ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta
Katedra informačních technologií

Násilná a mravnostní internetová kriminalita

Magisterská diplomová práce

Bc. et Bc. Michal Struška

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Struška Michal

Informatika

Název práce

Násilná a mravnostní internetová kriminalita

Anglický název

Violent and immoral internet criminality

Cíle práce

Tématem diplomové práce je násilná a mravnostní internetová kriminalita. Základním cílem této diplomové práce je seznámení se se základními pojmy spojenými s násilnou a mravnostní kriminalitou. Dalším cílem je nastínění jednotlivých trestných činů souvisejících s touto problematikou včetně nástrojů jejich prověřování a vyšetřování.

Metodika

Metodika vypracování této diplomové práce je založena na studiu informačních zdrojů zabývajících se tématem násilné a mravnostní internetové kriminality. Praktická část se pak týká analýzy nástrojů sloužících k prověřování a vyšetřování tohoto specifického druhu trestné činnosti s cílem odhalit jejich úskalí. Z výše uvedeného poté vycházejí závěry této diplomové práce.

Harmonogram zpracování

Studium odborných informačních zdrojů - 8-9/2011
Vypracování přehledu řešené problematiky - 10/2011
Vypracování analytické části práce - 11-12/2011
Komplexní dokončení diplomové práce - 1-2/2012
Odevzdání diplomové práce a teze - 3/2012

Rozsah textové části

60-80 stran

Klíčová slova

internetová kriminalita, kybernalita, násilí, mravnost, mravnostní kriminalita, násilná kriminalita, trestní zákoník, trestní řád, kyberterorismus, kyberstalking, dětská pornografie

---

Doporučené zdroje informací

JIROVSKÝ, Václav. Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství . Praha : Grada Publishing , 2007. 284 s. ISBN 978-80-247-1561-2.

ŠÁMAL, Pavel. Trestní zákoník II: komentář. 1. vyd. V Praze: C.H. Beck, 2009-2010. ISBN 97880740017892.

ŠÁMAL, Pavel. Trestní řád: komentář. 6., doplněné a přepracované vyd. V Praze: C.H. Beck, 2008, 23011 s. ISBN 978-807-4000-430.

VERTON, Dan. Black ice: neviditelná hrozba kyberterorizmu. Gliwice: Helion, 2004, 278 s. ISBN 83-736-1564-4.

výroční zpráva BIS 2010, http://www.bis.cz/n/2011-09-07-vyrocni-zprava-2010.html

Por. Ing. Michal Janoušek: Kyberterorismus: terorismus informační společnosti, http://www.mocr.army.cz/mo/obrana_a_strategie/2-2006cz/janousek.pdf

Kyberprostor [cit. 27.01.2012]. Wikipedia – the Free Encyclopedia. [online]. Dostupné na WWW: [http://cs.wikipedia.org/wiki/Kyberprostor].

ČÍRTKOVÁ, Ludmila. Moderní psychologie pro právníky: [domácí násilí, stalking, predikce násilí]. Vyd. 1. Praha: Grada, 2008, 150 s. Psyché (Grada). ISBN 978-802-4722-078.

NĚMEC, Miroslav. Kriminalistická taktika pro policisty. Vyd. 1. Praha: Eurounion, 2004. ISBN 978-807-3170-363.

Vedoucí práce

Brechlerová Dagmar, RNDr., Ph.D.

Termín odevzdání

březen 2012

doc. Ing. Zdeněk Havlíček, CSc.
Vedoucí katedry

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
Provozně ekonomická fakulta

prof. Ing. Jan Hron, DrSc., dr.h.c.
Děkan fakulty

V Praze dne 1.3.2012

Čestné prohlášení

Prohlašuji, že jsem svou magisterskou diplomovou práci vypracoval samostatně a uvedl v ní veškerou literaturu i prameny, ze kterých jsem při jejím zpracování vycházel.

…….
Bc. et Bc. Michal Struška

Poděkování

Děkuji vedoucí mé magisterské diplomové práce RNDr. Dagmar Brechlerové Ph.D. za čas, který mi věnovala při konzultacích, za pomoc a podnětné připomínky.

Násilná a mravnostní internetová kriminalita
The violent and the vice internet crimes

souhrn

S rychlým rozvojem informačních technologií přicházejí kromě výhod i nové hrozby. Cílem této diplomové magisterské práce je poukázat na jednu z těchto hrozeb, konkrétně na násilnou a mravnostní kriminalitu páchanou prostřednictvím sítě Internet. Samozřejmostí je v úvodu této práce seznámení čtenáře se základními pojmy spojenými s touto problematikou, kdy následuje výčet jednotlivých trestných činů, jejichž skutková podstata se týká těchto protiprávních jednání. Následuje popis nástrojů, za jejichž pomoci lze tuto specifickou trestnou činnost odhalovat a získávat tak zároveň důkazní prostředky. Praktická část spočívá v analýze postupu prověřování a vyšetřování násilné a mravnostní internetové kriminality se zaměřením na její specifika a úskalí.

klíčová slova
dětská pornografie, internetová kriminalita, kybernalita, kyberstalking, kyberterorismus, mravnost, mravnostní kriminalita, násilí, násilná kriminalita, trestní řád, trestní zákoník

summary

At the time of quick development of information technologies new threats appears except advantages. The goal of the diploma thesis is to show one of the threats, The violent and the vice crime committed by the Internet. It is obvious that the reader of the thesis meets concepts of the issues at the beginning. It is followed by enumeration of crimes relate to the credited infringements. The devices, which help to detect the specified crime and find out the evidences are the other part of the thesis. The practical part is dedicated to analyze procedures of the examination and investigation of the violent and the vice crimes focused on a specification and pitfalls.

keywords
child pornography, internet criminality, cybernality, cyberstalking, cyberterorism, morality, vice crime, violence, violent crime, criminal procedure, criminal code

Obsah

1 Úvod

S rozvojem společnosti jde ruku v ruce i rozvoj informačních a komunikačních technologií, který má významný vliv na trendy mezilidské komunikace. Nové informační technologie poskytují řadu výhod pro dorozumívání se jednotlivce s jednotlivcem i pro skupinové komunikace. S výhodami informačních technologií však přicházejí i nové hrozby, které mohou omezovat lidská práva a svobody, kdy v těch nejzávažnějších formách mohou být tyto technologie užity, jako nástroj k páchání trestné činnosti, která může mít různé podoby. Když pomineme případy, kdy se informační a komunikační technologie stávají přímo terčem útoku pachatelů trestné činnosti, jako jsou krádeže osobních počítačů, či útoky prováděné za účelem poškození či odcizení dat uložených na cílových počítačích nebo datových médiích, dostaneme se k protiprávním jednáním, jež útočí přímo proti integritě člověka. Mezi nejzávažnější protiprávní jednání, ke kterým dochází za užití informačních technologií a která poškozují lidskou důstojnost, patří násilná a mravnostní trestná činnost páchaná prostřednictvím sítě Internet. Právě tato protiprávní jednání jsou předmětem této magisterské diplomové práce. Druhou kapitolou této diplomové práce je seznámení čtenáře se základními pojmy a historií internetové kriminality. Třetí kapitola je poté exkurzem do oblasti legislativy, která je úzce spjata s touto problematikou, a popisuje tak zejména právní úpravy této specifické trestné činnosti v České republice. Následující čtvrtá kapitola pak představuje podrobněji jednotlivé skutkové podstaty násilné trestné činnosti páchané prostřednictvím sítě Internet, které jsou v prostředí České republiky považovány za pro společnost tak nebezpečné, že jsou uvedeny v trestním zákoníku. Totéž popisuje kapitola pátá, která se však zaměřuje na mravnostní trestné činy páchané prostřednictvím sítě Internet. Mimo výčet trestných činů upravuje česká legislativa zároveň právní nástroje určené k prověřování a vyšetřování trestných činů obecně, kdy jejich neúplný výčet je uveden v kapitole šesté. Kromě trestně-právní oblasti se na objasňování této specifické trestné činnosti spolupodílí i různá odvětví z oboru kriminalistiky a proto je v kapitole sedmé nastíněn vztah mezi internetovou kriminalitou, digitální stopou a kriminalistikou. V osmé kapitole jsou pak rozvedeny jednotlivé fáze odhalování internetové násilné a mravnostní trestné činnosti od jejího oznámení po podání návrhu na podání obžaloby s cílem poukázat na specifika a možná úskalí řešení násilné a mravnostní trestné činnosti páchané prostřednictvím sítě Internet.

Poslední devátou kapitolu tvoří závěr této diplomové práce, kde jsou shrnuty poznatky zejména z osmé kapitoly, která je praktickou částí této práce. Cílem této diplomové práce je tedy, jak vyplývá z obsahu kapitol, seznámení čtenáře s problematikou prověřování a vyšetřování násilné a mravnostní trestné činnosti s cílem upozornit na specifika a možné problémy, které s tímto souvisejí.

2 Historie internetové kriminality

Informační kriminalita, tedy kriminalita, která je páchána na informačních technologiích nebo jejich prostřednictvím, je často nazývána kybernetickou kriminalitou, zkráceně kybernalitou, v mezinárodních měřítkách „Cyber Crime“ nebo „Hi-tech Crime“.

Definice OSN: *"Tradiční zločinné aktivity jako krádež, podvod a padělání, tedy činy trestné ve většině zemí na světě. Počítač rovněž tvoří prostředí pro nové činy spočívající ve zneužití počítačů, které jsou nebo by měly být ve své podstatě trestné"*

Jako první počítačový zločin je v literaturách zabývajících se tímto tématem označován případ, který se stal ve Francii v roce 1801, tzn. téměř 150 let před vznikem prvního skutečného počítače. V této době tkadlec Jacquard zkonstruoval jednoduché zařízení, jehož cílem byla automatizace jednotlivých úkonů užívaných při tkaní specifických látek. V té době zaměstnanci této manufaktury ze strachu ze ztráty zaměstnání, která jim hrozila z důvodu jejich nahrazení tímto zařízením, prováděli série sabotáží, které vedly k přerušení dalšího vývoje tohoto zařízení. [MAT2002]

O vzniku prostředí kyberprostoru v dnešním pojetí, kde dochází k protiprávním jednáním, která budou popsána v následujících kapitolách této magisterské diplomové práce, můžeme hovořit od roku 1968, kdy došlo k prvnímu síťovému propojení mezi čtyřmi univerzitními počítači a ke vzniku zárodku sítě ARPANET, jež je „předchůdcem“ dnešní sítě Internet. S rychlejším, možná až moc rychlým, počátečním rozvojem těchto technologií nebyl již od počátku kladen příliš důraz na bezpečnost, jak se ukázalo postupem času. K prvním náznakům kybernality docházelo již na přelomu šedesátých a sedmdesátých let 20. století, kdy skupinka technologických nadšenců využívala nedokonalosti telefonní sítě pro uskutečňování nezpoplatněných dálkových telefonních hovorů. Tímto způsobem byla napadána komunikační síť firmy AT&T a v souvislosti s tímto jednáním se poprvé začalo hovořit o tzv. phreackingu. Nejednalo se tedy ještě o pronikání do počítačových sítí, o tzv. hacking. K prvním pokusům o hacking docházelo v osmdesátých letech 20. století, kdy se začali objevovat základní technologie dnešního Internetu. S příchodem technologie BBS (Bulletin Board System), tedy počítačů

umožňujících čerpání informací z databází pomocí standardizovaných dotazů, se začali vytvářet různé hackerské skupiny, jejichž smyslem byla výměna hesel do systémů, do kterých se těmto hackerům podařilo proniknout. V této době se však jednalo o hackery, kteří se do počítačových systémů dostávali spíše náhodným hádáním znění hesel. S příchodem prvních webových technologií se pomalu začaly rozvíjet první hackerské nástroje, tedy software umožňující prolamování hesel, monitoring sítě a další. V této době se zároveň začínají objevovat webové prezentace obsahující hackerské návody či přímo hackerský software ke stažení, čímž se hacking začíná dostávat do rukou širšímu okruhu lidí, včetně těch, co nemají o hackingu a s ním souvisejícími technologiemi hlubší povědomí. Hackeři v tom pravém slova smyslu pocházeli v 70. letech minulého století zejména z řad studentů soustředících se v okolí výpočetních center jednotlivých univerzit. Tito hackeři se postupně stávali vysoce postavenými představiteli velkých společností působících na trhu informačních technologií. Do této kategorie hackerů patřili i zakladatelé nejznámějších operačních systémů - Bill Gates nebo Linus Torvalds. Tato generace, dnes označovaná jako „stará garda“, vyrůstala v jiné době. Jejich hackerské aktivity byly zaměřené pouze na oblast univerzit a neškodili tak širšímu okruhu lidí, protože to v té době ani nebylo technicky možné. S rozvojem sítě Internet se aktivity „novodobých hackerů“ zaměřili i mimo univerzitní sítě, čímž se hackeři začali považovat za osoby, které škodí. Postupem času se také stále více informační technologie stávají nikoliv pouze cílem, ale také nástrojem dosažení útočníkem sledovaného zájmu, ať se již jednalo o finanční zisk či získání jiného prospěchu. V těch nejzávažnějších formách je s postupem času stále více vidět pronikání nástrojů kybernality do sféry organizovaného zločinu či dokonce terorismu. [JIR2007]

S postupným vývojem informačních a komunikačních technologií se tyto nástroje stále více rozšiřují mezi běžnou populaci obyvatel oproti dřívějším dobám, kdy byly počítače užívány zejména experty v této oblasti. Počítače již neslouží pouze ke zjednodušení lidských činností, ale stále častěji se s těmito technologii setkáváme v zábavném průmyslu. Informační a komunikační technologie se tak v dnešní době staly neodmyslitelnou součástí téměř každého člověka ve vyspělých zemích. Zároveň jsou informační a komunikační technologie stále častěji objevovány pachateli trestné činnosti, kteří tyto nástroje užívají k efektivnějšímu páchání již dříve prováděné trestné činnosti či páchání trestné činnosti nové. Informační a komunikační technologie v moderní

společnosti mají významný vliv na mezilidskou komunikaci, která se díky těmto technologiím stává výrazně anonymnější a zrádnější, což nahrává pachatelům trestné činnosti, pro které je pak jednodušší například vyhrožovat jinému bez toho, aniž by museli opustit místo svého bydliště a zároveň se osobním kontaktem s obětí prozradit. Zároveň tyto technologie umožňují provádět toto vyhrožování nebo jiné obtěžování systematicky dlouhodobě bez větších nákladů, kdykoliv si pachatel vzpomene. Problémem dnešní doby je zároveň postupné stírání vnímání skutečného života v reálném prostředí a života ve virtuálním světě, což dělá tato jednání o to nebezpečnější. [BOC2004]

3 Právo v kyberprostoru

Nejzákladnějším typem obrany proti nástrojům kybernality je legislativa v podobě všeobecné deklarace lidských práv, Mezinárodního paktu o občanských a politických právech, mezinárodních smluv a národních zákonů každého státu. V České republice se jedná zejména o Ústavu ČR, Základní listinu práv a svobod, mezinárodní úmluvy, trestní právo a další právní předpisy související s informačními technologiemi či prací s informacemi. Zatímco Ústava ČR spolu s Listinou základních práv a svobod se zabývá stanovením právního systému ČR a obecnou ochranou práv každého občana, trestní právo mimo jiné stanoví trestnost jednotlivých skutkových podstat kybernality a postupů jejich odhalování. Protiprávní jednání, která nejsou předmětem trestního práva, pak mohou být postižitelná dle dalších právních úprav souvisejících s informačními technologiemi a zpracováním informací. Tato kapitola se bude zabývat právě úvodem do trestního práva souvisejícího s páchaním kybernality, mezinárodními úmluvami v této právní oblasti a okrajově další legislativou týkající se obecně informačních systémů. [JIR2007]

3.1 Trestní právo hmotné

Trestní právo hmotné specifikuje základní podmínky trestní odpovědnosti s výčtem jednotlivých trestných činů a sankcemi, které lze pachatelům těchto trestných činů uložit. V trestním právu obecně platí tzv. princip "ultima ratio", který říká, že trestní právo má zasahovat do společenských vztahů pouze tam, kde jde o závažné poruchy těchto vztahů a kde již nelze ponechávat na občanech či jiných subjektech, aby se nápravy domohli cestou jiného práva. Z tohoto vyplývá míra důležitosti této právní oblasti právního systému ČR. [JIR2007]

Jedním z problémů právní úpravy kybernality v souvislosti s trestním právem je místní působnost. Působnost je v souvislosti s trestním právem hmotným chápána jako okruh společenských vztahů, v nichž se zákon uplatňuje. Pojem místní se pak, jak název sám napovídá, týká teritoriálního vymezení působnosti práva. V souvislosti s trestním právem hmotným to znamená, že aby mohlo být určité protiprávní jednání, které má znaky trestného činu, posuzováno dle právního systému ČR (konkrétně trestního zákoníku), musí být spácháno na území České republiky a to bez ohledu na to, jakého občanství je osoba

pachatele. Místem spáchání trestného činu je místo, kde došlo k jednání majícímu znaky trestného činu nebo místo následku trestného činu či místo, kde k následku trestného činu mělo dojít. Přestože trestní zákoník řeší například trestnou činnost páchanou na palubě lodi nebo letadla registrovaného v České republice, s případy páchání trestné činnosti v globálním kyberprostoru je to poněkud složitější. Tyto případy se řeší dle tzv. principu distančních deliktů, který se však zabývá pouze případy, kdy se pachatel dopustí na území republiky protiprávního jednání, které porušuje nebo ohrožuje zájem chráněný zákonem, i když účinek nastal nebo měl nastat zcela nebo z části v cizině. Princip distančního deliktu tedy řeší pouze případ, kdy pachatel nacházející se v době páchání trestné činnosti na území České republiky, napadá zájmy chráněné zákonem v jiném státě. Problematickým tedy zůstává trestní stíhání pachatele, který útokem vykonaným prostřednictvím počítačové sítě způsobí škodu (poruší nebo ohrozí zájem chráněný zákonem), avšak se sám nachází při páchání tohoto jednání na území jiného státu, kde toto jednání nebude trestné. V takovýchto případech jsou jediným nástrojem na dopadení pachatele fungující mezinárodní dohody a účinná spolupráce. Trestní právo hmotné je v České republice upraveno zákonem č. 40/2009 Sb. trestní zákoník. Jak již bylo uvedeno, trestní právo hmotné obsahuje mimo jiné výčet jednotlivých trestných činů včetně těch mravnostních a násilných, které mohou být páchány prostřednictvím sítě Internet. Tyto budou rozebrány v následujících kapitolách č. 4 a 5. [JIR2007]

3.2 Trestní právo procesní

Trestní právo procesní upravuje postup orgánů činných v trestním řízení, čímž chrání práva a oprávněné zájmy fyzických i právnických osob. Trestní právo procesní určuje procedurální postup trestního řízení, tj. postup zjištění, zda byl spáchán trestný čin, určení pachatele trestného činu, uložení trestu pachateli nebo ochranného opatření a rozhodnutí jejich vykonání. Trestní právo procesní realizuje trestní právo hmotné. V trestním právu procesním se mimo osobu pachatele rozeznávají další subjekty, které mají z hlediska svých pravomocí, vyplývajících z jejich postavení, vliv na průběh samotného trestního řízení. Těmto osobám dává trestní řád k vykonávání svého vlivu určitá procesní práva a procesní povinnosti. Patří sem zejména svědci, poškození, soudní znalci a tlumočníci. Dále v průběhu trestního řízení vystupují orgány činné v trestním řízení, kam

patří soudy, státní zastupitelství a policejní orgány, kdy tyto orgány vedou trestní řízení s cílem spravedlivě rozhodovat o jeho samotném průběhu od oznámení po konečné rozhodnutí. Oproti poškozeným stojí na druhé straně osoba, proti které se trestní řízení vede, tj. osoba pachatele, její obhájce a další zúčastněné osoby. Zejména soudní znalci hrají důležitou roli v trestním řízení probíhajícím v souvislosti s podezřením ze spáchání kybernality, neboť se jedná o poměrně specifickou oblast znalecké činnosti. Služeb soudních znalců v souvislosti s kybernalitou se v průběhu trestního řízení využívá zejména ve fázi prověřování a to formou odborných vyjádření nebo znaleckých posudků, na základě kterých jsou pak prováděny rozhodnutí orgánů činných v trestním řízení. V souvislosti s řešením kybernetické kriminality je někdy třeba zároveň využívat mezinárodní spolupráce, jež je taktéž upravena trestním řádem. Tyto postupy řeší zejména otázku právní pomoci, obsah institutů spolupráce a otázky pravomoci a příslušnosti. [JIR2007]

Procesní právo je v České republice upraveno zákonem č. 141/1961 Sb. o trestním řízení soudním. Mimo výše uvedené trestní řád stanoví nástroje pro prověřování a vyšetřování trestné činnosti. Některé z nich budou uvedeny v kapitole č. 6. [TRŘ2008]

3.3 Mezinárodní úmluvy

Součástí českého právního řádu jsou i některé mezinárodní smlouvy, k jejichž dodržování se Česká republika zavázala. V souvislosti s těmito mezinárodními smlouvami platí zásada, že pokud zákon stanoví něco jiného, než mezinárodní smlouva, tak se užije ustanovení právě mezinárodní smlouvy. Přijaté mezinárodní smlouvy tedy mají přednost před ostatními zákony. Jeden z nejvyšších evropských orgánů, Rada Evropy, začal projevovat iniciativu v oblasti počítačové kriminality již koncem 80. let. V roce 1989 byla vypracována studie obsahující doporučení pro úpravy a vytváření nové legislativy, která by měla kriminalizovat činy, spáchané prostřednictvím počítačových sítí. Jednalo se o doporučení Rady Evropy č. 9 z roku 1989. Poté následovalo doporučení Rady Evropy č. 13 z roku 1995, které se týkalo páchání trestné činnosti prostřednictvím informačních technologií. V roce 1997 byla sestavena Komise expertů na závažnější protiprávní jednání v kyberprostou (Commitee of Experts of Crime in Cyber-Space), která měla na starost návrh mezinárodní dohody usnadňující mezinárodní spolupráci při odhalování počítačových zločinů. [JIR2007]

Zde je výčet těch nejdůležitějších mezinárodních smluv týkajících se kybernality:

- Akční plán eEurope+
- Opční protokol k Úmluvě OSN o právech dítěte proti obchodováním s dětmi, dětské prostituci a dětské pornografii ze dne 25. května roku 2000
- Úmluva o kybernetické kriminalitě, Budapešť, ze dne 23. listopadu 2001
- Úmluva Rady Evropy o ochraně dětí před sexuálním vykořisťováním a zneužíváním ze dne 25. října 2007
- Rámcové rozhodnutí Rady EU 2004/68/SVV o boji proti sexuálnímu zneužívání dětí a dětské pornografii
- Úmluva o právech dítěte č. 104/1991 Sb.
- Mezinárodní úmluva o potlačování obchodu s necudnými publikacemi a jejich rozšiřování č. 96/1927 Sb.
- Úmluva o zákazu a okamžitých opatřeních k odstranění nejhorších forem dětské práce č. 90/2002 Sb.

