vůbec mohou tyto entity být dle českého práva trestněprávně odpovědné, za jakých podmínek a na základě jaké právní konstrukce lze tuto odpovědnost založit. Rozborem tradičních institutů trestního práva ve spojení s výkladem ustanovení zákona o některých službách informační společnosti došla autorka k závěru, že trestní odpovědnost ISP v českém právu skutečně existuje. Její založení je však na rozdíl od odpovědnosti civilněprávní vázáno nejen na naplnění podmínek daných předmětným zákonem č. 480/2004 Sb., jednání zakládající odpovědnost musí navíc splňovat veškeré formální a materiální požadavky stanovené trestním právem tak, aby mohlo být označeno za trestný čin.

Ve vazbě na trestněprávní odpovědnost ISP byla pak v kapitole páté diskutována problematika konstrukce a realizace pravomocí státních orgánů blokovat či odpojovat komunikační linky. Kvůli zpřehlednění se rozhodla autorka tyto postupy rozdělit do tří skupin podle charakteru blokovaného obsahu a okruhu subjektů autoritativním rozhodnutím státního orgánu dotčených. Vznikla tak jedna podkapitola věnovaná jednorázovému blokování závadného obsahu, druhá blokování na základě stupňovité odezvy a další zaměřená na filtrování a digitální cenzuru, přičemž se autorka snažila zohlednit jak českou tak zahraniční právní úpravu. Obzvláště z pohledu českého práva je daná problematika úzce propojena s procesem vyšetřování a dalšími postupy v rámci trestního řízení, které byly v textu průběžně diskutovány. Na základě analýzy dané problematiky lze dojít k poměrně zásadnímu zjištění, že v českém právu neexistují odpovídající ustanovení, o která by se orgány činné v trestním řízení mohly při nařizování zajištění dat se závadným obsahem opřít. Využívají tak obecného zmocnění daného trestním řádem, které je však pro tento účel nevyhovující a posouvá tak celý proces na hranici zákonnosti. V závěru tak nezbývá nežli shrnout, že česká právní úprava ještě v mnoha ohledech pokulhává za rapidním vývojem v oblasti kyberkriminality a existuje celá řada legislativních změn, které bude v nejbližším časovém horizontu nutno přijmout a uvést v praxi.

9 Použité prameny

Knižní publikace

ČEPELKA, Č. – ŠTURMA, P. *Mezinárodní právo veřejné.* 1. vyd. Praha: Nakladatelství C. H. Beck, 2008. 761 s.

FENYK, J. – SVÁK, J. – KLÍMA, K. *Europeizace trestního práva*. 1. vyd. Bratislava: Bratislavská vysoká škola práva, 2008. 229 s.

FILIP, J. – SVATOŇ, J. – ZIMEK, J. *Základy státovědy.* 4. vyd. Brno: Vydavatelství Masarykovy univerzity, 2006. 266 s.

GOLDSMITH, J. – WU, T. *Who controls the Internet: Illusions of a borderless World*. 2. vyd. Oxford: Oxford University Press, 2008. 223 s.

GŘIVNA, T. – POLČÁK, R. – HERCZEG, J. et al. *Kyberkriminalita a právo*. 1. vyd. Praha: Nakladatelství Auditorium, 2008. 220 s.

KOHL, U. *Jurisdiction and the Internet*. 1. vyd. Cambridge: Cambridge University Press, 2007. 323 s.

KOOPS, B.-J. – BRENNER, S. W. a kol. *Cybercrime and Jurisdiction: A Global Survey*. 1. vyd. Hague: T. M. C. Asser Press, 2006. 355 s.

KRATOCHVÍL, V. – FENYK, J. – KALVODOVÁ et al. *Kurs trestního práva: Trestní právo hmotné, obecná část.* 1. vyd. Praha: Nakladatelství C. H. Beck. 2009. 797 s.