3.4 Další právní úprava

- Zákon o elektronických komunikacích č. 127/2005 Sb.
- Autorský zákon č. 121/200 Sb.
- Zákon o ochraně osobních údajů č. 101/2000 Sb.
- Zákon o některých službách informační společnosti č. 480/2004 Sb.
- Zákon o informačních systémech veřejné správy č. 365/2000 Sb.

4 Násilné trestné činy kybernality

Dle definice uváděné Světovou zdravotnickou organizací (World Health Organisation, WHO), agenturou Spojených národů, je násilí:

"záměrné použití nebo hrozba použití fyzické síly proti sobě samému, jiné osobě nebo skupině či společnosti osob, které působí nebo má vysokou pravděpodobnost způsobit zranění, smrt, psychické poškození, strádání nebo újmu." [WHO]

Z výše uvedeného vyplývá, že se v tomto pojetí definice násilí nejedná, stejně jako z pozice legislativy, pouze o fyzické násilí, které by samozřejmě bylo prostřednictvím sítě Internet neuskutečnitelné, ale postačí pohrůžka násilí. Následující podkapitoly rozebírají jednotlivé skutkové podstaty trestního zákoníku č. 40/2009 Sb. týkající se násilné trestné činnosti, kterou je možné páchat prostřednictvím sítě Internet. Odstavce či jednotlivá písmena následujících ustanovení, která by mohla být stěží spáchána prostřednictvím sítě Internet, budou přeškrtnuta.

4.1 Vydírání dle § 175 tr. zákoníku

(1) Kdo jiného násilím, pohrůžkou násilí nebo pohrůžkou jiné těžké újmy nutí, aby něco konal, opominul nebo trpěl, bude potrestán odnětím svobody na šest měsíců až čtyři léta nebo peněžitým trestem.

(2) Odnětím svobody na dvě léta až osm let bude pachatel potrestán,
a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny,
~~b) spáchá-li takový čin nejméně se dvěma osobami,~~
~~c) spáchá-li takový čin se zbraní,~~
~~d) způsobí-li takovým činem značnou škodu,~~
e) spáchá-li takový čin na svědkovi, znalci nebo tlumočníkovi v souvislosti s výkonem jejich povinnosti, nebo
f) spáchá-li takový čin na jiném pro jeho skutečnou nebo domnělou rasu, příslušnost k etnické skupině, národnost, politické přesvědčení, vyznání nebo proto, že je skutečně nebo domněle bez vyznání.

(3) Odnětím svobody na pět až dvanáct let bude pachatel potrestán,
~~a) způsobí-li takovým činem těžkou újmu na zdraví,~~

b) spáchá-li takový čin v úmyslu umožnit nebo usnadnit spáchání trestného činu vlastizrady (§ 309), teroristického útoku (§ 311) nebo teroru (§ 312), nebo
~~c) způsobí-li takovým činem škodu velkého rozsahu.~~

~~(4) Odnětím svobody na osm až šestnáct let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 smrt.~~

(5) Příprava je trestná. [TRZII]

Předmětem ochrany tohoto trestného činu je svobodné rozhodování člověka. Pachatel tedy nutí jiného k tomu, aby něco konal, opominul nebo trpěl a to násilím, pohrůžkou násilí nebo jiné těžké újmy. Právě pohrůžka násilím nebo jiné těžké újmy zakládá možnost spáchání tohoto trestného činu nekontaktně, tj. mimo jiné prostřednictvím sítě Internet, přičemž pro spáchání tohoto trestného činu není nutné, aby pachatel dosáhl toho, co svou výhrůžkou sledoval. Poškozený zároveň musí tyto výhrůžky vnímat svými smysly a tyto si uvědomovat, v opačném případě se jedná o pokus vydírání. Pohrůžkou násilí je myšleno násilí, které má být vykonáno bezprostředně, ale i v bližší či vzdálenější budoucnosti. Výklad zároveň hovoří o tom, že výhrůžce nemusí být poškozený přímo přítomen, tzn., že k vyhrožování může dojít distančně například právě za užití sítě Internet. [TRZII]

Pohrůžka jiné těžké újmy může znamenat hrozbu způsobení újmy na majetku, vážné újmy na cti či dobré pověsti, může směřovat k rozvrácení manželství nebo rodinného života apod. Jinou těžkou újmou může být myšleno i zahájení trestního stíhání osoby v důsledku oznámení trestného činu, kterým pachatel poškozenému hrozí. Při posuzování, zda se jedná o jinou těžkou újmu, je nutné přihlížet k osobním poměrům napadeného, k jeho vyspělosti, zkušenostem, psychickému stavu apod.. [TRZII]

Jednou z podob naplnění skutkové podstaty trestného činu vydírání ve smyslu § 175 trestního zákoníku je tzv. kybernetické výpalné. Jedná se o relativně nový typ trestné činnosti, která je založena na zastrašování poškozené vydírané osoby prezentováním výhrůžky proniknutí do spravovaného nebo vlastněného systému za účelem zneužití nebo ztráty dat. Jedná se o projekci klasického deliktu do počítačového prostředí. [JIR2007]

4.2 Teroristický útok dle § 311 tr. zákoníku

(1) Kdo v úmyslu poškodit ústavní zřízení nebo obranyschopnost České republiky, narušit nebo zničit základní politickou, hospodářskou nebo sociální strukturu České republiky nebo mezinárodní organizace, závažným způsobem zastrašit obyvatelstvo nebo protiprávně přinutit vládu nebo jiný orgán veřejné moci nebo mezinárodní organizaci, aby něco konala, opominula nebo trpěla,
a) provede útok ohrožující život nebo zdraví člověka s cílem způsobit smrt nebo těžkou újmu na zdraví,
~~b) zmocní se rukojmí nebo provede únos,~~
c) zničí nebo poškodí ve větší míře veřejné zařízení, dopravní nebo telekomunikační systém, včetně informačního systému, pevnou plošinu na pevninské mělčině, energetické, vodárenské, zdravotnické nebo jiné důležité zařízení, veřejné prostranství nebo majetek s cílem ohrozit tím lidské životy, bezpečnost uvedeného zařízení, systému nebo prostranství anebo vydat majetek v nebezpečí škody velkého rozsahu,
d) naruší nebo přeruší dodávku vody, elektrické energie nebo jiného základního přírodního zdroje s cílem ohrozit tím lidské životy nebo vydat majetek v nebezpečí škody velkého rozsahu,
~~e) zmocní se letadla, lodi nebo jiného prostředku osobní či nákladní dopravy nebo nad ním vykonává kontrolu, anebo zničí nebo vážně poškodí navigační zařízení nebo ve větším rozsahu zasahuje do jeho provozu nebo sdělí důležitou nepravdivou informaci, čímž ohrozí život nebo zdraví lidí, bezpečnost takového dopravního prostředku anebo vydá majetek v nebezpečí škody velkého rozsahu,~~
~~f) nedovoleně vyrábí nebo jinak získá, přechovává, dováží, přepravuje, vyváží či jinak dodává nebo užije výbušninu, jadernou, biologickou, chemickou nebo jinou zbraň, anebo provádí nedovolený výzkum a vývoj jaderné, biologické, chemické nebo jiné zbraně nebo bojového prostředku nebo výbušniny zakázané zákonem nebo mezinárodní smlouvou, nebo~~
g) vydá lidi v obecné nebezpečí smrti nebo těžké újmy na zdraví nebo cizí majetek v nebezpečí škody velkého rozsahu tím, že způsobí požár nebo povodeň nebo škodlivý účinek výbušnin, plynu, elektřiny nebo jiných podobně nebezpečných látek nebo sil nebo se dopustí jiného podobného nebezpečného jednání, nebo takové obecné nebezpečí zvýší nebo ztíží jeho odvrácení nebo zmírnění, bude potrestán odnětím svobody na pět až patnáct let, popřípadě vedle tohoto trestu též propadnutím majetku.

(2) Stejně bude potrestán, kdo jednáním uvedeným v odstavci 1 vyhrožuje, nebo kdo takové jednání, teroristu nebo člena teroristické skupiny finančně, materiálně nebo jinak podporuje.

(3) Odnětím svobody na dvanáct až dvacet let, popřípadě vedle tohoto trestu též propadnutím majetku, nebo výjimečným trestem bude pachatel potrestán,
a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny,
b) způsobí-li takovým činem těžkou újmu na zdraví nebo smrt,
~~c) způsobí-li takovým činem, že větší počet lidí zůstal bez přístřeší,~~
d) způsobí-li takovým činem přerušení dopravy ve větším rozsahu,
e) způsobí-li takovým činem škodu velkého rozsahu,
f) získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu,
g) ohrozí-li takovým činem závažně mezinárodní postavení České republiky nebo postavení mezinárodní organizace, jejíž je Česká republika členem, nebo

h) spáchá-li takový čin za stavu ohrožení státu nebo za válečného stavu.

(4) Příprava je trestná. [TRZII]

O terorismu se začalo ve větší míře hovořit po útocích, které se udály 11. září roku 2011, kdy kromě budov, na které útoky směřovaly, bylo stejně důležité i napadení moci, která se za nimi skrývá: stovky tisíců kilometrů koaxiálních a optických kabelů a počítačů, které propojují, elektřina, která tyto počítače napájí a vyživuje, zásobování vodou, které udržuje v chodu jak vodní elektrárny, tak lidi, kteří obsluhují počítače, autobusy, železnice a kamiony, které dodávají součástky pro infrastrukturu, telekomunikační sítě, díky kterým mezi sebou mohou počítačové systémy komunikovat. Podporuje také finanční systémy bank, pojišťovacích společností, makléřských a dalších finančních institucí, které tyto technologie financují, pojišťují a zároveň na nich závisí samotná jejich existence. [VER2006]

Příští útok se může odehrát v kyberprostoru. Velká část ekonomiky nejen Spojených států závisí na správném fungování digitálního světa. Většina lidí si pod pojmem kyberprostor představí Internet. Teroristický útok však neohrožuje pouze World Wide Web. Téměř vše, co děláme, je nějakým způsobem ovlivňováno elektronickým světem. Bez správně fungujících počítačů a sítí bychom nebyli schopni vyrábět elektřinu v jaderných, tepelných a dalších elektrárnách. I kdybychom ji dokázali vyrobit, útok na počítačové systémy by ji znemožnil rozvádět. Počítačové technologie kontrolují i lékařskou evidenci, správní systémy a systémy objednávek, výroby, zpracování a distribuce. Proto, aby mohl teroristický vyvolat chaos, nemusí tyto systémy zcela ničit, ale stačí je soustavně nějakou dobu narušovat. To pak podkope zákazníkovu důvěru a následuje vlna ekonomických ztrát. [VER2006]

Vzhledem k tomu, že mírou moderní společnosti je schopnost využívání informací, objevuje se zde v souvislosti s teroristickými útoky relativně nový pojem - kyberterorismus, ve kterém se, jak už název napovídá, jedná o spojení terorismu a kyberprostoru. [JAN2006]

D. E. Denning definuje pojem Kyberterorismus následovně:

„Kyberterorismus je konvergencí terorismu a kyberprostoru obecně chápaný jako nezákonný útok nebo nebezpečí útoku proti počítačům, počítačovým sítím a informacím v

nich skladovaným v případě, že útok je konán za účelem zastrašit nebo donutit vládu, nebo obyvatele k podporování sociálních nebo politických cílů.“ [JAN2006]

Kyberprostor je pak definován jako označení virtuálního světa vytvářeného moderními technologiemi (počítači, telekomunikačními sítěmi apod.) paralelně ke světu „reálnému“. Jde o počítačový trojrozměrný svět analogický s internetem, ve kterém se uživatelé pohybují pomocí virtuální reality. [WIKIKYB]

Útoky vedené v souvislosti s kyberterorismem můžeme rozdělit do dvou kategorií:

- ***lokální kyberútok*** – samostatný přímý útok směřující na konkrétní technologii či službu. Nebezpečnost tohoto typu útoku závisí na zkušenostech, cílech a možnostech skupiny pachatelů. Pro zorganizování a realizaci takového útoku jsou potřeba zkušení uživatelé s určitou mírou odbornosti v oblasti síťových služeb a IT specialisté, kteří mají potřebné znalosti a zkušenosti v oblasti bezpečnosti počítačových sítí. [JAN2006]

- ***souběžný útok*** – jedná se o nebezpečnější variantu útoku, při kterém dochází k několika souběžným útokům na konkrétní oblasti či cíle na několika různých úrovních. Kyberútok je v tomto případě pouze jakousi přípravnou fází pro napadení pachatelem nebo podpůrnou akcí směřující k dezorientaci a likvidaci poškozeného, a která může být v přímé součinnosti s přímou akcí speciálních jednotek nebo např. leteckým bombardováním či dělostřeleckou přípravou. Zároveň může také docházet k několika různým druhům útoků (např. zajistit rozšíření nebezpečného malware pomocí zablokování určitých služeb sítě). [JAN2006]

Výše uvedené možné scénáře týkající se napadení kyberútokem se v současné situaci České republiky nejeví jako tolik reálné oproti situaci v USA, která je v porovnání s Českou republikou pravděpodobnějším cílem kyberútoků. Klidnější situaci v tomto směru v České republice mimo jiné dokládá kapitola 1.8. Výroční zprávy Informační bezpečnostní služby pro rok 2010 (aktuálně poslední veřejnosti dostupná výroční zpráva), která mimo jiné říká, že v České republice bylo prováděno monitorování především systémů úřadů a institucí veřejné správy s prvky tzv. e-Governmentu, i systémů právnických subjektů ze soukromoprávní sféry, jejichž narušení, poškození či zničení by mohlo mít vážné dopady na bezpečnostní a ekonomické zájmy ČR a fungování

společnosti, kdy se nepodařilo zjistit žádné závažnější útoky na tyto systémy. [BIS2010]

V prostředí České republiky v souvislosti s právní úpravou je terorismus považován za jednou z nejhorších a společensky nejškodlivějších forem mezinárodního organizovaného zločinu. Je hrozbou pro demokracii, svobodný výkon lidských práv, pro hospodářský a společenský rozvoj. Po událostech ze dne 11. září 2001 se boj proti terorismu stal také jedním z prioritních cílů Evropské unie. Ustanovení § 311, tj. trestní úpravy týkající se teroristických útoků, je naplněním závazku, který Česká republika přijala vstupem do Evropské unie. Z členství v Evropské unii vyplývá povinnost členských států aplikovat pravidla přijímána orgány Unie. Jedním z těchto rozhodnutí je i rámcové rozhodnutí Rady EU o boji proti terorismu. [TRZII]

Objektem trestného činu teroristického útoku je především ústavní zřízení a obranyschopnost České republiky, demokratické principy, na nichž je republika založena, základní hospodářská struktura státu, stejně jako i život a zdraví obyvatel republiky. Ochrana podle tohoto ustanovení je však poskytována nejen České republice, ale i mezinárodním organizacím a cizím státům. [TRZII]

Poškození ústavního zřízení neznamená jen jej v plné míře rozvrátit. Proto je dostačující, když pachatel svým jednáním má v úmyslu třeba jen pouze způsobení poruchy v řádném fungování ústavního systému. Analogicky toto platí i ve vztahu k útoku na obranyschopnost republiky. Podstatu pojmu základní politická, hospodářská nebo sociální struktura republiky lze vyvodit z toho, že Česká republika je demokratický právní stát, jehož politický systém je založen na svobodném vzniku a volné soutěži politických stran, které respektují základní demokratické principy a odmítají násilí jako prostředek k prosazování svých zájmů a jehož ekonomika je založena na principech tržního hospodářství a rovnoprávnosti všech forem vlastnictví. [TRZII]

V souvislosti s kyberterorismem je nutné v návaznosti na legislativní úpravy stanovit, co je myšleno sítí elektronických komunikací. Rozumí se tím přenosové systémy, popřípadě spojovací nebo směrovací zařízení a jiné prostředky, které umožňují přenos signálů po vedení, rádiem, optickými nebo jinými elektromagnetickými prostředky, včetně družicových sítí, pevných sítí s komutací okruhů nebo paketů a mobilních zemských sítí, sítí pro rozvod elektrické energie v rozsahu, v jakém jsou používány pro přenos signálů, sítí pro rozhlasové a televizní vysílání a sítí kabelové televize, bez ohledu na druh přenášené informace. Rozsah pojmu elektronických sítí je tak definován dostatečně široce.

Informačním systémem se pak zpravidla rozumí funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost. Každý informační systém zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, a dále nástroje umožňující výkon informačních činností. Informační činností (automatizovaně nebo jinými prostředky) je tvorba získávání, shromažďování, ukládání na nosiče informací, uchovávání, používání, vyhledávání, úprava nebo pozměňování, předávání, šíření, zpřístupňování, výměna, třídění nebo kombinování, blokování a likvidace informací ukládaných na hmotných nosičích technickými prostředky reprodukovatelným způsobem. [TRZII]

4.3 Vyhrožování s cílem působit na orgán veřejné moci dle § 324 tr. zákoníku

(1) Kdo jinému vyhrožuje usmrcením, ublížením na zdraví nebo způsobením značné škody
a) v úmyslu působit na výkon pravomoci orgánu státní správy, územní samosprávy, soudu nebo jiného orgánu veřejné moci, nebo
b) pro výkon pravomoci takového orgánu,
bude potrestán odnětím svobody až na tři léta.

~~*(2) Odnětím svobody až na pět let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 se zbraní.*~~ [TRZII]

Objektem skutkové podstaty trestného činu vyhrožování s cílem působit na orgán veřejné moci podle § 324 je zájem na řádném výkonu pravomoci orgánu státní správy, územní samosprávy, soudu a jiných orgánů veřejné moci. Vyhrožováním je pak myšleno psychické působení na vůli jiného člověka, kdy výhrůžka může být adresována nejen státnímu orgánu a jeho členům jako celku, ale i proti jeho jednotlivému pracovníku nebo i jiné osobě, ale musí být prostředkem působení na výkon pravomoci orgánu veřejné moci, nebo pachatel musí jednat pro výkon pravomoci takového orgánu, tedy v pohnutce postihnout státní orgán za to, že svoji pravomoc vykonal. V druhém případě se tedy jedná o pomstu za vykonání pravomoci. K naplnění skutkové podstaty je vyžadováno, aby pachatel vyhrožoval některou újmou v tomto ustanovení výslovně uvedenou. Jde vlastně o vyhrožování spácháním některého úmyslného trestného činu, zejména vraždy

(vyhrožování usmrcením), ublížení na zdraví, těžké ublížení na zdraví (vyhrožování ublížením na zdraví) nebo poškození cizí věci, popř. jiného majetkového trestného činu (vyhrožování způsobením značné škody). Újma, kterou pachatel hrozí, nemusí hrozit bezprostředně, postačuje vyhrůžka jednáním a následky vzdálenými. Vyhrůžka musí být míněna vážně a musí být řečena takovým způsobem, aby byla způsobilá v cílové osobě vyvolat obavu, že pachatel tuto svou výhrůžku splní. Je nerozhodné, jestli pachatel měl skutečně úmysl výhrůžku splnit. Je rozhodné, zda výhrůžka v konkrétním případě u poškozeného byla způsobilá vyvolat důvodnou obavu z jejího uskutečnění. [TRZII]

4.4 Vyhrožování s cílem působit na úřední osobu dle § 326 tr. zákoníku

(1) Kdo jinému vyhrožuje usmrcením, ublížením na zdraví nebo způsobením značné škody
a) v úmyslu působit na výkon pravomoci úřední osoby, nebo
b) pro výkon pravomoci úřední osoby, bude potrestán odnětím svobody až na tři léta.

~~*(2) Odnětím svobody až na pět let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 se zbraní.*~~ [TRZII]

Obdobně jako u trestného činu Vyhrožování s cílem působit na orgán veřejné moci dle § 324 trestního zákoníku je objektem tohoto trestného činu zájem na ochraně nerušeného výkonu pravomoci úřední osoby při plnění úkolů státu nebo společnosti. Předmětem ochrany je na rozdíl od ustanovení § 324 trestního zákoníku jednotlivec, nositel pravomoci úřední osoby, tj. osoby, které plní úkoly státu nebo společnosti a používají při tom svěřené pravomoci pro plnění těchto úkolů. [TRZII]

4.5 Násilí proti skupině obyvatelů a proti jednotlivci dle § 352 tr. zákoníku

(1) Kdo skupině obyvatelů vyhrožuje usmrcením, ublížením na zdraví nebo způsobením škody velkého rozsahu, bude potrestán odnětím svobody až na jeden rok.

(2) Kdo užije násilí proti skupině obyvatelů nebo jednotlivci nebo jim vyhrožuje usmrcením, ublížením na zdraví nebo způsobením škody velkého rozsahu pro jejich

skutečnou nebo domnělou rasu, příslušnost k etnické skupině, národnost, politické přesvědčení, vyznání nebo proto, že jsou skutečně nebo domněle bez vyznání, bude potrestán odnětím svobody na šest měsíců až tři léta.

(3) Stejně jako v odstavci 2 bude potrestán, kdo se spolčí nebo srotí ke spáchání takového činu. [TRZII]

Toto ustanovení chrání klidné občanské soužití proti vyhrožování usmrcením, ublížením na zdraví nebo způsobením škody velkého rozsahu nebo i proti použití násilí, které však nelze realizovat prostřednictvím Internetu. V odstavci 2 je tato ochrana specifikována, jde-li o útoky motivované rasovou, etnickou, národností nebo jinou podobnou příslušností ke skupině obyvatel. Při takovém jednání nerozhoduje, zda je jednání pachatele vedeno pohnutkou, která je založena na opravdové příslušnosti jednotlivce nebo skupiny obyvatelů k určité rase, etnické skupině, národnosti, politickému přesvědčení nebo vyznání, anebo zda tak jen usuzuje z určitých znaků vztahujících se ke konkrétnímu jednotlivci nebo skupině obyvatelů. Vyhrožování násilím může být stejně jako skutkové podstaty trestného činu vydírání směřováno do budoucnosti, nemusí být bezprostřední. Zároveň není třeba, aby výhrůžka skutečně vzbudila obavu u adresáta. Musí však být objektivně způsobilá vyvolat obavu z provedení toho, čím se hrozí. Adresát výhrůžky nemusí být přítomen, je však třeba, aby se o ní mohl alespoň dovědět. Ve věci je třeba zvážit, zda jednání pachatele směřuje proti jednotlivci, nebo proti skupině obyvatelů. V praxi totiž výhrůžka, která na první pohled směřuje podle svého doslovného znění vůči jednotlivci, může být ve skutečnosti a podle svého smyslu zaměřena proti skupině osob a naopak. Pro zhodnocení skutečného smyslu pachatelova projevu je důležitý poměr k osobě, proti které výhrůžky působí, a k celé skupině obyvatelů, pohnutka jeho projevu, předcházející jednání pachatele i osoby či osob, proti nimž výhrůžka směřuje, apod.. Spolčení nebo srocení ke spáchání činu uvedenému v odstavci 2 je vlastně forma přípravy, která je povýšena na dokonaný trestný čin. Toto ustanovení proto postihuje jako samostatný trestný čin (předčasně dokonaný) jednání spočívající v tom, že se pachatel spolčí nebo srotí proto, aby jednal, jak je vymezeno v odstavci 2, aniž by k tomuto popsanému jednání došlo. Proto je skutková podstata trestného činu uvedeného v § 352 odst. 3 naplněna a uvedený trestný čin je dokonán, došlo-li ke spolčení a srocení, aniž by

již k užití násilí nebo vyhrožování, jak předpokládá odstavec 2, došlo, jestliže však k tomu cíli spolčení a srocení směřovalo. [TRZII]

4.6 Nebezpečné vyhrožování dle § 353 tr. zákoníku

(1) Kdo jinému vyhrožuje usmrcením, těžkou újmou na zdraví nebo jinou těžkou újmou takovým způsobem, že to může vzbudit důvodnou obavu, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.

(2) Odnětím svobody až na tři léta nebo zákazem činnosti bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1
a) jako člen organizované skupiny,
b) vůči dítěti nebo těhotné ženě,
~~c) se zbraní,~~
d) na svědkovi, znalci nebo tlumočníkovi v souvislosti s výkonem jejich povinnosti, nebo
e) na zdravotnickém pracovníkovi při výkonu zdravotnického zaměstnání nebo povolání nebo na jiném, který plnil svoji obdobnou povinnost vyplývající z jeho zaměstnání, povolání, postavení nebo funkce nebo uloženou mu podle zákona. [TRZII]

Objektem tohoto trestného činu je zájem na ochraně jednotlivce proti některým závažným výhrůžkám. Obsah výhrůžky je zde specifikován usmrcením, těžkou újmou na zdraví nebo jinou těžkou újmou. Jako jinou těžkou újmu lze brát újmu srovnatelnou s důsledky, které nastávají při usmrcení nebo těžké újmy na zdraví

Jiná těžká újma musí být posuzována jednak s přihlédnutím k těžkým újmám v tomto ustanovení výslovně uvedeným (usmrcení, těžká újma na zdraví) a jednak ke specifickým okolnostem konkrétního případu s přihlédnutím i k tomu, jakým způsobem subjektivně pociťuje osoba, které je vyhrožováno. Za vyhrožování jinou těžkou újmou lze považovat například vyhrožování způsobení škody velkého rozsahu nebo škody na věci vysoké umělecké hodnoty, ke které má navíc osoba poškozená větší citový vztah. Zároveň se v případě jiné těžké újmy může jednat o vyhrožování usmrcením či těžké újmy na zdraví v souvislosti s osobou blízkou. Také se může jednat o únos osoby blízké. Klíčové pro posuzování nebezpečnosti je vzbuzení důvodné obavy z naplnění toho, čím je vyhrožováno. Důvodná obava je přitom chápána jako vyšší stupeň tísnivého pocitu ze zla,

kterým je vyhrožováno. Z výkladu k tomuto ustanovení zároveň vyplývá, že důvodná obava nemusí vzniknout, ale její vznik musí být reálný, proto je třeba pečlivě hodnotit povahu a závažnost vyhrožování. Je třeba odlišit nebezpečné vyhrožování od projevů, při kterých je sice použito silných slov, ale ve skutečnosti vzhledem k povaze se o nic vážnějšího nejedná. V praxi bývá posuzování toho, zda dané výroky vzbuzují důvodnou obavu, obtížné, neboť výhrůžky je třeba posuzovat s ohledem na konkrétní okolnosti případu, zejména k povaze výhrůžky, k fyzickým a charakterovým vlastnostem pachatele ve srovnání s fyzickými a povahovými rysy poškozeného, k jejich vzájemnému vztahu a dalších skutečností. Například z okolnosti, že výhrůžka byla adresována starší osamělé ženě nebo dítěti, lze usuzovat, že vyhrožování bylo způsobilé vzbudit důvodnou obavu. Podobně v případě, kdy bylo vyhrožování doprovázeno projevy, které ilustrovaly odhodlání pachatele výhrůžky naplnit (např. výhrůžka usmrcením nebo způsobením těžké újmy na zdraví doprovázená výhružným manipulováním s nožem), bude též možné dovodit, že byla způsobilá vzbudit důvodnou obavu.

Není třeba, aby ten, kterému je vyhrožováno, byl výhrůžkám přímo přítomen. Postačí, pokud je výhrůžka směřovaná poškozenému takovým způsobem, při kterém si je pachatel vědom toho, že se poškozený o této dozví, např. za užití další osoby, telefonicky, faxem apod.. Toto zakládá možnost i využití sítě Internet, kdy vyhrožování může být provedeno prostřednictvím elektronické pošty nebo například prostřednictvím sociální sítě. [TRZII]

4.7 Nebezpečné pronásledování dle § 354 tr. zákoníku

(1) Kdo jiného dlouhodobě pronásleduje tím, že
a) vyhrožuje ublížením na zdraví nebo jinou újmou jemu nebo jeho osobám blízkým,
~~b) vyhledává jeho osobní blízkost nebo jej sleduje,~~
c) vytrvale jej prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontaktuje,
d) omezuje jej v jeho obvyklém způsobu života, nebo
e) zneužije jeho osobních údajů za účelem získání osobního nebo jiného kontaktu, a toto jednání je způsobilé vzbudit v něm důvodnou obavu o jeho život nebo zdraví nebo o život a zdraví osob jemu blízkých, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.

(2) Odnětím svobody na šest měsíců až tři roky bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1
a) vůči dítěti nebo těhotné ženě,
~~*b) se zbraní, nebo*~~
~~*c) nejméně se dvěma osobami.*~~ [TRZII]

Pokud jde o postižitelnost za jednání zahrnuté pod pojmem nebezpečné pronásledování v České republice, tak lze říci, že toto bylo možné již před 01.01.2010. Před tímto datem však bylo možné postihovat spíše dílčí útoky, vlastní podstata tohoto jednání nebyla reflektována a v praxi tak často docházelo k obtížnému řešení tohoto protiprávního jednání. K nápravě došlo právě dne 01.01.2010, kdy nabyl účinnosti nový trestní zákoník, čímž pod hrozbou trestní sankce vznikl nový trestný čin nebezpečného pronásledování, v zahraničí označován jako stalking. Tímto se Česká republika zařadila mezi země s tzv. antistalkingovou legislativou, mezi které dále patří Rakousko, Německo a Itálie. Cílem této legislativy je pomocí trestního práva ohroženým osobám zajistit efektivní ochranu před nebezpečnými útoky, které nepřípustně zasahují do jejího života. Termín stalking byl použit již v 90. letech v USA, kdy označoval určitý soubor charakteristik jednání člověka. Doslovným překladem je stalking vykládán jako činnost pronásledování, stopování divoké zvěře, což dobře vystihuje podstatu tohoto termínu s tím rozdílem, že namísto zvěře vystupuje lidská bytost, která je působení stalkera vystavena útokům nezřídka končícím tragicky, stejně jako je tomu u úspěšného lovu. První definice stalkingu vycházející z klinických studií vznikly již v první polovině 90. let. Označily pojem stalking jako úmyslné, zlovolné a opakované pronásledování s obtěžováním jiné osoby. V odborné, zejména psychiatrické a psychologické praxi, se stalkingem rozumí způsob chování, kdy se pachatel zaměří na nějakého člověka, po kterém slídí, obtěžuje a pronásleduje jej, je mu vyhrožováno, je často fyzicky napadán a v některých případech dokonce usmrcen. U obětí jsou tímto jednáním pachatele vyvolávány pocity strachu. [TRZII]

Průběžným vyvoláváním pocitů strachu u obětí stalkingu těmto způsobuje vážné psychické následky. Konkrétně se jedná o poměrně vážné příznaky traumatizace projevující se přes poruchy spánku a koncentrace až po emocionální labilitu, úzkost apod.. Významný statistický údaj říká, že jedna čtvrtina obětí stalkingu má suicidiální myšlenky a zároveň sociální dopady jsou značné. Oběti jsou ze strachu nuceni měnit své každodenní návyky, kdy polovina z nich se cítí na to, změnit své bydliště nebo pracoviště, aby se tak ukryla před pronásledovatelem. Z jednoho výzkumu provedeného v souvislosti s

psychickou zátěží obětí stalkingu vyplývá, že tito pronásledovaní trpí posttraumatickou stresovou poruchou v takovém stupni, který odpovídá psychickému stavu osob, kteří přežili leteckou katastrofu. [ČÍR2008]

Moderní styl života v informační společnosti sám o sobě vytváří pro pronásledování vhodné podmínky. Zejména síť Internet nabízí vcelku nenáročné a jednoduché možnosti, jak obtěžovat vyhlédnuté cíle v podobě osob. Stalker může svou oběť systematicky deptat bez velkých nákladů a často z pohodlí domova. Přitom je nepopiratelné, že tyto nevyžádané kontakty, které nemají věcný důvod a od počátku je zřejmé, že jsou pouze obtěžující, bez vyžádání a často i proti samotné vůli pronásledované oběti, přesahují únosnou společenskou hranici. V souvislosti s naplňováním skutkové podstaty Nebezpečné pronásledování ve smyslu § 354 trestního zákoníku prostřednictvím sítě Internet se hovoří o tzv. kybestalkingu, který tedy představuje speciální podobu stalkingu. Tento pojem použil poprvé v roce 1999 Deirmenjian a charakterizoval ho jako stalking v kybernetickém prostoru, tedy pronásledování prostřednictvím Internetu. Ke kyberstalkingu patří zejména:

- zasílání obtěžujících e-mailů,
- negativní zprávy o oběti v různých chat-roomech,
- nevyžádané, zlovolné prezentace oběti na různých místech v Internetovém prostoru,
- vyhrožování prostřednictvím Internetu, elektronická sabotáž (zavirování počítače, slídění v počítači oběti, odcizování elektronických dat). [ČÍR2008]

Internet nabízí opravdu široké spektrum možností pro stalkery, jak anonymně dlouhodobě a systematicky obtěžovat cílovou oběť. U kyberstalkingu, stejně jako u jiných forem nebezpečného pronásledování, je pravděpodobnější, že pachatelem, tj. stalkerem, bude osoba mužské pohlaví a obětí žena. Zároveň se z praxe ukazuje, že pronásledovatel a osoba pronásledovaná se znají z reálného světa a v minulosti měli bližší nebo dokonce intimní vztah. Čistě internetové známosti, které se později překlopí do stalkingu, jsou spíše výjimečné. [ČÍR2008]

Z pohledu legislativy představuje objekt toho trestného činu ochranu narušeného mezilidského soužití konkretizovaného u nebezpečného pronásledování ochrannou tělesné

a duševní integrity, osobní svobody a soukromí každého jedince. Objektivní stránka tohoto trestného činu obsahuje dlouhodobé pronásledování jiné osoby, které je prováděno v konkrétních, zákonem přesně stanovených formách jednání, které jsou v oběti způsobilé vzbudit důvodnou obavu o život, zdraví oběti nebo život a zdraví osob oběti blízkých. Musí se jednat o dlouhodobé pronásledování, které musí být prováděno tak intenzivně, že to již ohrožuje psychickou a v některých případech i fyzickou integritu člověka. Na počátku se ještě nemusí jednat o zřetelně patologické, asociální chování. Hranici mezi tím, co je ještě společensky akceptovatelné a co již je třeba posuzovat jako patologické, sociálně škodlivé chování, není vždy snadné rozlišit. K překročení této hranice může dojít nenápadným způsobem, kdy jednání stalkera postupně nabývá na intenzitě a teprve od určitého okamžiku se pro oběť stává nebezpečným. Taková hranice je nepochybně překonána například v případě, že se pronásledovatel bezvýsledně snaží získat přízeň oběti, navzdory tomu, že v jejím pronásledování v řádu měsíců až let proti její vůli pokračuje, popřípadě když se začne vůči oběti chovat násilně. Dlouhodobostí ve smyslu tohoto ustanovení je třeba rozumět přinejmenším několik vynucených kontaktů nebo pokusů o ně, které zároveň musejí být způsobilé v oběti vyvolat důvodnou obavu. Z tohoto vyplývá, že ojedinělé nebo náhodné nevyžádané kontakty, byť jsou nežádoucí, tyto požadavky nesplňují. Zpravidla se v praxi bude jednat o systematicky, soustavně a vytrvale prováděná jednání, která vybočují z běžných norem lidského chování, které mohou v některých případech gradovat. Vysoká frekvence těchto různorodých projevů jako je posílání dárků, sexuálně nepřístojné e-maily, otrávení domácího zvířete, spamové zahlcení schránky elektronické pošty, čekání před domem, a dalších jsou prováděny s úmyslem pachatele změnit obvyklý způsob života oběti, ohrozit jeho duševní rovnováhu, postupně jej dostat pod svůj bezvýhradní vliv a moc. V případě vyšší frekvence provádění těchto jednání, tj. jednotlivých forem nebezpečného pronásledování, tím kratší může být období, které je pak posuzováno jako dlouhodobé pronásledování. Všechny výše uvedené skutečnosti by měly být zvažovány při hodnocení, zda byla v konkrétním případě splněna podmínka dlouhodobosti nebezpečného pronásledování ve smyslu § 354 trestního zákoníku nebo se jednalo o pouhý exces v chování krátkodobé, jednorázové povahy. [TRZII]

V souvislosti s naplňováním této skutkové podstaty s využitím sítě Internet bude do dílčích jednání, tj. forem nebezpečného pronásledování patřit například nevyžádané zasílání zpráv elektronické pošty často s vulgárním nebo agresivním obsahem, zahlcování

schránky elektronické pošty spamy, záměrná distribuce virů do počítače oběti, opakované vzkazy, volání prostřednictvím různorodých komunikačních softwarů jako je například skype či icq apod.. Omezováním v obvyklém způsobu života je pak takové omezení dosavadního života oběti, ke kterému dochází proti jeho vůli formou nežádoucích zásahů pachatele do oblastí jejího osobního, rodinného, ale i profesního života, kdy nemusí být zasahováno do všech těchto oblastí. Rozhodující zde bude vždy subjektivně pociťovaná újma poškozeného, byť určitým způsobem objektivizována, nikoliv tedy hodnocení podle jakéhosi „zprůměrovaného" obvyklého způsobu života, neboť může být rozdílně pojato sledování kantora svým žákem na každém kroku v porovnání se sledováním slavného herce jeho obdivovatelem. U sledování slavného herce, by pak zjednodušeně řečeno bylo třeba obecně pro naplnění skutkové podstaty nebezpečného pronásledování větší intenzity obtěžování. [TRZII]

5. Mravnostní trestné činy kybernality

Mravností se rozumí soubor jednání, která odpovídají přijatým společenským pravidlům a hodnotám dané morálky, zejména pokud jsou taková jednání v rozporu s okamžitým prospěchem či zájmem jednajícího. Mravnostní trestné činy vzhledem k jejich dopadům na chráněný zájem jsou zařazovány mezi nejzávažnější trestné činy vůbec. Mravnostní kriminalita totiž hluboce zasahuje do nejcitlivější sféry osobní integrity. Jedná se tedy o skupinu trestných činů, jejichž typickým obsahem je protiprávní zasahování do sféry svobodného rozhodování o pohlavním styku, mravního a tělesného vývoje. O to nebezpečnější jsou tato jednání v případech, kdy se v osobách obětí jedná o děti, které jsou takovým zásahem mnohem více traumatizováni. V takových případech tato jednání zanechávají velmi často trvalé následky na zdraví oběti, a to jak v podobě tělesného poškození, tak i traumatizujícího psychického poškození. Nejčastějším prostředkem nátlaku na oběť je zde užití násilí, které je však na rozdíl od násilné kriminality prostředkem k narušení svobody rozhodování v pohlavních vztazích, či narušení mravního a tělesného vývoje dětí. Násilí zde může mít a u mravnostní kybernality zpravidla má povahu pohrůžky násilím, tj. povahu psychického nátlaku na oběť. V následujících podkapitolách jsou uvedeny skutkové podstaty mravnostní kriminality, které mohou být spáchány prostřednictvím sítě Internet. U některých skutkových podstat jsou některé jejich části přeškrtnuté, což značí skutkové podstaty, které mohou být stěží spáchány prostřednictvím sítě Internet. [CHM2003]

5.1 Sexuální nátlak dle § 186 tr. zákoníku

(1) Kdo jiného násilím, pohrůžkou násilí nebo pohrůžkou jiné těžké újmy donutí k pohlavnímu sebeukájení, k obnažování nebo jinému srovnatelnému chování, bude potrestán odnětím svobody na šest měsíců až čtyři léta nebo zákazem činnosti.