KRATOCHVÍL, V. – KUCHTA, J. – MATES, P. *Trestní právo hmotné: Obecná část*. 3. vyd. Brno: Masarykova univerzita, 2003. s. 97.

LESSIG, L. *Code 2.0*. 1. vyd. New York: Basic Books. 2006, 410 s.

MALENOVSKÝ, J. *Mezinárodní právo veřejné: jeho obecná část a poměr k jiným právním systémům, zvláště právu českému*. 5. vyd. Brno: Vydavatelství Masarykovy univerzity a Nakladatelství Doplněk, 2008. 551 s.

MUSIL, J – KRATOCHVÍL, V. – ŠÁMAL, P. a kol. *Kurs trestního práva: Trestní právo procesní*. 2. vyd. Praha: Nakladatelství C. H. Beck, 2003. 1079 s.

POLČÁK, R. *Právo na internetu: Spam a odpovědnost ISP.* 1. vyd. Brno: Computer Press, a.s. 2007, 150 s.

THOMAS, D. – LOADER, B. D. *Cybercrime*. 2. vyd. London: Nakladatelství Routledge, 2000. 300 s.

ZITTRAIN, J. *The Future of the Internet and How to Stop It*. 1. vyd. New Haven: Yale University Press, 2008. 342 s.

Periodické prameny

BRENNER, S. W. The Emerging Consensus on Criminal Conduct in Cyberspace. *International Journal of Law and Information Technology*. 2002, roč. 10, č. 2, s. 150.

BRENNER, S. W. – KOOPS, B.-J. Approaches to Cybercrime Jurisdiction. *Journal of High Technology Law*. 2004, roč. 4, č. 1, s. 6.

BŘÍZA, P. – ŠVARC, M. Komunitarizace trestního práva v Lisabonské smlouvě a její (případná) reflexe v právním řádu České republiky. *Trestněprávní revue*. 2009, roč. 8, č. 6, s. 161 – 170.

GOODMAN, M. D. Why the Police Don´t Care About Computer Crime. *Harvard Journal of Law and Technology.* 1997, roč. 10, s. 468 – 469.

HERCZEG, J. – GŘIVNA, T. Právo na přístup k Internetu, blokace stránek a digitální gilotina. *Trestněprávní revue*. 2010, roč. 9, č. 4, s. 2 – 3.

SIEBER, U. Responsibility of Internet Providers – a Comparative Legal Study with Recommendations for Future Legal Policy. *Computer Law & Security Report*. 1999, roč. 15, č. 5, s. 291 – 310.

VOLEVECKÝ, P. Kybernetická trestná činnost v mezinárodních dokumentech a v dokumentech ES/EU. *Trestní právo*. 2009, roč. 8, č. 7 – 8, s. 26 – 38.

Elektronické zdroje

BAKER, C. E. *Hate Speech* [online]. University of Pennsylvania Law School, 2008, vyd. 3.10.2008 [cit. 2010-25-01]. Dostupné z: <http://lsr.nellco.org/cgi/viewcontent.cgi?article=1212&context=upenn_wps>.

CANNON, C. M. Free Speech vs. Hate Speech. *Politics Daily* [online]. vyd. 18. 08. 2009 [cit. 2010-24-01]. Dostupné z: <http://www.politicsdaily.com/2009/08/18/free-speech-vs-hate-speech>.

DHAVA, D. *Google Execs Convicted In Italian Abusive Video Case* [online]. vyd. 25. 02. 2010 [cit. 2010-03-05]. Dostupné z: <http://news.ebrandz.com/google/2010/3155-google-execs-convicted-in-italian-abusive-video-case.html>.

KUNER, C. *Judgment of the Munich Court in the „CompuServe Case" (Somm Case)* [online]. vyd. 15. 07. 2010 [cit. 2010-03-05] Dostupné z: <http://www.kuner.com/data/reg/somm.html>.