(2) Stejně bude potrestán pachatel, který přiměje jiného k pohlavnímu styku, k pohlavnímu sebeukájení, k obnažování nebo jinému srovnatelnému chování zneužívaje jeho závislosti, jeho bezbrannosti nebo svého postavení a z něho vyplývající důvěryhodnosti nebo vlivu.

(3) Odnětím svobody na jeden rok až pět let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2
a) na dítěti, nebo
~~b) nejméně se dvěma osobami.~~

(4) Odnětím svobody na dvě léta až osm let bude pachatel potrestán,
~~a) spáchá-li čin uvedený v odstavci 1 se zbraní,~~
~~b) spáchá-li čin uvedený v odstavci 1 nebo 2 na osobě ve výkonu vazby, trestu odnětí svobody, ochranného léčení, zabezpečovací detence, ochranné nebo ústavní výchovy anebo v jiném místě, kde je omezována osobní svoboda, nebo~~
~~c) spáchá-li takový čin jako člen organizované skupiny.~~

(5) Odnětím svobody na pět až dvanáct let bude pachatel potrestán,
a) spáchá-li čin uvedený v odstavci 1 na dítěti mladším čtrnácti let, nebo
~~b) způsobí-li takovým činem těžkou újmu na zdraví.~~

~~(6) Odnětím svobody na deset až patnáct let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 nebo 2 smrt.~~

(7) Příprava je trestná. [TRZII]

Podstata trestného činu sexuální nátlak dle § 186 trestního zákoníku je upravena tak, že přejímá právní úpravu trestného činu vydírání, uvedeného v kapitole 4.1 této diplomové práce, konkrétně část uvedenou v odstavci 1 vydírání („kdo jiného násilím, pohrůžkou násilí nebo pohrůžkou jiné těžké újmy donutí“) a tuto dále rozšiřuje i na pohlavní ukájení, obnažování nebo jiné srovnatelné chování. Takové jednání je postihováno i v případě, že pachatel k takovému chování přiměje jiného zneužívaje jeho bezbrannosti. Je zde tedy doplněna ochrana i proti dalším formám sexuálního zneužívaní tak, aby byla zjištěna ochrana i před takovým v praxi se též vyskytujícím jednáním. Tato právní úprava je zároveň provedením rámcového rozhodnutí Rady Evropské unie 2004/68/SVV o boji proti sexuálnímu zneužívání dětí a dětské pornografii. Tato skutková podstata také naplňuje požadavky návrhu Úmluvy Rady Evropy o ochraně dětí před sexuálním vykořisťováním a sexuálním zneužíváním. S pomocí této právní úpravy je zde tedy dána možnost postihu i u méně závažných forem sexuálního zneužívání dětí v případě, že pachatel zneužije závislosti dítěte, jeho bezbrannosti (tj. zvláštní zranitelnosti zejména fyzického či mentálního postižení) nebo svého postavení a z něho vyplývající důvěryhodnosti nebo vlivu. Právní úprava trestného činu sexuální nátlak tak efektivně plní závazky České republiky vůči Evropské unii a Radě Evropy. U všech skutkových podstat,

jež jsou obsahem tohoto ustanovení, není postihováno stejné jednání, ale liší se ve své povaze a účinku na oběť. V prvním případě odstavce 1 tohoto ustanovení je postihováno jednání spočívající v donucení pachatelem pohrůžkou násilí nebo jiné těžké újmy, kdežto ve druhém případě u skutkové podstaty odstavce 1 a odstavce 2 spočívá jednání pachatele v tom, že jiného přiměje. [TRZII]

Jak ze znění samotného ustanovení vyplývá, objektem tohoto trestného činu je svoboda rozhodování v pohlavních vztazích, neboť naplnění skutkové podstaty trestného činu sexuální nátlak dle § 186 trestního zákoníku má zpravidla nepříznivý vliv na mravní vývoj zneužité osoby. Protože bylo do trestního zákoníku zahrnuto chování pachatele, kterým tento donutí oběť k pohlavnímu sebeukájení, k obnažování nebo jiným srovnatelným chováním, zvýšeně chrání oběti sexuálních útoků, které jsou vystaveny chování, při němž nedochází k fyzickému pohlavnímu kontaktu s pachatelem, ale pachatel je nutí, aby ony sami prostřednictvím svého těla a na něm prováděných sexuálních nebo erotických úkonů nebo jeho obnažováním působily na sexuální vnímání pachatele. Na tomto se pachatel sám přímo nepodílí, ale poté, co k tomuto jednání svou oběť přinutí, tak toto pozoruje, aby se tak sexuálně vzrušoval. V souvislosti s Internetem může být trestný čin sexuální nátlak spáchán například za běhu webkamery v kombinaci s komunikačním softwarem Skype. Sebeukájením je v souvislosti se sexuálním nátlakem myšleno takové chování, při kterém osoba pohlavně ukájí samu sebe drážděním vlastních pohlavních orgánů. Obnažováním je myšleno vysvlékání se oběti, při kterém se stávají viditelným takové části těla, které z estetických a tradičních důvodů bývají zakryty. Jde tedy o vysvlékání jednotlivých částí oděvu prováděné za účelem sexuálního vzrušení pachatele, kdy jsou odhalovány zejména eroticky významné části těla. [TRZII]

5.2 Šíření pornografie dle § 191 tr. zákoníku

(1) Kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, v němž se projevuje násilí či neúcta k člověku, nebo které popisuje, zobrazuje nebo jinak znázorňuje pohlavní styk se zvířetem, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Kdo písemné, fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo
a) nabízí, přenechává nebo zpřístupňuje dítěti, nebo
b) na místě, které je dětem přístupné, vystavuje nebo jinak zpřístupňuje, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(3) Odnětím svobody na šest měsíců až tři léta bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2
a) jako člen organizované skupiny,
b) tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně
účinným způsobem, nebo
c) v úmyslu získat pro sebe nebo pro jiného značný prospěch.

(4) Odnětím svobody na jeden rok až pět let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2
a) jako člen organizované skupiny působící ve více státech, nebo
b) v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu. [TRZII]

Objektem trestného činu šíření pornografie dle § 191 odstavce 1 trestního zákoníku je zájem na ochraně mravopočestnosti dospělých před obtěžováním tzv. tvrdou pornografií. Oproti tomu odstavec 2 tohoto ustanovení chrání zájem na ochraně mravního rozvoje a výchovy mládeže proti negativnímu působení pornografie. Je tedy tímto ustanovením omezeno právo na svobodu projevu, vyhledávání a šíření informace. Pro potřeby tohoto ustanovení je pornografickým dílem myšleno takové dílo, které zvláště intenzivním a vtíravým způsobem zasahuje a podněcuje sexuální pud, překračuje podle převládajících názorů ve společnosti uznávané hranice sexuální slušnosti, uráží nepřijatelným způsobem cit pro sexuální slušnost, vyvolává pocit studu. Při posuzování musejí být tedy splněny dvě podmínky a to, zda celkový dojem posuzovaného díla působí morální pohoršení osobě s „běžným" cítěním a zda toto dílo podněcuje sexuální pud. Samotné zobrazení nahého lidského těla tedy vždy nemusí představovat pornografické dílo, i když by mohlo vzbuzovat sexuální vzrušení. Posuzování pornografického díla je někdy závislé na kontextu, ve kterém je dílo publikováno, nikoli však na tom, komu je předkládáno ani na záměru autora. Za pornografické dílo zároveň nemůže být považováno umělecké, historické a vědecké dílo. Pro určení pornografického charakteru je důležitý obsah celého díla, nikoli pouze určité části, výseče, kapitoly apod.. Pokud jde o šíření jiné než tvrdé a dětské pornografie v jakýchkoli podobách, tak toto se ve smyslu české legislativy

nepovažuje za trestné. Za pohlavní styk se zvířetem je považován jakýkoliv způsob ukájení pohlavního pudu na zvířeti. Jedná se zejména o sodomii, tj. pohlavní styk se zvířetem (spojení pohlavních orgánů člověka a zvířete), a zoofilii, tj. dotyk a hlazení zvířete vedoucí k pohlavnímu ukojení. [TRZII]

V souvislosti s informačními technologiemi se po právní stránce veřejně přístupnou počítačovou sítí rozumí funkční propojení počítačů do sítí s cílem vytvořit informační systém pracující s tzv. dálkovým přístupem, jakým je především Internet a jiné podobné informační systémy. Jedná se o veřejně přístupnou počítačovou síť tvořenou soustavou serverů, datových propojení a k nim připojených počítačů. Z pohledu organizačního jde o spojení prvků jako jsou provozovatelé jednotlivých sítí a podsítí, zprostředkovatelé připojení, jednotlivé uživatele a další subjekty. Webové stránky jsou z tohoto pohledu elektronické dokumenty nacházející se na určitých serverech, jejichž obsah je propojen pomocí hypertextových odkazů na jiná místa těchto dokumentů, na jiné dokumenty serveru nebo na dokumenty jiných serverů nacházejících se v síti Internet. Za takovou síť není považována např. uzavřená počítačová síť některé z právnických osob nebo jiné organizace, neboť nesplňuje podmínku veřejné přístupnosti. [TRZII]

5.3 Výroba a jiné nakládání s dětskou pornografií dle § 191 tr. zákoníku

(1) Kdo přechovává fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě, bude potrestán odnětím svobody až na dva roky.

(2) Kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě, anebo kdo kořistí z takového pornografického díla, bude potrestán odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(3) Odnětím svobody na dvě léta až šest let nebo propadnutím majetku bude pachatel potrestán, spáchá-li čin uvedený v odstavci 2
a) jako člen organizované skupiny,
b) tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně
účinným způsobem, nebo
c) v úmyslu získat pro sebe nebo pro jiného značný prospěch.

(4) Odnětím svobody na tři léta až osm let nebo propadnutím majetku bude pachatel potrestán, spáchá-li čin uvedený v odstavci 2
a) jako člen organizované skupiny působící ve více státech, nebo
b) v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu. [TRZII]

Objekt ustanovení § 192 trestního zákoníku se týká zájmu společnosti na ochraně mravního vývoje dětí a ochraně před jejich sexuálním zneužíváním. Dětskou pornografií je zde myšleno podle trestního zákoníku pornografické dílo zobrazující nebo jinak využívající dítě. Za tato díla lze považovat například snímky obnažených dětí v polohách vyzývavě předvádějících pohlavní orgány za účelem sexuálního uspokojení, dále pak snímky dětí zachycující polohy skutečného či předstíraného sexuálního styku s nimi, popř. i jiné obdobně sexuálně dráždivé snímky dětí. V případě, že se nejedná o výše uvedené pornografické snímky a přesto jsou posuzovaná díla účelem uspokojení osob trpících sexuální deviací, v těchto případech osob, pro které jsou sexuálně atraktivní nedospělé osoby, nelze tyto fotografie považovat za materiály zobrazující dětskou pornografii. Dítětem je ve smyslu trestního zákoníku považována osoba mladší osmnácti let. Podobně jako u výše uvedených mravnostních trestných činů k postihu dětské pornografie zavazuje Českou republiku celá řada mezinárodních smluv i legislativa EU. Patří mezi ně hlavně Opční protokol k Úmluvě OSN o právech dítěte proti obchodováním s dětmi, dětské prostituci a dětské pornografii ze dne 25. května roku 2000, o Úmluvu o kybernetické kriminalitě, Budapešť, ze dne 23. listopadu 2001 (zejména článek 9) a o Úmluvu Rady Evropy o ochraně dětí před sexuálním vykořisťováním a zneužíváním ze dne 25. října 2007. V souvislosti s Evropskou unií se jedná o rámcové rozhodnutí Rady EU 2004/68/SVV o boji proti sexuálnímu zneužívání dětí a dětské pornografii. Přechovávání dětské pornografie je kriminalizováno, neboť její společenská nebezpečnost je vážnější oproti jiným formám pornografie. Postihují se tedy i konzumenti dětské pornografie, přičemž nezáleží na způsobu a délce přechovávání těchto pornografických materiálů. Nevyžaduje se, aby měl pachatel dětskou pornografii přímo u sebe, postačí, že ji má ve své moci. V souvislosti se sítí Internet tedy postačuje, pokud pachatel si tyto materiály uchovává prostřednictvím účtu elektronické pošty nebo za užití jiné služby nějakého ze serverů Internetu. V případě, že uživatel sítě Internet při vyhledávání jiných stránek náhodně narazí na s stránky s dětskou pornografií, tak její prohlížení není trestné, pokud obsah těchto stránek není ukládán na nosič informací. Většina Internetových prohlížečů je

založena na principu automatického ukládání webových stránek nebo jiných dat do vyrovnávací paměti počítače. Tyto dočasné soubory nebo vytvořené cookies nelze považovat za přechovávání ve smyslu tohoto zákona. Na hraně je situace, kdy si bude uživatel cíleně a pravidelně prohlížet konkrétní stránky s dětskou pornografií. V zásadě lze říci, že toto není trestné, neboť obsah těchto webů není v dispozici uživatele, který tyto stránky navštěvuje. Toto samozřejmě však nemá vliv na provozovatele těchto serverů, kteří vědomě tyto pornografické materiály vystavují. Z předmětného ustanovení a v něm uvedených trestních sazeb zároveň vyplývá, že závažnější než přechovávání dětské pornografie je její šíření, které je také považováno za společensky nebezpečnější než šíření tvrdé pornografie. [TRZII]

5.4 Zneužití dítěte k výrobě pornografie dle § 193 tr. zákoníku

(1) Kdo přiměje, zjedná, najme, zláká, svede nebo zneužije dítě k výrobě pornografického díla nebo kořistí z účasti dítěte na takovém pornografickém díle, bude potrestán odnětím svobody na jeden rok až pět let.

(2) Odnětím svobody na dvě léta až šest let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1
a) jako člen organizované skupiny, nebo
b) v úmyslu získat pro sebe nebo pro jiného značný prospěch.

(3) Odnětím svobody na tři léta až osm let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1
a) jako člen organizované skupiny působící ve více státech, nebo
b) v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu. [TRZII]

Objektem tohoto trestného činu je kromě zájmu společnosti na ochraně dětí před sexuálním zneužíváním a zájmu na řádném mravním vývoji dětí, jako je tomu u předchozího uváděného ustanovení, je i svoboda rozhodování. S větší pečlivostí se tímto ustanovením chrání osoby mladší 18 let proti zneužití pachatelem k výrobě pornografického díla, neboť samotná výroba nemusí vždy zahrnovat zneužití takové osoby. Důvodem je skutečnost, že výrobou je myšleno i samotné rozmnožování pornografických fotografií nebo střih a jiné zpracování takových filmových děl, výroba pornografických videokazet či DVD z již hotového původního materiálu. Dítětem je zde myšlena taktéž

osoba mladší osmnácti let. Dalším pojmem užitým v tomto ustanovení je zjednání, čímž se rozumí uzavření dohody mezi dítětem a pachatelem, že se dítě bude přímo účastnit výroby při výrobě pornografického díla, kdy dohoda je podmíněna souhlasným projevem vůle obou stran. Najmutí je pak speciální případ zjednání, při kterém se jedná taktéž o dohodu, jejímž znakem je ovšem úplata, která nemusí mít pouze podobu peněžních prostředků. Další formou je zlákání, které je považováno za získání dítěte k účasti zejména nabízením nebo předstíráním konkrétních výhod. Nejedná se však o úplatu. Jednání, kdy pachatel úmyslně vzbudí, a to jiným způsobem než zlákáním, v osobě mladší osmnácti let rozhodnutí účastnit se výroby pornografického díla, se nazývá svedením. Neoznámení naplnění skutkové podstaty tohoto ustanovení trestního zákoníku je trestné. [TRZII]

5.5 Svádění k pohlavnímu styku dle § 202 tr. zákoníku

(1) Kdo nabídne, slíbí nebo poskytne dítěti nebo jinému za pohlavní styk s dítětem, pohlavní sebeukájení dítěte, jeho obnažování nebo jiné srovnatelné chování za účelem pohlavního uspokojení úplatu, výhodu nebo prospěch, bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem.

(2) Odnětím svobody na šest měsíců až pět let bude pachatel potrestán,
a) spáchá-li čin uvedený v odstavci 1 na dítěti mladším čtrnácti let,
b) spáchá-li takový čin ze zavrženíhodné pohnutky,
c) pokračuje-li v páchání takového činu po delší dobu, nebo
d) spáchá-li takový čin opětovně. [TRZII]

Objektem trestného činu svádění k pohlavnímu styku je zájem na řádné výchově a ochraně dětí, a to proti útokům svádění k prostituci, která je České republice v hlubokém rozporu s morálkou občanské společnosti. U trestného činu svádění k pohlavnímu styku je stejně jako u zahraničních právních úprav (např. ve Švédsku nebo v Rakousku) sankcionováno jednání pachatele, který učiní nabídku, slíbí nebo poskytne osobě mladší 18 let nebo jinému za pohlavní styk s dítětem, pohlavní sebeukájení dítěte, jeho obnažování nebo jiné srovnatelné chování úplatu nebo jinou výhodu či prospěch, což ve většině případů vede k výraznému mravnímu poškození takového dítěte a k narušení jeho hodnotového systému. Jeho potrestání v souvislosti se sankcemi tohoto ustanovení je v souladu s trendy, které prohlubují ochranu dětí před takovým jednáním v sexuální oblasti.

Cílem tohoto ustanovení je tedy chránit děti před takovými nežádoucími a společensky nepřijatelnými sexuálními jednáními, kterými jsou v tomto případě sexuální služby, jejichž smyslem je pohlavní uspokojení. Pod tuto skutkovou podstatu nelze zařadit případy, kdy se nejedná o sexuální uspokojení nebo uspokojení pudu, ale důvodem požadavku na např. obnažení dítěte a s tím spojené nabídky finanční nebo jiné úplaty, která je dítěti nabídnuta, je např. natáčení uměleckého filmu nebo vytváření jiného uměleckého díla, např. sochy, obrazu, umělecké fotografie apod., kdy dítě slouží pouze jako model. Sankciováni tedy nemohou být malíři, filmaři, fotografové, a další umělci, kteří bez úmyslu sexuálního uspokojení vytvářejí umělecké dílo, kterému je předlohou dítě v takových situacích a pózách, kterých by se jinak tato skutková podstata týkala. Objektivní stránka zde spočívá v jednání pachatele, který osobě mladší 18 let nebo jiné osobě za pohlavní styk s dítětem nebo za jeho pohlavní sebeukájení, obnažování nebo jiné srovnatelné chování za účelem pohlavního uspokojení nabídne, slíbí nebo poskytne úplatu nebo jinou výhodu či prospěch. Úplata nabízená pachatelem nemusí být určena přímo dítěti, ale i jiné osobě. Trestní zákoník tímto rozšiřuje okruh osob, ve vztahu ke kterým je úplata, výhoda nebo prospěch ta sexuální služby osoby mladší 18 let nabízena, slíbena nebo poskytnuta tak, že kromě samotného dítěte dopadají na další žádným způsobem neohraničené osoby. Takovou osobou může být kdokoli, tj. jak osoba příbuzná dítěti, tak osoba ve vztahu k němu cizí, tj. kuplíř. V posuzování těchto případů je rozhodné, aby vůči těmto osobám směřovala za poskytnuté sexuální služby dítěte finanční úplata nebo jiná výhoda či prospěch. V jiném srovnatelném chování se může jednat o jednání, které není ani pohlavním stykem, pohlavním sebeukájením nebo obnažováním, např. některé sexuálně patologické praktiky spočívající v sadistickém či masochistickém jednání nebo tzv. pissingu vyžadovaném pachatelem za úplatu nebo jinou výhodu či prospěch. Prosté ukázání nahého těla dítěte bez obnažování před osobou pachatele za účelem jeho sexuálního vzrušení by mohlo být podřazeno pod jiné srovnatelné chování. V předmětném ustanovení ve kvalifikované podstatě je zároveň uveden pojem zavrženíhodná pohnutka, která dle výkladu musí být v zásadním rozporu s morálkou občanské společnosti a svědčí zpravidla o značném morálním narušení pachatele, neboť poukazuje na jeho bezohledné sobectví, bezcitnost a pohrdavý postoj k základním lidským hodnotám. Zavrženíhodná pohnutka charakterizuje subjektivní stránku pachatele. V konkrétních se pak může jednat o sexuální zvrhlost nebo snahu po nízkém ukájení sexuálního pudu anebo o pomstychtivost apod. Za

zavrženíhodnou pohnutku přesto, že se jedná o pro společnost velice škodlivé jednání, tu však nelze považovat „pouhou" snahu ukojit svůj sexuální pud, neboť se v tomto jednání pachatele jedná o základní skutkovou podstatu. [TRZII]

6 Právní nástroje odhalování kybernality

Právní nástroje pro odhalování kybernality či trestné činnosti obecně jsou zakotveny v zákoně č. 141/1961 Sb. o trestním řízení soudním (trestním řádu). Ty, které jsou nejtěsněji spojeny s odhalováním kybernality, budou stručně popsány v následujících podkapitolách. Všechny následující právní nástroje je nutné užívat v souladu se zákonnými podmínkami a to takovým způsobem, aby jejich výstupy mohly být užity jako důkazní prostředky před soudem. [TRŘ2008]

6.1 Domovní prohlídka a prohlídka jiných prostor a pozemků dle § 82 tr. řádu

Domovní prohlídka je metoda kriminalistické praktické činnosti spočívající ve vytipování a následném prověřování míst, tedy domů a bytů, za účelem zajištění osob a věcí důležitých pro trestní řízení. Domovní prohlídka je pro účely trestního řízení velice významná, ale zároveň citlivá, neboť jde vždy o zásah do určitých oblastí lidských práv, které jsou zaručeny Listinou základních práv a svobod, konkrétně o prolomení nedotknutelnosti obydlí. Domovní prohlídku lze tedy dle příslušných ustanovení trestního řádu vykonat, je-li důvodné podezření, že se v bytě nebo jiných prostorách sloužících k bydlení nebo v prostorách k nim náležejících nachází věc nebo osoba důležitá pro trestní řízení. Obdobné je to v případě prohlídky jiných prostor s tím rozdílem, že se prohledávají prostory nesloužící k bydlení namísto bytových prostor. [NĚM2004]

Při výkonu domovní prohlídky či prohlídky jiných prostor, pro jejíž nařízení byly splněny zákonné podmínky, lze mimo jiné v souvislosti s kybernalitou jako věci důležité pro trestní řízení zajistit i výpočetní techniku a záznamová média (nosiče informací), a to i když existuje možnost, že zajištěné nosiče informací obsahují vedle záznamů o skutečnostech důležitých pro trestní řízení i informace o skutečnostech, které se netýkají probíhajícího trestního řízení a ke kterým se váže státem uložená nebo uznaná povinnost mlčenlivosti. [NĚM2004]

Trestní řád dále stanoví, že vykonat domovní prohlídku nebo prohlídku jiných

prostor lze jen po předchozím výslechu toho, u koho nebo na kom se má takový úkon vykonat, a to jen tehdy, jestliže se výslechem nedosáhlo ani dobrovolného vydání hledané věci nebo odstranění jiného důvodu, který vedl k tomuto úkonu. Smyslem předchozího výslechu před provedením domovní prohlídky nebo prohlídkou jiných prostor, jako vážného, byť ze zákonem stanovených podmínek zcela legálního zásahu do ústavně zaručeného základního práva, pak je tento zásah odvrátit. Před samotným provedením domovní prohlídky nebo prohlídky jiných prostor je třeba osobu, u které je tato prohlídka prováděna, poučit o jejich právech a povinnostech vyplývajících z trestního řádu. [TRŘ2008]

6.2 Odposlech a výpis telekomunikačního provozu dle § 88 a § 88a tr. řádu

V případě, že je vedeno trestní řízení pro zvlášť závažný trestný čin nebo pro jiný úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva, může být vydán příkaz k odposlechu a záznamu telekomunikačního provozu, pokud lze důvodně předpokládat, že jím budou získány významné skutečnosti pro trestní řízení a nelze-li sledovaného účelu dosáhnout jinak nebo bylo-li by jinak jeho dosažení podstatně ztížené. Odposlech a záznam telekomunikačního provozu provádí pro potřeby všech orgánů činných v trestním řízení Policie České republiky, konkrétně Útvar zvláštních činností. Bez příkazu k odposlechu a záznamu telekomunikačního provozu může orgán činný v trestním řízení nařídit odposlech a záznam telekomunikačního provozu, nebo jej provést i sám, je-li vedeno trestní řízení pro trestný čin obchodování s lidmi (§ 168 trestního zákoníku), svěření dítěte do moci jiného (§ 169 trestního zákoníku), omezování osobní svobody (§ 171 trestního zákoníku), vydírání (§ 175 trestního zákoníku), únosu dítěte a osoby stižené duševní poruchou (§ 200 trestního zákoníku), násilí proti skupině obyvatelů a proti jednotlivci (§ 352 trestního zákoníku), nebezpečného vyhrožování (§ 353 trestního zákoníku) nebo nebezpečného pronásledování (§ 354 trestního zákoníku), pokud s tím uživatel odposlouchávané stanice souhlasí. V případě potřeby užití telekomunikačního provozu jako důkazu, je třeba, aby jeho součástí byl protokol s údaji uvedenými o místě, času způsobu a obsahu provedeného záznamu, stejně jako orgán, který záznam pořídil. Ty

záznamy, které nebudou sloužit jako důkaz před soudem je policejní orgán povinen označit, spolehlivě uchovat tak, aby byla zajištěna jejich ochrana před neoprávněným zneužitím, a v protokolu, který je založen v trestním spisu poznamenat, kde jsou uloženy. Pokud je vedena jiná trestní věc, než ta, ve které byl odposlech a záznam telekomunikačního provozu proveden, lze záznam jako důkaz užít pouze v případě, že i v této trestní věci je vedeno trestní stíhání pro některý z výše uvedených trestných činů nebo souhlasí-li s tím uživatel odposlouchávané stanice. [TRŘ2008]

Jak ze samotných ustanovení vyplývá, odposlech a záznam telekomunikačního provozu (elektronické komunikace) je za podmínek vymezených v těchto ustanoveních povoleným zásahem do tajemství zpráv podávaných telefonem nebo jiným podobným zařízením, stejně jako jiných zařízeních elektronické komunikace. Jedná se o nástroj sloužící k zajišťování. Základní rozdíl mezi ustanoveními § 88 o odposlechu a záznamu telekomunikačního provozu (elektronické komunikace) a § 88a o zjišťování údajů o uskutečněném telekomunikačním provozu (elektronické komunikace) je v tom, že § 88 směřuje do budoucna, zatímco § 88a se týká již uskutečněného telekomunikačního provozu (elektronické komunikace). Podle toho je třeba v konkrétním případě použít příslušný příkaz, a to buď k odposlechu a záznamu telekomunikačního provozu podle § 88 odst. 1, 2 trestního řádu či nařízení k odposlechu a záznamu telekomunikačního provozu podle § 88 odst. 5 trestního řádu (se souhlasem uživatele odposlouchávané stanice), anebo k zjištění údajů o uskutečněném telekomunikačním provozu podle § 88a odst. 1 trestního řádu, resp. § 88a odst. 2 tr. řádu (se souhlasem uživatele telekomunikačního zařízení). Telekomunikačním provozem se rozumí komunikace s využitím telefonu, telefaxu, mobilního telefonu, vysílačky i jiného telekomunikačního zařízení, včetně zasílání zpráv elektronickou poštou. Pokud jde o zachycení komunikace prostřednictvím elektronické pošty nebo webových stránek, tyto formy odposlechu a záznamu telekomunikačního provozu jsou zatím využívány spíše výjimečně. Sporné je, jak pohlížet na e-mailovou zprávu po jejím vytištění prostřednictvím tiskárny připojené k počítači. Podle některých názorů jde v tomto případě o zásilku ve smyslu § 87c, podle jiných názorů se zase jedná podobně jako u vytištěné faxové zprávy o součást telekomunikačního provozu, jehož výsledek zachycený v listinné podobě. [TRŘ2008]

Pod pojem úmyslné trestné činy, k jejichž stíhání zavazuje vyhlášená mezinárodní smlouva, patří v souvislosti s mravnostní a násilnou trestnou činností páchanou

prostřednictvím sítě Internet tyto:

- násilí proti skupině obyvatelů a proti jednotlivci podle § 196 odst. 2 TrZ (Mezinárodní úmluva o potlačení a trestání zločinu apartheidu – č. 116/1976 Sb.),
- trestný čin ohrožování mravnosti podle § 205 TrZ (Mezinárodní úmluva proti rozšiřování necudných publikací – č. L/1912 ř. z., č. 184/1922 Sb.; Mezinárodní úmluva o potlačování obchodu s necudnými publikacemi a jejich rozšiřování – č. 96/1927 Sb.; Protokol doplňující Úmluvu o potírání obchodu s necudnými publikacemi, Lake Succes, 4. května 1949),
- ochrana dětí, včetně jejich ochrany před sexuálním zneužíváním a zneužíváním v oblasti dětské pornografie apod. [TRŘ2008]

6.3 Využití znalců a odborníků

Při odhalování, objasňování a vyšetřování trestných činů jsou mnohé kriminalisticky významné informace obsažené ve stopách pro orgány činné v trestním řízení nesrozumitelné nebo jednoduše těžko získatelné bez potřebných znalostí či speciálních zařízení. K získání takových informací ze stop, k jejich pochopení a využití je třeba aplikovat specifické metody, prostředky a znalosti z oblasti vědy, techniky, umění nebo řemesel. Těmito specifickými znalostmi disponuje pouze omezený okruh odborníků. Teprve jejich prostřednictvím je možné získat kriminalisticky relevantní informace a zpřístupnit je tak orgánům činným v trestním řízení. Pokud pomineme ty nejjednodušší formy pomoci odborníků jako je konzultativní činnost, mohou orgány činné v trestním řízení využívat služeb odborníků formou odborných vyjádření, která se užívají v jednodušších případech. Tato odborná vyjádření mohou vyhotovovat dle zákona příslušné orgány, za které se v praxi považují např. lékaři, laboratoře, úřady apod. V trestním řízení mohou také odborná vyjádření podávat v oboru kriminalistika často Kriminalistický ústav Praha a odbory kriminalistické techniky a expertíz správ krajů Policie ČR. Vždy se však musí jednat o subjekty s náležitě odbornou kvalifikací. Tou nejvýznamnější formou využívání odborníků je činnost soudních znalců, která je prováděna formou znaleckých posudků. Znalecká činnost je upravena zákonem o znalcích a tlumočnících č. 36/1967 Sb.

a prováděcí vyhláškou Ministerstva spravedlnosti č. 37/1967 Sb., ve znění pozdějších předpisů. V trestním řízení je využívání znalců upraveno trestním řádem. [MUS2001]

Tvorba znaleckého posudku se pomyslně skládá ze 4 částí. První částí je tzv. vstupní etapa, ve které znalec určuje cíle, případně stanovuje metody zkoumání. Na základě dodaných materiálů dokumentuje stav předaných objektů zkoumání, případně dožaduje doplnění těchto objektů nebo informací k nim se vztahujících. Ve druhé etapě, tzv. analyticko-syntetické, dochází k vlastnímu podrobnému zkoumání jednotlivých předaných objektů a jejich součástí. V této etapě v některých znaleckých odvětvích může docházet i ke zničení předmětů zkoumání. Ve třetí etapě, týkající se vyvozování a formulování závěrů znalec, sestavuje závěry zjištěné předchozími fázemi zkoumání. Jedná se tedy o mentálně nejnáročnější část znaleckého zkoumání. Poslední částí je zpracování znaleckého posudku do podoby srozumitelné pro jejich adresáta, tj. pro orgány činné v trestním řízení. Vyhotovený znalecký posudek by poté měl být orgánem činným v trestním řízení vyhodnocován jak z hlediska formálního, tak z hlediska obsahové stránky. [MUS2001]

Znalecký posudek je zvláštním, speciálním, samostatným druhem důkazu. Je nutné tento odlišit od důkazu výpovědí svědka, který totiž vypovídá o skutečnostech týkajících se trestné činnosti, o nichž nabyl vědomost mimo trestní řízení a bez souvislosti s ním. Zatímco znalec se seznamuje se skutečnostmi týkajícími se trestné činnosti (o nichž má podat s použitím svých odborných znalostí posudek) teprve během trestního řízení, a to studiem spisů nebo přítomností při provádění úkonů trestního řízení. Jestliže svědkem určité události byla osoba, která by mohla být v dané trestní věci přibrána jako znalec, vyslechne se tato osoba jako svědek a za znalce se přibere někdo jiný. [TRŘ2008]

V souvislosti s trestním řízením vedeným proti pachateli, který spáchal některý z trestných činů prostřednictvím sítě Internet uvedených v kapitolách 4 a 5 této diplomové práce, se nejčastěji v souvislosti se znaleckým zkoumáním využívá služeb soudních znalců z oboru Kybernetika, odvětví Výpočetní technika. Soudní znalci z tohoto oboru mají zpravidla k dispozici tzv. forenzní laboratoře, kde dochází na základě Opatření dle § 105 trestního řádu ke zkoumání zajištěných stop ukrytých ve výpočetní technice. Když je předpoklad, že bude soudní znalec potřeba již v průběhu zajišťovaní digitálních stop, je možné tohoto přizvat k místu předpokládaného výskytu digitálních stop, tj. zpravidla k ohledání místa činu nebo na místo provedení domovní prohlídky či prohlídky jiných

prostor. Výstupem práce soudních znalců je pak znalecký posudek, v jehož závěrech jsou odpovědi na předem položené otázky policejního orgánu. Z těchto závěrů se poté často odvíjí další postup v trestním řízení a to podle toho, zda se povede potvrdit předem dané podezření ze spáchání nějakého trestného činu, jehož znaky jsou uvedeny v trestním zákoníku, nebo se toto podezření nepotvrdí a pak následuje odložení věci, případně zastavení trestního stíhání. [RAC2005]

7 Kybernalita a kriminalistika

V odborné literatuře se lze setkat s mnohými definicemi kriminalistiky, kdy v souhrnu lze říci, že:

"Kriminalistika je samostatný vědní obor sloužící ochraně občanů a státu před trestnými činy tím, že objasňuje zákonitosti vzniku, trvání a zániku stop a zákonitosti vyhledávání, shromažďování a zkoumání stop a tím, že vypracovává podle potřeb trestního zákoníku a trestního řádu metody, postupy, prostředky a operace v zájmu úspěšného odhalování, vyšetřování a předcházení trestné činnosti." [MUS2001]

Pojmem nejvíce spojeným s kriminalistikou je stopa. Zjednodušeně lze říci, že kriminalistika je nauka o stopách trestného činu. Stopa je následkem trestného činu, je změnou v objektivní realitě, která přetrvává i po dokonání trestného činu a umožňuje trestný čin odhalit a objasnit. Teorie stop vychází z filosofické teorie vzájemného působení, která říká, že při vzájemném, současném působení dvou nebo více objektů navzájem dochází ke vzájemnému předávání informací o působení jednotlivých objektů a o jejich vlastnostech. Pro kriminalistiku mají význam pouze některé změny, které obecně souvisejí s kriminalisticky relevantní událostí. Kriminalistická stopa by měla splňovat 3 základní kritéria:

- musí se jednat o změnu, která je v příčinné nebo jiné souvislosti s kriminalisticky relevantní událostí
- doba existence změny musí být alespoň od jejího vzniku do zjištění
- změna musí být dekódovatelná (zkoumatelná) existujícími kriminalistickými metodami a prostředky. [MUS2001]

Každá kriminalistická stopa musí mít kriminalisticko technický význam, který spočívá především v tom, že kriminalistickou stopu lze využít v procesu kriminalistické identifikace a následně tak identifikovat osobu, věc nebo zvíře, kterými byla kriminalistická stopa vytvořena. Další vlastností je kriminalisticko taktický význam, který

spočívá v tom, že kriminalistická stopa poskytuje informace o osobách, které se podíleli na konkrétní události, o jejich činnosti, způsobu provedení činu, jejich fyzických, případně i psychických schopnostech, předmětu zájmu, způsobu příchodu a odchodu z místa apod.. [MUS2001]

V souvislosti s kybernalitou a kriminalistikou se objevuje pojem digitální stopa. Nejširším okruhem specialistů akceptovatelná definice digitální stopy říká, že se jedná o jakoukoliv informaci s vypovídající hodnotou pro danou relevantní událost, uložená nebo přenášená v digitální podobě. Tímto způsobem definovaná digitální stopa pokrývá jak oblast počítačů a počítačové komunikace, tak i oblast digitálních přenosů (mobilní telefony, digitální TV apod.), videa, audia, digitální fotografie, data kamerových systémů, data elektronických zabezpečovacích systémů, a jakýchkoliv dalších technologií spojených s kybernalitou. Digitální stopy jsou charakteristické tím, že vznikají působením člověka na aplikační nebo systémový software, funkčnost digitálního zařízení nebo automatickým působením jednoho zařízení, technologie na druhé. Digitální stopy, stejně jako každý jiný druh kriminalistických stop, mají své obecné a individuální druhové charakteristiky a vlastnosti, které z pohledu orgánů činných v trestním řízení mají typické pozitivní i negativní aspekty a důsledky. [SOU2005]

Po vymezení digitální stopy je třeba tuto zařadit do jednotlivých kategorií kriminalistických stop. Výchozím třídícím atributem digitální stopy je její informační obsah. Podle definice je digitální stopa jakákoliv informace s vypovídající hodnotou relevantní pro vyšetřování konkrétního činu, uložená nebo přenášená v digitální podobě. Informace jako taková je sice nehmotná, ale pro to, abychom mohli tuto analyzovat, je třeba ji nejprve zachytit a poté uložit na nějaké paměťové médium. Proto se digitální stopa řadí mezi stopy hmotné, materiálního charakteru. Digitální stopa vzniká působením člověka prostřednictvím nějakého softwaru či fyzikálním působením. Ve všech případech vzniku digitální stopy se na odrážející objekt přenášejí charakteristiky vnitřní stavby působícího, odráženého objektu. Proto jsou digitální stopy stopami vnitřní stavby odráženého objektu. Digitální stopa se také ve své primární podobě, kdy je uložená nebo přenášená, řadí mezi mikrostopy, protože pro její zviditelnění je třeba nějakého dalšího zařízení, nejčastěji zobrazovacího zařízení v podobě displeje či monitoru, který zprostředkovává podobu informace lidským smyslům. Digitální stopa vzniká zejména působením fyzikálních sil a energií a proto je řazena mezi stopy fyzikální. [SOU2005]

V souvislosti s digitálními stopami je třeba vysvětlit pojem zajištění digitálních stop. Jedná se o proces, který začíná okamžikem, kdy informace nebo zařízení jsou zajištěny nebo uloženy pro expertizní zkoumání. Předpokládá se, že digitální stopa bude před soudními orgány plnohodnotně akceptována jako důkaz. Dále se předpokládá, že proces zajištění musí být přiměřený a legální pro práci s důkazním materiálem v podmínkách dané země. Fyzické a datové objekty se stávají důkazem teprve tehdy, jsou-li akceptovatelné orgány činnými v trestním řízení. Datovými objekty se pak myslí objekty nebo informace s věrohodnou vypovídající hodnotou, jež jsou asociovány s fyzickými prvky. Datové objekty mohou mít různorodé formáty, ale nikdy nesmějí změnit původní informaci. Mezi datové objekty lze zařadit například databáze, adresáře, soubory, informační obsahy virtuálních pamětí, digitální audio nebo video nahrávky apod. Fyzickými objekty jsou myšleny prvky, na kterých jsou uloženy datové objekty nebo přes které jsou tyto přenášeny. Fyzickými objekty mohou být pevné disky počítačů, různá paměťová média jako CD, DVD apod. [KAR2006]