KUŽNÍK, J. – NÝVLT, V. – KASÍK, P. *Český senát chce cenzurovat internet. Zakázal by porno a další stránky.* [online]. Vydáno 23. 01. 2009 [cit. 2010-03-23]. Dostupné z: <http://technet.idnes.cz/cesky-senat-chce-cenzurovat-internet-zakazal-by-porno-a-dalsi-stranky-1ee-/sw_internet.asp?c=A090123_131417_sw_internet_kuz>.

PETERKA, J. *Stalo se: Český senát chce zakázat (stránkované) porno.* [online]. Vydáno 26. 01. 2009 [cit. 2010-03-23]. Dostupné z: <http://www.lupa.cz/clanky/stalo-se-cesky-senat-chce-zakazat-porno>.

PISA, N. *Google Italy ruling ‚threat to internet freedom'* [online]. vyd. 24. 02. 2010 [cit. 2010-03-05]. Dostupné z: <http://www.telegraph.co.uk/technology/google/7308384/Google-Italy-ruling-threat-to-internet-freedom.html>.

POLČÁK, R. Místní působnost trestního práva. *Kolizní otázky internetových právních vztahů* [online] Brno: Masarykova univerzita, [cit. 2010-02-04]. Dostupné z: <http://is.muni.cz/do/1499/el/estud/praf/js09/kolize/web/pages/trestni-pravo.html>.

VŠETEČKA, R. *Průlomový verdikt. Šéfové Googlu nesou vinu za video na internetu* [online]. vyd. 24. 02. 2010 [cit. 2010-03-05]. Dostupné z: <http://technet.idnes.cz/prulomovy-verdikt-sefove-googlu-nesou-vinu-za-video-na-internetu-1cj-/sw_internet.asp?c=A100224_135248_sw_internet_vse>.

Cyberterrorism. [online]. NATO [cit. 2010-24-01]. Dostupné z: <http://www.nato.int/STRUCTUR/library/bibref/cyberterrorism.pdf>.

Digital Economy Bill [HL] 2009-10 [online]. [cit. 2010-03-07]. Dostupné z: <http://services. parliament.uk/bills/2009-10/digitaleconomy.html>.

I Love You. *Wikipedia* [online]. Naposledy editováno 15. 12. 2009 [cit. 2010-02-04]. Dostupné z: <http://cs.wikipedia.org/wiki/I_Love_You>.

Loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet [online]. [cit. 2010-03-05]. Dostupné z: <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021208046&dateTexte>.

Mezinárodní pakt o občanských a politických právech. [online]. [cit. 2010-02-08]. Dostupné z: <http://www.osn.cz/dokumenty-osn/soubory/mezinar.pakt-obc.a.polit.prava.pdf>.

Mezinárodní spolupráce v boji proti informační kriminalitě [online]. [cit. 2010-02-22]. Dostupné z: <www.mvcr.cz/soubor/cyber-vyzkum-studie-mezinarodni-pdf.aspx>.

Oficiální stránky Rady Evropy [online]. Council of Europe, Status as of: 2010-03-20 [cit. 2010-03-20].
Dostupné z: <http://conventions.coe.int/treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG>.

Orgány a ostatní instituce Evropské unie: Evropská komise [online]. Europa [cit. 2010-03-30].
Dostupné z: <http://europa.eu/institutions/index_cs.htm>.

Orgány a ostatní instituce Evropské unie: Rada Evropské unie [online]. Europa [cit. 2010-03-30].
Dostupné z: <http://europa.eu/institutions/index_cs.htm>.

Reaction to the Green Paper on conflicts of jurisdiction and the ne bis in idem-principle in criminal proceedings [SEC (2005) 1767]. [online]. Leiden University, European Institute. [cit. 2010-02-04]. Dostupné z: <http://ec.europa.eu/justice_home/news/consulting_public/conflicts_jurisdiction/contributions/university_leiden_en.pdf>.