Souhrn datových a fyzických objektů je pak nazýván originálem digitální stopy, které jsou zajištěny pro potřeby expertizního, forenzního zkoumání. Originály digitálních stop jsou základním důkazním materiálem. Pro vyhodnocování a další práci se zajištěnými daty se z originálů stop poté vytvářejí tzv. pracovní duplikáty nebo kopie digitálních stop. Při procesu jejich vytváření nesmí docházet ke změně informačního obsahu originálu digitální stopy. Zároveň musí být tento proces opakovatelný se stejným výsledkem. K dalšímu využití je pak tímto způsobem k dispozici materiál k dalšímu zkoumání se stejnou informační hodnotou jako originál. Je pak garantována neměnnost originálů digitální stopy jako důkazního materiálu. Při duplikaci digitální stopy vzniká přesná digitální reprodukce všech datových objektů, které jsou uloženy na fyzickém objektu na fyzicky stejný typ datového média. S duplikátem lze poté bezpečně a plnohodnotně pracovat jako s originálem. Duplikace originální digitální stopy má však i své zápory v podobě velkých objemů dat, neboť vůči originálu jsou objemově vždy 1:1. Duplikáty digitálních stop se proto vytvářejí zejména pro důkazní šetření, aby bylo možné předložit původní materiál k opětovnému zkoumání jiným, nezávislým znalcem v těch případech, kdy samotný fyzický objekt nelze z různých důvodů přímo zajistit pro potřeby práce orgánů činných v trestním řízení ve vyšetřování. Další možností, která odstraňuje nevýhodu duplikace, je vytvoření kopie digitální stopy, při kterém se vytváří přesná reprodukce originální digitální stopy z

původního fyzického objektu na jiné fyzicky nezávislé datové médium. Při tomto procesu nemusí být nezbytně nutně reprodukovány všechny datové objekty původního fyzického objektu, ale pouze ty podstatné pro vyšetřování. Praktickým příkladem může být zkopírování jediné fotografie z paměťové karty digitálního fotoaparátu, kde je uloženo větší množství fotografií, a následný rozbor této fotografie. Kopie tedy obsahují pouze část datových objektů, ale informační hodnota každého takového reprodukovaného objektu musí zůstat zachována. Je však nutné brát zřetel na to, že pouhé kopie digitálních stop nemusejí být dostatečným důkazem, protože jsme se při jejich výběru mohli mýlit, zajistit jen určitou část dat atd.. Z pohledu forenzního šetření je proto nutné mít k dispozici originály digitálních stop nebo jejich duplikáty v nezměněném stavu. Pomocí nich lze následně transparentně prokázat oprávněnost a správnost zvoleného postupu vyšetřování a přípravy důkazního materiálu. [KAR2006]

Vzhledem ke skutečnosti, že v dnešní moderní době vznikají digitální stopy prostřednictvím rozmanitých druhů digitálních zařízení, začíná praktická forenzní činnost vnímat integraci technologických objektů a expertizní činnost chápat komplexně se zaměřením na standardizaci datových a komunikačních formátů. Je nutné přihlížet ke společné podstatě digitálních stop a sjednotit tak jednotné postupy pro vyhledávání, zajišťování předávání a analýzy digitálních stop a tyto procesy standardizovat i v mezinárodním měřítku takovým způsobem, aby splňovali garanci kvality a transparentnosti. [KAR2006]

8 Specifika a problémy odhalování kybernality

Tato kapitola je praktickou částí celé diplomové práce a klade si za cíl poukázat na specifika a úskalí jednotlivých fází zpracování trestných činů využívajících sítě Internet, neboť tato specifická skupina trestných činů vyžaduje specifické znalosti a postupy prověřování a vyšetřování, které se odlišují od ostatní trestné činnosti zejména tím, v jakém prostředí jsou páchány. Pro názornost bude výše uvedené ukázáno na případu trestného činu Výroba a jiné nakládání s dětskou pornografií dle § 192 trestního zákoníku, který je typickým zástupcem této problematiky, páchaného prostřednictvím elektronické pošty. Proces odhalování tohoto trestného činu bude demonstrován na jednotlivých fázích řešení tohoto trestněprávního jednání počínaje oznámením tohoto protiprávního jednání, přes prověřování a vyšetřování. Informace budou čerpány z praktických zkušeností policejního vyšetřovatele při odhalování a následného vedení trestního řízení až po podání návrhu na podání obžaloby státnímu zastupitelství. Vlastním přínosem praktické části tedy bude analýza postupů prověřování a vyšetřování násilné a mravnostní internetové kriminality s cílem zjistit odlišnosti těchto postupů od prověřování a vyšetřování ostatní trestné činnosti, případně poukázání na zjištěná úskalí těchto postupů v prostředí České republiky.

8.1 Oznámení

Obecně oznámení protiprávního jednání může být provedeno písemně nebo osobně prostřednictvím policejního orgánu nebo státního zástupce, kdy tyto subjekty jsou povinni takové oznámení přijmout a učinit taková opatření, která povedou k prověření oznámených skutečností za účelem zjištění, zda se jedná či nejedná o spáchání trestného činu. V případě oznámení takového protiprávního jednání policejnímu orgánu je třeba oznámení vyhodnotit a určit věcnou a místní příslušnost. Pokud jde o věcnou příslušnost, spadá trestný čin Výroba a jiné nakládání s dětskou pornografií dle § 192 trestního zákoníku zpravidla do věcné příslušnosti Služby kriminální policie a vyšetřování. Zároveň je třeba určit místní příslušnost, která je v případě kybernality poněkud komplikovanější. Pokud je

od počátku známá totožnost pachatele a místem spáchání trestného činu, což zpravidla nebývá, postoupí se oznámení policejnímu orgánu Služby kriminální policie a vyšetřování s místní působností v místě, kde došlo ke spáchání trestného činu. Pro trestné činy kybernality je však typické, že místo spáchání trestného činu není od počátku známé. Proto je třeba určit prvotní místní příslušnost dle jiného kritéria. V případě, že není známo místo spáchání trestného činu, je místně příslušný ten policejní orgán, v jehož územní působnosti má bydliště pachatel. Pachatel této trestné činnost však znám zpravidla od počátku také není. Proto se místní příslušnost řídí pravidlem, že místně příslušný policejní orgán je ten, v jehož místní působnosti je místo, kde trestný čin vyšel najevo. Místně příslušný je tedy policejní orgán, který se jako první o trestném činu dozvěděl. Určení místní příslušnosti koresponduje s místní příslušností soudů a tedy i státních zastupitelství, z čehož vyplývá, že v případě oznámení o podezření ze spáchání trestného činu přechovávání a jiné nakládání s dětskou pornografií postupují shodně státní zastupitelství, když postupují věc k projednání policejnímu orgánu. Zpravidla jsou u těchto trestných činů věcně příslušná obvodní nebo okresní státní zastupitelství.

Oznamovatelé bývají většinou uživatelé různých služeb Internetu. Může se jednat o uživatele elektronické pošty, veřejných serverů určených mimo jiné k chatování či o uživatele erotických serverů. Dětská pornografie může být zároveň vystavována prostřednictvím webových prezentací, které jsou pak hlášeny náhodnými návštěvníky. Zřídkakdy se stává, že oznamovateli jsou přímo správci nebo provozovatelé internetových serverů, kteří závadový obsah zjistí náhodou nebo jsou na něj upozorněni ze strany uživatelů serveru. Provozovatelé serverů nemají ze zákona povinnost kontrolovat obsah vkládaný uživateli.

Další možností k ohlášení závadového obsahu je oznámení prostřednictvím neziskového nevládního sdružení Národní centrum bezpečnějšího Internetu založeného v roce 2006, spíše známého jako projekt Safer Internet. Součástí tohoto projektu je tzv. Horká linka (www.horkalinka.cz), prostřednictvím které lze hlásit některý ze závadových obsahů vyskytujících se v síti Internet. Tato hlášení jsou poté přijata a dále pracovníky linky analyzována. V případě potvrzení závadového obsahu je věc hlášena přímo Policii ČR nebo v případě zahraničních serverů předána místně příslušné zahraniční horké lince. Safer Internet je záslužnou službou Internetu a nejen proto je spolufinancován a podporován příslušnými orgány Evropské unie. Takovýchto projektů existuje v České

republice celá řada. Vznikly na území a pro podmínky České republiky, ale zároveň vycházejí z celosvětových zkušeností a příkladů, zejména z nejrozšířenějšího typu komunikace cestou sociálních sítí : facebook, twitter, myspace apod.. Na webových prezentacích těchto projektů se kromě možnosti oznámení závadových obsahů nacházejí upozornění, návody, jak se chovat a nechovat na Internetu, co dělat když se někdo stane obětí internetové kriminality, kdy všechny tyto informace jsou srozumitelnou formou prezentovány nejen dětem všech věkových kategorií, rodičům i pedagogům, ale zároveň všem uživatelům internetu s odkazy a kontakty na příslušné organizace, kde hledat pomoc i radu.

Po přijetí oznámení policejním orgánem následuje jeho vyhodnocení spočívající v analýze oznámených skutečností provedené za účelem potvrzení či vyvrácení podezření ze spáchání trestného činu. V případě podezření ze spáchání trestného činu, konkrétně trestného činu přechovávání a jiné nakládání s dětskou pornografií, jsou ve věci zahájeny úkony trestního řízení ve smyslu § 158 odst. 3 trestního řádu, čímž je zahájena fáze prověřování, jež je obsahem následující kapitoly. V případě, že se nepotvrdí podezření ze spáchání nějakého trestného činu ve smyslu trestního zákoníku, je věc uložena ad-acta. Mimo oznámení provedeného další osobou mohou být zjištěny okolnosti podmiňující zahájení úkonů trestního řízení dle § 158 odst. 3 trestního řádu vlastním šetřením policejního orgánu, tj. na základě vlastních poznatků, nebo mohou vyplynout z jiné prověřované trestní věci. Takto se často děje, neboť v souvislosti s trestním stíháním jiné osoby za předmětnou trestnou činnost často vyjdou najevo adresáti či odesílatelé dětské pornografie, kteří jsou následně prověřováni. Do doby sepsání Záznamu o zahájení úkonů trestního řízení se ve věci provádí šetření nikoliv na základě trestního řádu, ale na základě zákona o Policii č. 273/2008 Sb..

8.2 Prověřování

Sepsáním Záznamu o zahájení úkonů trestního řízení dle § 158 odst. 3 tr. řádu je zahájena fáze prověřování. V této fázi je tedy již na základě přezkoumání oznámení odůvodněn závěr, že mohl být spáchán trestný čin uvedený v trestním zákoníku. Od této chvíle je postup policejního orgánu řízen trestním řádem, který zároveň policejnímu

orgánu umožňuje využití dalších nástrojů odhalování trestných činů.

V souvislosti s trestným činem Výroba a jiné nakládání s dětskou pornografií, jehož skutková podstata je uvedena v § 192 trestního zákoníku, v případě páchání tohoto trestného činu prostřednictvím elektronické pošty je základním nástrojem využití ustanovení § 8 trestního řádu, který nařizuje povinnost státním orgánům, právnickým a fyzickým osobám bez zbytečného odkladu i bez úplaty vyhotovovat dožádání orgánů činných v trestním řízení při plnění jejich úkolů. V praxi jsou od počátku z přijatého oznámení známy pouze informace o názvu účtu elektronické pošty, datum a čas odeslané závadové zprávy a její závadový obsah. V případě potvrzení, že se skutečně jedná o závadový obsah, tj. v řešeném případě dětská pornografie, je třeba zjistit uživatele tohoto účtu elektronické pošty. Toto lze zpravidla realizovat několika způsoby. První možností, která nejméně zasahuje do práv osob na soukromí, je zaslání dotazu právě ve smyslu § 8 tr. řádu poskytovateli zájmového účtu elektronické pošty, jejímž účelem je získání registračních údajů, mezi které lze zařadit jméno, příjmení, datum narození, kontaktní emailová adresa, případně autentizační mobilní telefon. V tomto případě se však mohou objevit tři problémy. Prvním je skutečnost, že údaje vložené při registraci účtu elektronické pošty nejsou nikým kontrolovány a proto si je může osoba zakládající tento účet vymyslet. Druhý problém nastává, když se poskytovatel služby elektronické pošty nachází na území jiného státu. V tomto případě lze požadavek realizovat cestou Interpolu, tj. mezinárodní mezivládní organizace zabezpečující policejní spolupráci v kriminálně-policejní oblasti mezi smluvními státy organizace, kdy vyřízení tohoto požadavku bývá většinou v řádu měsíců a proto tento způsob není efektivní a to s ohledem na to, že získané informace můžou být vymyšlené, jak bylo uvedeno v souvislosti s prvním problémem. Třetí problém nastává tehdy, když poskytovatelem emailového uživatelského účtu je menší společnost, například obchodní firma, kde by dotazem na informace o uživateli zájmového účtu hrozilo vyzrazení prověřování věci. Postup ve smyslu § 8 trestního řádu může být a ve většině případů je neúčelný.

Druhým způsobem zjištění možného pachatele je výpis údajů o uskutečněném telekomunikačním provozu dle § 88a trestního řádu, případně odposlech a záznam telekomunikačního provozu dle § 88 trestního řádu. Za využití těchto nástrojů trestního řádu se vážným způsobem zasahuje do práv prověřovaných osob. Proto není samotné rozhodnutí o využití těchto nástrojů pouze na vůli policejního orgánu, ale je třeba udělení

příkazu místně příslušným soudem. Pomocí ustanovení § 88 a § 88a trestního řádu lze mimo jiné získat tzv. logy přístupů do předmětného účtu elektronické pošty, které obsahují kromě data a času přístupu také IP adresu, prostřednictvím které bylo v době přístupů do tohoto účtu vstupováno. IP adresa je číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti. Dotazem, který je možné provést v síti Internet (např. prostřednictvím služby ripe.net), lze zjistit poskytovatele konkrétní IP adresy a následným dotazem na tohoto poskytovatele (za užití příkazu soudu) lze zjistit bod připojení, tj. konkrétní adresu, kde je využíváno tohoto připojení, včetně osoby, která uzavírala smlouvu s poskytovatelem, tj. osoby pravděpodobného uživatele. Zároveň je tímto způsobem možné získat obsah zpráv telekomunikačního provozu, který se poté může stát významným důkazním prostředkem v celém trestním řízení, neboť je tímto způsobem možné získat informace o dalším šíření nebo přechovávání dětské pornografie. Zde je nutné připomenout rozdíl mezi ustanovením § 88 trestního řádu a 88a trestního řádu. Informace vyžádané s využitím § 88 trestního řádu směřují do budoucnosti od doby realizování odposlechu, zatímco využitím § 88a trestního řádu se získávají údaje o již uskutečněném telekomunikačním provozu. Ani tyto nástroje trestního řádu však nejsou zcela bezproblémové a to z pohledu legislativy, neboť zejména v posledních letech se využití těchto nástrojů, zejména využití § 88a trestního řádu, výrazně omezilo. Původně platná ustanovení § 97 odst. 3,4 zákona č. 127/2005 Sb. o elektronických komunikacích nařizovalo právnickým a fyzickým osobám zajišťujících veřejnou komunikační síť (včetně poskytovatelů elektronické pošty a internetového připojení) uchovávat po dobu 6 až 12 měsíců provozní a lokalizační údaje, do nichž spadaly právě IP adresy, byla dne 22.03.2011 zrušena Nálezem ústavního soudu České republiky č. Pl. ÚS 24/10, čímž byla podstatně narušena možnost odhalování tak závažných trestných činů souvisejících s dětskou pornografií. Tímto však omezení prověřování trestné činnosti tohoto druhu neskočilo, neboť dne 04.01.2012 byl na základě návrhu Obvodního soudu pro Prahu 6 Nálezem Ústavního soudu č. Pl. ÚS 42/11 zrušeno ustanovení § 88a trestního řádu jako takové s účinností od 01.10.2012, kdy ústavní soud tímto termínem ponechal zákonodárcům prostor k vytvoření nové právní úpravy související s tímto ustanovením. Je pravdou, že trestní řád stále nabízí možnost využití ustanovení § 88, avšak tento je spojen se striktnějšími podmínkami k vydání příkazu k odposlechu a záznamu telekomunikačního provozu, neboť je větším zásahem do práv a svobod člověka. Zároveň je z pohledu

policejního orgánu realizace takového příkazu spojena ve srovnání s ustanovením § 88a trestního řádu se složitějším administrativním procesem vyplývajícím z nutnosti vyššího stupně utajení. V případě, že se zákonodárcům tedy nepodaří k 01.10.2012 schválit nový návrh ustanovení § 88a trestního řádu, nebude zbývat nic jiného než problematiku dětské pornografie řešit za pomoci odposlechů, čímž se doba celého trestního řízení prodlouží. Stejně tak bude kladen vyšší nárok na personální zatížení policejního orgánu. K věci je nutné zároveň poznamenat, že v případě, že se jedná o zahraničního poskytovatele služeb elektronické pošty nebo poskytovatele elektronické pošty na úrovni např. podniku, nastávají stejné problémy jako v případě součinnost dle § 8 trestního řádu.

Dalším problémem, se kterým se policejní orgán v průběhu prověřování v souvislosti s ustanovením pachatele přes IP adresu, kterou tento užívá ke vstupům do účtů elektronické pošty nebo jiných služeb Internetu, je skutečnost, že pachatel může využívat tzv. anonymizéry, které maskují skutečnou IP adresu pachatele, a namísto ní vystupují pod IP adresou jiného serveru, přes který do příslušných služeb Internetu vstupují. V těchto případech by poté bylo třeba s žádostí oslovit tyto servery, které tuto "nepravou" IP adresu poskytují, a dotázat se provozovatelů těchto serverů, kdo (přes jakou IP adresu) v určitý čas přistupoval na jimi provozovaný server. Problémem je však skutečnost, že tyto servery se z 99 % nacházejí mimo území české republiky a řešit tyto žádosti je tak téměř nemožné. Překážkou k ustanovení osoby pachatele se také může stát skutečnost, že za IP adresou, prostřednictvím které byly zjištěny přístupy do zájmového účtu některé ze služeb sítě Internet, se neskrývá pouze jeden konkrétní počítač, ale například celá firemní síť. Toto je pak třeba řešit pomocí opatrného místního šetření, aby nedošlo k vyzrazení záměru prověřování trestné činnosti konkrétní osoby. Výpis údajů o uskutečněném telekomunikačním provozu stejně jako odposlech a záznam telekomunikačního provozu slouží zároveň k odhalení dalších pachatelů, kteří prověřovanému pachateli dětskou pornografii buď zasílají, nebo je jim zasílána dětská pornografie právě prověřovaným pachatelem.

V případě, že je zjištěna osoba pachatele a místo, kde tato osoba užívá připojení k síti Internet, případně místo, kde se pachatel zdržuje, může být za účelem zajištění dalších důkazů pro trestní řízení přistoupeno k domovní prohlídce nebo prohlídce jiných prostor a pozemků dle § 82 trestního řádu. Domovní prohlídku a prohlídku jiných prostor je možné provést v případě, je-li důvodné podezření, že v bytě nebo jiném prostoře sloužícím k

bydlení nebo v prostorách k nim náležejících, případně v prostorách nesloužících k bydlení je věc nebo osoba důležitá pro trestní řízení. V případě trestného činu Výroba a jiné nakládání s dětskou pornografií tedy postačí skutečnost, že je prokázáno, že prostřednictvím konkrétní IP adresy, která je přidělována z námi zjištěného konkrétního místa, které je poté předmětem provedení domovní prohlídky nebo prohlídky jiných prostor, bylo přistupováno do uživatelského účtu, prostřednictvím kterého byla šířena nebo přechovávána dětská pornografie. Domovní prohlídka je značným zásahem do soukromí a osobního vlastnictví a proto je pro její provedení třeba Příkazu soudu, který je v případě splnění zákonných podmínek vyhotoven na návrh státního zástupce. V příkaze k domovní prohlídce musí být uvedeno mimo přesného uvedení místa domovní prohlídky také období, kdy bude provedena, kým bude provedena a účel jejího provedení, tj. co se bude v jejím průběhu zajišťovat. V případě trestných činů souvisejících s dětskou pornografií se jedná o počítače, datová média, případně záznamová zařízení atd. Před samotným započetím domovní prohlídky je třeba předat Příkaz vydaný soudem osobě, u níž má být domovní prohlídka nebo prohlídka jiných prostor provedena. Dále je třeba ve smyslu § 84 trestního řádu provést předchozí výslech osoby, u které má být domovní prohlídka nebo prohlídka jiných prostor provedena. Pokud se tímto výslechem a následným dobrovolným vydáním požadovaných věcí nepodaří uspokojit účel domovní prohlídky nebo prohlídky jiných prostor, pak se teprve může domovní prohlídka nebo prohlídka jiných prostor provést. Může nastat situace, že přípojný bod byl ustanoven v provozovně nějaké obchodní společnosti, kde je pak třeba pro prověření věci provést prohlídku nebytových prostor. Zde může nastat problém s obsahem výpočetní techniky, která může a často také obsahuje data potřebná pro provoz podniku. Zároveň může nastat situace, kdy se za zájmovou IP adresou využívanou na konkrétní adrese schovává celá síť počítačů. V těchto případech je možné k provedení domovní prohlídky nebo prohlídky jiných prostor přizvat soudního znalce z oboru kybernetika, odvětví výpočetní technika, který na místě zkoumáním počítačů a to i ve spolupráci s místním správcem sítě může označit konkrétní počítač, prostřednictvím, kterého bylo přistupováno do zájmových účtů elektronické pošty. V případě prověřování počítačů uvnitř firmy, na kterých jsou data důležitá pro provoz podniku, může soudní znalec na místě provést obraz disku, který je pak předmětem zkoumání, a počítač samotný se pak nemusí zajišťovat. Na místě provedení domovní prohlídky nebo prohlídky jiných prostor je také možné přímo vyhodnocovat datová média za účelem rozhodnutí, která

souvisejí s prověřovanou trestní věcí, tj. která budou v průběhu domovní prohlídky zajištěna a která ne. V průběhu domovní prohlídky nebo prohlídky jiných prostor je zároveň třeba důkladně dokumentovat zajištěné věci minimálně fotodokumentací a věci zajišťovat do zapečetěných obálek, případně jiných prostředků, aby tak nebyla narušena jejich důkazní hodnota z důvodu nesprávného zajištění, tzn., aby nemohlo dojít k manipulaci s nimi, dříve než budou zkoumány příslušným soudním znalcem. V souvislosti s prověřováním trestných činů souvisejících s dětskou pornografií, kde je podezření, že v místě provádění domovní prohlídky dochází k pohlavnímu zneužívání dítěte pachatele, je třeba před provedením domovní prohlídky zajistit účast pracovníka příslušného Odboru péče o dítě městského úřadu.

Před započetím provedení domovní prohlídky nebo prohlídky jiných prostor je třeba mít na paměti, že se jedná o úkon, kterým vyjde u pachatele najevo, že je prověřován pro podezření ze spáchání trestného činu. Z tohoto důvodu je třeba mít v této době provedeny všechny zajišťovací úkony, které bylo možné provést bez účasti pachatele, neboť od této doby pachatel může činit kroky k maření dalších zajišťovacích úkonů. Příkladem může být smazání obsahu účtu elektronické pošty pachatelem, případně varování dalších osob (dalších pachatelů nebo spolupachatelů) podílejících se na trestné činnosti. Pro předcházení vyzrazení a maření prověřovacích nebo později vyšetřovacích úkonů samozřejmě slouží další nástroje trestního řádu, jako je omezení osoby pachatele na svobodě jeho zadržením dle § 76 trestního řádu a následným podáním podnětu k podání návrhu na vzetí do vazby státnímu zástupci, avšak na vzetí pachatele do vazby však nelze spoléhat, neboť toto je podmíněno sdělením obvinění pachateli, což není vždy na základě do té doby nashromážděných důkazů možné a zároveň skutečnost, zda obviněný bude nebo bude vzat do vazby není na volbě policejního orgánu, ale na rozhodnutí místně a věcně příslušného soudu.

Další postup se tedy odvíjí od důkazní situace daného případu. Pokud nejsou prozatím k dispozici důkazní prostředky k zahájení trestního stíhání, tj. důkazy zjištěné například výpisem údajů o telekomunikačním provozu nebo odposlechem a záznamem telekomunikačního provozu, a je zajištěna výpočetní technika, u které je podezření, že jejím prostřednictvím byl spáchán trestný čin, přibere se opatřením ve smyslu § 105 trestního řádu soudní znalec z oboru kybernetika, odvětví výpočetní technika. V průběhu vyhotovování opatření dle § 105 trestního řádu je třeba důkladně zvážit otázky, na které

bude soudní znalec v průběhu zkoumání odpovídat. Mezi standardní otázky související s dětskou pornografií patří zajištění veškerých pornografických materiálů. Jedná se o zajištění veškerých pornografických materiálů, nikoliv pouze dětské pornografie, neboť k tomuto se soudní znalec z oboru kybernetika, odvětví výpočetní technika není oprávněn vyjadřovat. Tyto materiály je třeba získat nikoliv pouze z aktuálních dat uložených na pevném disku, případně na datových médiích, ale zároveň je nutné provést obnovu smazaných dat. Mezi další otázky pokládané znalci patří zajištění veškeré dostupné komunikace učiněné prostřednictvím účtů elektronické pošty (pokud je užíván nějaký poštovní klient pro správu pošty přímo v počítači), nebo prostřednictvím komunikačních softwarů jako je např. ICQ či Skype, včetně názvů užívaných uživatelských účtů. Podstatná může být také historie internetových prohlížečů, případně dočasně ukládané soubory těchto prohlížečů. Další otázky se pak odvíjejí od konkrétních řešených případů. Může se jednat například o vyhledání konkrétních textových řetězců.

8.3 Vyšetřování

V případě, že jsou známy a řádně zadokumentovány skutečnosti nasvědčující tomu, že byl spáchán trestný čin, vydá policejní orgán Usnesení o zahájení trestního stíhání dle § 160 odst. 1 trestního řádu, jehož předáním pachateli je zahájena fáze vyšetřování. V Usnesení dle § 160 trestního řádu je třeba důkladně popsat jednání, jež má znaky trestného činu a je kladeno za vinu pachateli, včetně jeho odůvodnění. V případě trestného činu Výroba a jiné nakládání s dětskou pornografií dle § 192 trestního zákoníku spáchaného prostřednictvím elektronické pošty se jedná o rozhodnutí, zda se pachatel v případě šíření dětské pornografie tohoto činu dopustil prostřednictvím veřejně přístupné počítačové sítě nebo jiným obdobně účinným způsobem. Do roku 2011 bylo šíření dětské pornografie prostřednictvím účtů elektronické pošty zpravidla posuzováno jako kvalifikovaná skutková podstata ve smyslu § 192 odst. 2 věta první, odst. 3 písm. b) trestního zákoníku, kdy využití elektronické pošty bylo považováno za šíření prostřednictvím veřejně přístupné počítačové sítě. V roce 2011 bylo vydáno několik rozhodnutí Nejvyššího soudu, která tuto skutečnost však mění, konkrétně rozhodnutí č. 8Tdo 407/2011 ze dne 27.04.2011, č. 3 Tdo 414/2011 ze dne 04.05.2011, č. 3 Tdo 669/2011 ze dne 01.06.2011 a č. 7 Tdo 687/2011 ze

dne 13.07.2011. Z obsahu rozhodnutí č. 8 Tdo 407/2011, které je stejně jako ostatní výše uvedená rozhodnutí považováno za judikát, vyplývá, že pokud pachatel rozešle počítačové soubory obsahující dětskou pornografii prostřednictvím elektronické pošty většímu množství emailových adresátů, lze v takovém případě i elektronickou poštu považovat za okolnost naplňující zákonný znak "jiným obdobně účinným způsobem". Není zde však definováno, co znamená větší množství emailových adresátů. Rozhodnutí č. 3 Tdo 414/2011 taktéž říká, že pokud jsou pornografické materiály zasílány prostřednictvím elektronické pošty, tj. že jsou určeny konkrétním adresátům (uživatelům konkrétního účtu elektronické pošty), kteří jako jediní mají do těchto účtů přístup, nemůže být naplněn znak veřejné přístupnosti a nelze tak toto jednání posuzovat jako kvalifikovanou skutkovou podstatu ve smyslu § 192 odst. 2 věta první, odst. 3 písm. b) trestního zákoníku. Zde bylo řešeno zaslání 5 zpráv elektronické pošty pachatelem s obsahem dětské pornografie. Závěrem Rozhodnutí č. 3 Tdo 669/2011 je obdobně jako u prvního jmenovaného Rozhodnutí to, že znak "jiným obdobně účinným způsobem" obsažený ve skutkové podstatě trestného činu Výroba a jiné nakládání s dětskou pornografií dle § 192 odst. 3 písm. b) trestního zákoníku je srovnatelný se znakem šíření tiskem, filmem, rozhlasem, televizí a veřejně přístupnou počítačovou sítí v případě, že se jedná o takové množství případů, kdy se předávaný závadný obsah (např. prostřednictvím elektronické pošty) dostane k většímu množství konečných množství, kdy toto množství není opětovně definováno. V tomto konkrétním případě pachatel za období od 17.10.2008 do 09.03.2009 rozeslal celkem 32 zpráv s obsahem dětské pornografie a to celkem 18ti různým příjemcům. Nejvyšší soud tak v tomto případě rozhodl, že se nejedná o větší počet emailových adresátů a s ohledem na rozsah spáchané činnosti se tak nemůže jednat o kvalifikovanou skutkovou podstatu ve smyslu šíření jiným obdobně účinným způsobem. Rozhodnutí č. 7 Tdo 687/2011 pak mimo jiné říká, že kromě počtu rozeslaných zpráv a počtu adresátů je třeba brát v úvahu také časové období, za které byly tyto zprávy rozeslány. V tomto konkrétním případě se jednalo o rozeslání celkem 11 emailových zpráv s obsahem dětské pornografie za období cca 3 týdnů. Vzhledem k menšímu rozsahu jednání pachatele s přihlédnutím k délce období jeho jednání je Nejvyšší soud toho názoru, že v daném případě není splněná podmínka pro kvalifikování skutku dle § 192 odst. 3 písm. b) trestního zákoníku. Z výše uvedeného vyplývá, že posuzování trestného činu Výroba a jiné nakládání s dětskou pornografií ve smyslu § 192 odst. 3 písm. b) trestního

zákoníku není legislativně jednoznačně upraveno a rozhodování o skutečnosti, zda se jedná o šíření dětské pornografie jiným obdobně účinným způsobem tak v závěru rozhodují soudy na základě konkrétních okolností daného případu. Z pohledu policejního orgánu je však třeba ve sporných případech, kdy by se mohlo jednat o kvalifikovanou skutkovou podstatu ve smyslu § 192 odst. 3 písm. b) trestního zákoníku se k přiklánět k této, neboť oproti základní skutkové podstatě je zde značný rozdíl v horní hranici pachateli hrozící trestní sazby, tj. nikoliv pouze 3 roky, ale 6 let. Důvodem je skutečnost, že v případě právě této kvalifikované skutkové podstaty je dle ustanovení § 36 odst. 3 trestního řádu nutná obhajoba. V případě sdělení obvinění přečinu Výroba a jiné nakládání s dětskou pornografií dle § 192 odst. 2 trestního zákoníku policejním orgánem a následnou změnou této kvalifikace na kvalifikovanou skutkovou podstatu soudem, by bylo obviněnému upřeno právo na bezplatné přidělení obhájce ex-offo státem, což by bylo nepřípustné.

Dalším nástrojem trestního řádu je výslech obviněného, který slouží zejména osobě obviněného k vyjádření se ke skutečnostem, které jsou mu kladeny za vinu. Tento výslech je již na rozdíl od předchozích podání vysvětlení brán jako důkazní prostředek před soudem. Před započetím tohoto úkonu je třeba důkladné přípravy otázek, aby se výslechem podařilo objasnit logické rozpory mezi skutečnostmi zjištěnými důkazy a samotným tvrzením obviněného. Obviněný může využít svého práva a může tak odmítnout vypovídat. Důkazní hodnotu mají také provedené výslechy případných svědků provedené po zahájení trestního stíhání pachatele. V případě, že je zjištěno, že se pachatel dopouštěl i samotné výroby dětské pornografie formou fotografování či natáčení osob mladších 18 let vyzývavě předvádějících své pohlavní orgány za účelem sexuálního uspokojení, dále pak osob mladších 18 let v polohách skutečného či předstíraného sexuálního styku s nimi, popřípadě jiných obdobně sexuálně dráždivých činnostech, je třeba tyto osoby mladší 18 let vyslechnout. V případě, že se jedná o osoby mladší 15 let, je třeba provádět výslech zvlášť šetrně a po obsahové stránce tak, aby výslech v dalším řízení zpravidla už nebylo třeba opakovat. K výslechu se přibere pedagog nebo jiná osoba mající zkušenosti s výchovou mládeže, která by přispěla ke správnému vedení výslechu.

V případě zjištění, že v prověřované a následně vyšetřované věci lze vyloučit provádění šíření dětské pornografie pachatelem za účelem pouze získání majetkového prospěchu, lze přistoupit ke zkoumání duševního stavu obviněného, neboť tento může trpět nějakou duševní či sexuální poruchou, která může být nebezpečná pro společnost. K

takovému zkoumání se přibere soudní znalec z oboru zdravotnictví, odvětví psychiatrie a sexuologie. Podnětem pro přibrání soudního znalce z oboru zdravotnictví, odvětví psychiatrie by měly být pochyby policejního orgánu o plné příčetnosti obviněného. Soudní znalec z oboru zdravotnictví, odvětví sexuologie se pak přibírá v případech, kdy je podezření na jednání pachatele motivací sexuálního charakteru. V takových případech může být součástí otázek pokládaných soudnímu znalci provedení tzv. falopletizmografického vyšetření (PPG), které měří fyziologické reakce penisu v souvislosti s vizuálními podněty různého charakteru. Tohoto vyšetření se užívá k diagnostice sexuální orientace či sexuální deviace, včetně pedofilie. V případě znalcem zjištěné sexuální deviace pachatele je pak možné v závěru znaleckého posudku uvést návrhy na nařízení ochranné léčby v ambulantní nebo ústavní formě. Rozdíl mezi ambulantní a ústavní formou spočívá v tom, že u ambulantní formy nedochází k omezení pachatele na svobodě. O uložení ochranného léčení následně rozhodují soudy.

V případech využití služeb soudních znalců z oboru zdravotnictví, odvětví psychiatrie, sexuologie, se nejčastěji používají následující otázky:

- Proveďte vyšetření za pomoci PPG.
- Byla u zkoumané osoby zjištěna sexuální deviace? V případě, že ano, o jakou sexuální deviaci se jedná?
- Mohla zjištěná sexuální deviace ovlivnit u zkoumané osoby rozpoznávací a ovládací schopnosti a do jaké míry?
- Je pobyt zkoumané osoby na svobodě možný vzhledem ke zjištěné sexuální deviaci? Jaká opatření navrhujete?
- Jaká je prognóza vývoje sexuální deviace?
- Je nutné u zkoumané osoby nařízení ochranného léčení, případně jiné opatření a jaké?

Zároveň je pak možné přibrat soudního znalce z oboru zdravotnictví, odvětví psychologie, který může zkoumat například motivaci obviněného ke spáchání trestného činu, jeho osobnost a intelekt, jaký bude vývoj jeho osobnosti ve vztahu k

protispolečenskému jednání, zda je možná jeho resocializace, posouzení jeho věrohodnosti a další.

Po skončení všech vyšetřovacích úkonů proběhne seznámení se spisovým materiálem osobou obviněného, případně jeho obhájcem, kteří se v průběhu tohoto úkonu mohou seznámit s dosud nashromážděnými důkazy a následně mají možnost uvést návrhy na doplnění vyšetřování, případně se jinak vyjádřit k vyšetřované trestní věci. Poté je již spisový materiál s návrhem na podání obžaloby postoupen státnímu zastupitelství. Součástí návrhu na podání obžaloby jsou jednotlivé skutky, které jsou obviněnému kladeny za vinu včetně uvedení jejich právní kvalifikace a návrhu důkazů, které spáchání těchto skutků potvrzují. V případě, že spisový materiál obsahuje i zajištěné věci, jejichž prostřednictvím došlo ke spáchání některého z trestných činů spáchaných obviněným, postoupí se tyto spolu se spisovým materiálem s návrhem na uložení trestu propadnutí věci ve smyslu § 70 trestního řádu.

9 Závěr

Internet se stal v dnešní informační společnosti součástí každodenního života mnoha lidí bez rozdílu věku či pohlaví. Jeho využívání však nepřináší pouze výhody, ale zároveň se s jeho příchodem objevují i rizika, která mohou přesahovat hranici virtuálního světa a značně tak působit na integritu člověka. Pokud tato rizika překročí určitou hranici, která je upravena legislativou v oblasti trestního práva, stávají se tato jednání trestným činem, postižitelným dle příslušných ustanovení trestního zákoníku. Přestože ve virtuálním světě nedochází přímo k fyzickému kontaktu osoby pachatele s obětí, mohou být tyto trestné činy násilného nebo mravnostního charakteru. V případě násilné trestné činnosti se může jednat o delikty jako je vydírání, nebezpečné vyhrožování, nebezpečné pronásledování či další jednání, která souvisejí s agresivitou pachatele. V případech mravnostní kriminality jsou často obětí děti, jejichž psychika je znatelně zranitelnější, než je tomu v případech dospělých osob. Jedním z cílů této diplomové práce bylo seznámení se základními pojmy souvisejícími s násilnou a mravnostní internetovou kriminalitou. Tento cíl byl splněn vypracováním kapitol č. 2-5.

Typickým znakem násilné a mravnostní internetové kriminality je vysoká latentnost a nízká objasněnost těchto činů. Vysoká latentnost je způsobena skutečností, že u páchání trestných činů prostřednictvím sítě Internet zpravidla nejsou přítomni žádní svědci a samotné oběti, které často pocházejí z řad dětí, se bojí tato protiprávní jednání oznámit. Nižší objasněnost je způsobena jedním z hlavních atributů sítě Internet, tj. anonymitou, která znatelně nahrává pachatelům v páchání této trestné činnosti. Dalším problémem je skutečnost, že digitální stopy, které mohou vést k osobě pachatele, pak existují pouze omezenou minimální dobu a po uplynutí času, než dojde ke zjištění či oznámení násilné nebo mravnostní internetové kriminality již nejsou pro účely trestního řízení tyto stopy k dispozici. Přes tato negativní specifika násilné a mravnostní internetové kriminality nabízí trestní řád řadu nástrojů k jejich prověřování a vyšetřování. Seznámení s těmito nástroji bylo dalším cílem této diplomové práce, kdy tohoto cíle v teoretické rovině se podařilo dosáhnout v kapitolách č. 6 a 7.

Cílem praktické části, tj. vlastním přínosem této diplomové práce, byla analýza průběhu prověřování a vyšetřování násilné a mravnostní internetové kriminality z pohledu

policejního vyšetřovatele s cílem poukázat na specifika a možné problémy těchto postupů. Naplnění tohoto cíle bylo realizováno v kapitole č. 8 a vychází z praktických zkušeností policejního vyšetřovatele při řešení předmětné trestné činnosti. Je nepochybné, že prověřování a vyšetřování této trestné činnosti má svá specifika vyplývající zejména z charakteru prostřední, ve kterém je tato trestná činnost páchána, tj. charakteru prostředí sítě Internet. Zejména tímto se postupy prověřování a vyšetřování násilné a mravnostní trestné činnosti odlišují od postupů prověřování a vyšetřování ostatních protiprávních jednání v trestně-právní rovině. Jedná se tedy zejména o zajišťování a následné vyhodnocování digitálních stop. Vyhodnocením těchto postupů byly zjištěny dva zásadní problémy. Prvním z nich je skutečnost, že v době psaní této diplomové práce je zde problém s legislativou, neboť zákony České republiky nepřikazují poskytovatelům telekomunikačních služeb uchovávat provozní údaje související s telekomunikačním provozem, tak jak tomu bylo v minulosti. Nedílnou součástí těchto provozních údajů byly IP adresy, prostřednictvím kterých pachatelé z konkrétního místa přistupovali k určitým internetovým službám, s jejichž využitím poté páchali trestnou činnost. Dotazem na konkrétního poskytovatele Internetu, který měl na starosti přidělování zjištěné IP adresy, pak bylo možné jednoduše zjistit, komu byla tato IP adresa v konkrétní době přidělena. Tyto provozní údaje však ve většině případů poskytovatelé služeb sítě Internet odmítají poskytnout a to právě s odkazem na skutečnost, že tyto již nemusejí dle současné platné právní úpravy uchovávat. Druhým zásadním problémem vyplývajícím z analýzy postupů prověřování a vyšetřování násilných a mravnostních trestných činů páchaných prostřednictvím sítě Internet je nedostatečná mezinárodní spolupráce. Tato nedostatečnost je spatřována v souvislosti s páchání internetové kriminality zejména v tom, že pokud pachatel páchající trestnou činnost z počítače umístěného na území České republiky k tomuto využije služby nějakého zahraničního serveru (např. služeb elektronické pošty poskytované zahraničním poskytovatelem), je pak téměř nemožné odhalení osoby pachatele, neboť mezinárodní spolupráce tohoto druhu je buď zcela nemožná nebo neefektivní.