Report: Global Censorship in the Digital Age [online]. [cit. 2010-03-09].
Dostupné z: <http://library.thinkquest.org/07aug/02035/notebook.html#rep_ov>.

Restatement (Third) of Foregn Relations Law of the United States [online]. [cit. 2010-02-04].
Dostupný z: <www.macalester.edu/courses/intl114/docs/restatement.pdf>.

Restatements of Law. *Tarlton Law Library* [online]. Last updated 26 January 2010 [cit. 2010-02-04].
Dostupné z: <http://tarlton.law.utexas.edu/vlibrary/outlines/restatements.html>.

Sněmovní tisk 722/0, část č. 1/2: Novela zákona o loteriích a jiných podobných hrách [online]. [cit. 2010-03-25].
Dostupné z: <http://www.psp.cz/sqw/historie.sqw?o=5&t=722>.

Úmluva o ochraně lidských práv a základních svobod. [online]. [cit. 2010-02-08].
Dostupné z: <http://www.echr.coe.int/NR/rdonlyres/82E3CE7F-5D3D-46EB-8C13-4F3262F9E20B/0/CzechTch%C3%A8que.pdf>.

Základní definice vztahující se k tématu kybernetické bezpečnosti. [online]. Ministerstvo vnitra České Republiky, 2009 [cit. 2010-24-01]. Dostupné z: <http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx>.

Právní předpisy

Children´s Internet Protection Act (Pub. L. 106-554)

Dodatkový protokol č. 189 k Úmluvě o kyberkriminalitě, o kriminalizaci činů rasistické a xenofobní povahy

Loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet

Rámcové rozhodnutí Rady 2001/413/SVV ze dne 28. května 2001, o potírání podvodů a padělání bezhotovostních platebních prostředků

Rámcové rozhodnutí Rady 2004/68/SVV ze dne 22. prosince 2003, o boji proti pohlavnímu vykořisťování dětí a dětské pornografii

Rámcové rozhodnutí Rady 2005/222/SVV ze dne 24. února 2005, o útocích proti informačním systémům

Rozhodnutí Rady 92/242/EHS ze dne 31. března 1992, o bezpečnosti informačních systémů

Rozhodnutí Rady 2000/375/SVV ze dne 29. května 2000, o boji proti dětské pornografii na internetu

Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000, o některých aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („směrnice o elektronickém obchodu“)

Úmluva Rady Evropy č. 185 o kyberkriminalitě

Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů

Zákon č. 480/2004 Sb., o některých službách informační společnosti, ve znění pozdějších předpisů

Zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů

Oficiální dokumenty orgánů ES

Sdělení Komise Evropskému parlamentu, Radě, Hospodářskému a sociálnímu výboru a výboru regionů KOM(2006) 688 ze dne 15. listopadu 2006, boj proti spamu a špionážnímu („*spyware*“) a škodlivému softwaru („*malicious software*“)

Sdělení Komise Evropskému parlamentu, Radě a Evropskému výboru regionů KOM(2007)267 ze dne 22. května 2007, k obecné politice v boji proti počítačové kriminalitě

Sdělení Komise Evropskému parlamentu, Radě, Hospodářskému a sociálnímu výboru a výboru regionů KOM(2009) 149 ze dne 30. března 2009, o ochraně kritické informační infrastruktury

Závěry Rady 2009/C 62/05 ze dne 27. listopadu 2008, o společné pracovní strategii a konkrétních opatřeních v oblasti boje proti počítačové trestné činnosti

Zpráva Komise Radě KOM(2008) 448 založená na článku 12 rámcového rozhodnutí Rady ze dne 24. února 2005 o útocích proti informačním systémům

Rozhodnutí

Rozhodnutí obvodního soudu v Mnichově číslo 8340 Ds 465 Js 173158/95

Rozhodnutí Ústavní Rady Francouzské republiky č. 2009-580 DC