Vzhledem ke skutečnosti, že je Česká republika vázáná mezinárodními úmluvami k řešení této trestné činnosti zejména se zřetelem na ochranu dětí, je třeba tyto legislativní nedostatky v co nejkratší době vyřešit a plnit tak zodpovědně tyto úmluvy. Zároveň je třeba vzhledem k rychlému vývoji informačních technologií, aby se nástroje a postupy

prověřování a vyšetřování této trestné činnosti vyvíjely ruku v ruce stejným tempem jako se vyvíjejí informační technologie, neboť s jejich vývojem zároveň narůstá četnost skutků internetové kriminality.

Seznam použitých pramenů a literatury

[BIS2010]
Výroční zpráva BIS 2010. Bezpečnostní informační služba [online]. [cit. 2012-01-20]. Dostupné z: http://www.bis.cz/n/2011-09-07-vyrocni-zprava-2010.html.

[BOC2004]
BOCIJ, Paul. Cyberstalking: harassment in the internet age and how to protect your family. Westport, conn.: Praeger, 2004, 268 s. ISBN 0-275-98118-5.

[ČÍR2008]
ČÍRTKOVÁ, Ludmila. Moderní psychologie pro právníky: [domácí násilí, stalking, predikce násilí]. Vyd. 1. Praha: Grada, 2008, 150 s. Psyché (Grada). ISBN 978-802-4722-078.

[CHM2003]
CHMELÍK, Jan. Mravnost, pornografie a mravnostní kriminalita. Vyd. 1. Praha: Portál, 2003, 201 s. ISBN 80-717-8739-6.

[JAN2006]
JANOUŠEK, Michal. Kyberterorismus: Terorismum informační společnosti [online]. [cit. 2012-03-01]. Dostupné z: http://www.mocr.army.cz/mo/obrana_a_strategie/2-2006cz/janousek.pdf.

[JIR2007]
JIROVSKÝ, Václav. Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství . Praha : Grada Publishing , 2007. 284 s. ISBN 978-80-247-1561-2.

[KAR2006]
PORADA Viktor, RAK Roman. Karlovarská právní revue. Vyd. 1. Karlovy Vary: Vysoká škola Karlovy Vary, 2005, roč. 2006(č. 4). Dostupné Z: http://mail.vskv.cz/download/KPR/archiv/2006/kpr4_2006.pdf.

[MAT2002]
MATĚJKA, Michal. Počítačová kriminalita. Vyd. 1. Praha: Computer Press, 2002, 106 s. ISBN 80-722-6419-2.

[MUS2001]
MUSIL, Jan a kol.. Kriminalistika. Vyd. 1. Praha: C. H. Beck, 2001, 512 s. ISBN 80-717-9362-0.

[NĚM2004]
NĚMEC, Miroslav. Kriminalistická taktika pro policisty. Vyd. 1. Praha: Eurounion, 2004. ISBN 978-807-3170-363.

[RAC2005]
RAC (Risk Analysis Consultants). Forenzní zkoumání digitálních důkazů - příručka vyšetřovatele. Praha. 2005. Dostupné z: http://www.rac.cz/rac/homepage.nsf/cz/883aabb42333cb35c12570fc0034a328/$file/guide%20051230.pdf.

[SOU2005]
BRADÁČ, Albert, PORADA Viktor a STRAUS Jiří. Soudní Inženýrství. Praha: Policejní Akademie České Republiky, 2001, roč. 2005(č. 04). Dostupné Z: http://www.sinz.cz/archiv/docs/Si-2005-04-183-192.pdf.

[TRŘ2008]
S□ÁMAL, Pavel. Trestní r□ád: komentár□. 6., doplne□né a pr□epracované vyd. V Praze: C.H. Beck, 2008, 23011 s. ISBN 978-807-4000-430.

[TRZII]
S□ÁMAL, Pavel. Trestní zákoník II: komentár□. 1. vyd. V Praze: C.H. Beck, 2009-2010. ISBN 97880740017892.

[VER2006]
VERTON, Dan. Black ice: neviditelná hrozba kyberterorizmu. Gliwice: Helion, 2004, 278 s. ISBN 83-736-1564-4.

[WHO]
Violent prevention alliance [online]. [cit. 12.02.2012]. Dostupné z: http://www.who.int/violenceprevention/approach/definition/en/index.html.

[WIKIKYB]
Kyberterorismus. Wikipedie [online]. [cit. 2012-02-26]. Dostupné z: http://cs.wikipedia.org/wiki/Kyberprostor.

Seznam příloh

- rozhodnutí č. 8 Tdo 407/2011 ze dne 27.04.2011 (str. I-VII)
- rozhodnutí č. 3 Tdo 414/2011 ze dne 04.05.2011 (str. VIII-XII)
- rozhodnutí č. 3 Tdo 669/2011 ze dne 01.06.2011 (str. XIII-XVII)
- rozhodnutí č. 7 Tdo 687/2011 ze dne 13.07.2011 (str. XVIII-XX)

8 Tdo 407/2011

K tomu, že i emailová pošta může být účinný způsob šíření pornografie mezi nezletilé osoby

Pokud pachatel rozešle počítačové soubory prostřednictvím emailové pošty většímu počtu emailových adresátů (dětem), lze v takovém případě i elektronickou poštu považovat za okolnost naplňující zákonný znak „jiným obdobně účinným způsobem“ ve smyslu § 205 odst. 3 písm. b) TZ [ve znění účinném do 31. 12. 2009, od 1. 1. 2010 ve smyslu přečinu šíření pornografie podle § 191 odst. 3 písm. b) TZ]. Přitom je třeba posoudit možnosti zabezpečení takové pošty a rizika úniku obsahu zpráv přepravovaných jejím prostřednictvím.

USNESENÍ

Nejvyšší soud

České republiky rozhodl v neveřejném zasedání konaném dne 27. dubna 2011 k dovolání nejvyšší státní zástupkyně podanému v neprospěch obviněného Bc. V. B., proti usnesení Krajského soudu v Brně ze dne 23. 9. 2010, sp. zn. 7 To 442/2010, který rozhodl jako soud odvolací v trestní věci vedené u Městského soudu v Brně pod sp. zn. 95 T 59/2010, takto:

Podle § 265k odst. 1 tr. ř. s e zrušujeusnesení Krajského soudu v Brně ze dne 23. 9. 2010, sp. zn. 7 To 442/2010.

Současně podle § 265k odst. 2 tr. ř. se zrušujívšechna další rozhodnutí na zrušené rozhodnutí obsahově navazující, pokud vzhledem ke změně, k níž došlo zrušením, pozbyla podkladu.

Podle § 265l odst. 1 tr. ř. se přikazuje Krajskému soudu v Brně, aby věc v potřebném rozsahu znovu projednal a rozhodl.

Odůvodnění:

Městský soud v Brně rozsudkem ze dne 19. 5. 2010, sp. zn. 95 T 59/2010, uznal obviněného Bc. V. B. (dále jen "obviněný") vinným, že:

"1) od přesně nezjištěné doby až do dne 5. 3. 2009, na různých místech města B. (například z počítače v bytě I. Z. v B. na ulici B. nebo z počítače na pracovišti Městské policie), odeslal ze své e-mailové schránky do e-mailových schránek:

nejméně 47 e-mailových zpráv s přílohami obsahujícími pornografické fotografie nebo videosoubory, které zobrazují nebo jinak využívají děti,2) v době od 2. 2. 2009 až do dne 16. 2. 2009, na různých místech města B. (například z počítače v bytě I. Z. v B. na ulici B. nebo z počítače na pracovišti Městské policie), odeslal ze své e-mailové schránky do e-mailových schránek:

nejméně 6 e-mailových zpráv s přílohami obsahujícími pornografické fotografie nebo videosoubory, které zobrazují pohlavní styk se zvířetem,

3) od přesně nezjištěné doby až do dne 10. 3. 20009, ve své e-mailové schránce, přechovával celkem 91 e-mailových zpráv s přílohami obsahujícími pornografické fotografie nebo videosoubory, které zobrazují nebo jinak využívají děti".

Takto zjištěné jednání obviněného soud právně kvalifikoval v bodě 1) jako trestný čin šíření pornografie podle § 205 odst. 2 písm. a) zákona č. 140/1961 Sb., trestního zákona, ve znění pozdějších předpisů (dále jen "tr. zák."), v bodě 2) jako přečin šíření pornografie podle § 191 odst. 1 zákona č. 40/2009 Sb., trestního zákoníku, ve znění pozdějších předpisů (dále jen "trestní zákoník"), a v bodě 3) jako trestný čin přechovávání dětské pornografie podle § 205a tr. zák., a uložil mu podle § 205 odst. 2 tr. zák. za užití § 35 odst. 1 tr. zák. úhrnný trest odnětí svobody v trvání deseti měsíců, jehož výkon podle § 58 odst. 1 a § 59 odst. 1 tr. zák. podmíněně odložil na zkušební dobu v trvání dvaceti měsíců.

Proti tomuto rozsudku podali obviněný a státní zástupce odvolání, o nichž Krajský soud v Brně rozhodl usnesením ze dne 23. 9. 2010, sp. zn. 7 To 442/2010, tak, že je podle § 256 tr. ř. zamítl.

Proti usnesení odvolacího soudu (konkrétně proti výroku, jímž bylo zamítnuto odvolání státního zástupce) podala nejvyšší státní zástupkyně (dále převážně jen "dovolatelka") v neprospěch obviněného dovolání z důvodů uvedených v § 265b odst. 1 písm. g) a *l*) tr. ř.

Dovolatelka po shrnutí obsahu meritorních rozhodnutí učiněných soudy nižšího stupně připomněla, že soud prvního stupně - pokud se týká právní kvalifikace skutků popsaných pod body 1) a 2) výroku jeho rozsudku - na rozdíl od obžaloby neposoudil jednání obviněného jako spáchané v kvalifikovaných skutkových podstatách § 205 odst. 3 písm. b) tr. zák., resp. § 191 odst. 3 písm. b) trestního zákoníku, tj. veřejně přístupnou počítačovou sítí, a že odvolací soud se s argumentací nalézacího soudu ztotožnil a odkázal na ni.

S názory obou soudů nižších instancí dovolatelka vyslovila nesouhlas. Uvedla, že základní skutková podstata trestného činu šíření pornografie podle § 205 odst. 2 písm. a) tr. zák., kterou soudy nijak nezpochybnily, byla ovšem naplněna ve formě "uvádění do oběhu", nikoli ve formě "jiného opatření" pornografického díla. Pod pojmem "uvedení do oběhu" u jmenovaného trestného činu je totiž třeba rozumět jednání pachatele, kterým se má předmět dostat postupně do rukou širšího okruhu osob, ať v originále či v kopiích. Nešlo by sice o oběh, pokud by se měl s pornografickým předmětem seznámit jen úzký okruh lidí, uzavřená společnost apod., avšak na druhé straně není třeba, aby se s ním skutečně širší okruh lidí seznámil, postačí pouhé uvádění do oběhu, tedy počátek tohoto oběhu. V dané trestní věci však ze skutkových zjištění vyplývá, že obviněný postupně zaslal 47 e-mailových zpráv s pornografickým obsahem na 24 e-mailových adres, a ačkoliv nebylo přesně zjištěno, kolik osob mělo k jednotlivým e-mailovým schránkám přístup, jak dlouho tam byly zprávy uloženy, zda byly dále přeposílány, apod., šlo o natolik intenzivní způsob šíření pornografických děl, že již šlo o "uvádění do oběhu" ve smyslu uvedeném shora.

Nejvyšší státní zástupkyně však ve svém podání především nesouhlasila s názory soudů, pokud dospěly k závěru, že nebyl naplněn znak spáchání činu "veřejně přístupnou počítačovou sítí". V této souvislosti citovala definici tohoto pojmu obsaženou v komentovaných vydáních trestního zákoníku a trestního zákona (např. Šámal P. a kol., Trestní zákoník II, § 140 - 421, Komentář, I. vydání, Praha: C.H.Beck 2010, str. 1699-1700) či v rozhodnutí Nejvyššího soudu České republiky (dále jen "Nejvyšší soud") ve věci vedené pod sp. zn. 6 Tdo 1135/2010.

V návaznosti na to dovolatelka zdůraznila, že e-mailová komunikace představuje neporovnatelně rychlejší a jednodušší způsob rozesílání pornografických děl velkému počtu subjektů na prakticky neomezenou vzdálenost, než umožňuje např. "klasická" poštovní zásilka. Nadto jde o komunikaci do značné míry anonymní, kdy pachateli postačuje pouhá znalost e-mailové adresy, aniž by musel nutně znát fyzickou totožnost příjemce. Zřejmě i proto vyslovila domněnku, že pokud by zákonodárce chtěl postihnout pouze takové formy využití veřejné počítačové sítě, které umožňují zpřístupnění pornografického díla prakticky jakémukoli uživateli (např. tzv. "zavěšení" na internetu), pak by příslušnou část ustanovení § 205 odst. 3 písm. b) tr. zák. [nyní § 192 odst. 3 písm. b) trestního zákoníku] formuloval jiným způsobem.

V souvislosti s tím dovolatelka vytkla oběma soudům nižších stupňů, že nepřihlédly k některým specifikům e-mailové komunikace. Rozdíl mezi e-mailovou komunikací, která je základním komunikačním prostředkem na Internetu, a komunikací formou klasické poštovní zásilky (dopisu, balíku) zasílané prostřednictvím veřejného přepravce konkrétnímu adresátovi spočívá nejen v tom, že e-mailové zprávy musí projít cizími počítači v síti předtím, než dosáhnou cílový počítač, což výrazně zjednodušuje možnost obsah zprávy zachytit a přečíst, ale i v tom, že naprostá většina providerů kopie všech e-mailových zpráv ukládá (zálohuje) na svoje servery před doručením a tyto zálohy často ponechává na serveru řadu měsíců po doručení zprávy, a to i v případě, že ve schránkách odesílatele i příjemce jsou již vymazány. Navíc také samotní uživatelé často tyto zprávy ponechávají uložené ve svých schránkách, kde k nim mohou získat přístup i jiné osoby než ty, kterým byly určeny [dovolatelka odkázala na rozhodnutí Nejvyššího soudu sp. zn. 11 Tdo 349/2008 *(správně mělo být sp. zn. 11 Tdo 349/2009)*, z něhož vyplývá, že po doručení do e-mailové schránky příjemce již elektronická pošta nepožívá ochrany tajemství dopravovaných zpráv ve smyslu tehdy platného ustanovení § 239 odst. 1 tr. zák.].

Nejvyšší státní zástupkyně neopomněla zmínit ani problematiku tzv. virů, jež mohou narušovat nebo likvidovat instalované programy, event. mohou být naprogramovány tak, že bez vědomí uživatele odesílají z jeho počítače uložená data a dokumenty. Možnost zpřístupnění pornografických děl šířených cestou e-mailové komunikace i dalším osobám než těm, kterým byla původně určena, je tudíž výrazně vyšší nežli v případě jiných způsobů komunikace.

Na základě těchto úvah dovolatelka dospěla k závěru, že skutek popsaný pod bodem 1) výroku o vině rozsudku soudu prvního stupně měl být právně kvalifikován jako trestný čin šíření pornografie podle § 205 odst. 2 písm. a), odst. 3 písm. b) tr. zák., jelikož s ohledem na množství rozeslaných fotografií a videosouborů s tématikou dětské pornografie byly nepochybně splněny i materiální podmínky pro aplikaci kvalifikované skutkové podstaty ve smyslu § 88 odst. 1 tr. zák.

Ve vztahu ke skutku vymezenému v bodě 2) odsuzujícího rozsudku dovolatelka uvedla, že v tomto případě byla pornografická díla zaslána pouze na dvě e-mailové adresy, proto lze souhlasit s tím, že přečin byl, pokud se týká znaků základní skutkové podstaty podle § 191 odst. 1 trestního zákoníku, spáchán formou "jiného opatření" pornografického díla. Jinak ovšem i tento skutek měl být - z důvodů rozvedených již výše - právně kvalifikován nikoli pouze podle uvedené základní skutkové podstaty, nýbrž jako přečin šíření pornografie v jeho kvalifikované podobě podle § 191 odst. 1, 3 písm. b) trestního zákoníku.

Z těchto důvodů nejvyšší státní zástupkyně v závěru svého podání navrhla, aby Nejvyšší soud:

1. podle § 265k odst. 1, 2 tr. ř. za podmínky uvedené v § 265p odst. 1 tr. ř. zrušil usnesení Krajského soudu v Brně ze dne 23. 9. 2010, sp. zn. 7 To 442/2010, ve výroku o zamítnutí odvolání státního zástupce, jakož i všechna další rozhodnutí na zrušený výrok obsahově navazující, pokud vzhledem ke změně, k níž došlo zrušením, pozbyla podkladu,

2. podle § 2651 odst. 1 tr. ř. přikázal Krajskému soudu v Brně, aby věc v potřebném rozsahu znovu projednal a rozhodl,

3. v souladu s § 265r odst. 1 písm. b) tr. ř. o dovolání rozhodl v neveřejném zasedání.

Současně dovolatelka vyslovila souhlas s projednáním věci v neveřejném zasedání i pro případ jiného, nežli navrhovaného rozhodnutí dovolacího soudu.

K podanému dovolání se vyjádřil obviněný prostřednictvím obhájce JUDr. Karla Schelleho, LL.M., a vyslovil nesouhlas s argumentací v něm obsaženou. Především znovu popřel svůj úmysl v té podobě, že by byl alespoň srozuměn s tím, že odesílání předmětných e-mailů může být zpřístupněno i jiným subjektům než adresátům. Své počínání v tomto kontextu přirovnal k obyčejné poštovní zásilce, která je taktéž adresována odesílatelem přímo příjemci, přičemž nelze ani v těchto případech zcela vyloučit, že se s jejím obsahem bez úmyslu odesílatele protiprávně seznámí cestou k adresátovi i jiné osoby (odlišné od adresáta). Vyjádřil názor, že dovolatelčiným právním výkladem by byl zcela popřen institut listovního tajemství zakotvený v čl. 13 Listiny základních práv a svobod, jakož i smysl trestněprávní represe pro osoby porušující tajemství dopravovaných zpráv podle § 182 trestního zákoníku. E-mailovou komunikaci označil za analogickou komunikaci poštovní, neboť se řídí stejnými pravidly a pro obě platí úmysl odesílatele seznámit s jejich obsahem příjemce a nikoho jiného. Pokud se s obsahem e-mailu seznámí bez vědomí odesílatele a příjemce jakýkoli jiný subjekt, jedná se o porušení výše uvedených základních práv i norem trestního práva. Takový postup však současně nemůže být přičítán k tíži odesílatele. Za šíření veřejnou počítačovou sítí označil uveřejnění na veřejně přístupných internetových stránkách.

Závěrem svého vyjádření obviněný navrhl, aby Nejvyšší soud podané dovolání podle § 265j tr. ř. zamítl. Současně vyslovil souhlas s jeho projednáním v neveřejném zasedání.

Nejvyšší soud jako soud dovolací (§ 265c tr. ř.) shledal, že v této trestní věci je dovolání přípustné [§ 265a odst. 2 písm. a), h) tr. ř.], bylo podáno osobou oprávněnou [§ 265d odst. 1 písm. a) tr. ř.], v zákonné lhůtě a na místě, kde lze podání učinit (§ 265e odst. 1, 2 tr. ř.), a splňuje i obligatorní náležitosti obsahu dovolání uvedené v § 265f odst. 1 tr. ř.

Vzhledem k tomu, že dovolání lze podat jen z důvodů uvedených v ustanovení § 265b tr. ř., musel Nejvyšší soud dále posoudit otázku, zda dovolatelkou uplatněné dovolací důvody lze považovat za důvody uvedené v citovaném ustanovení zákona, jejichž existence je zároveň podmínkou provedení přezkumu napadeného rozhodnutí dovolacím soudem. Současně je třeba dodat, že z hlediska § 265i odst. 1 písm. b) tr. ř. nepostačuje pouhé formální uvedení některého z důvodů vymezených v § 265b odst. 1 písm. a) až *l*) tr. ř. odkazem na toto zákonné ustanovení, ale tento důvod musí být také skutečně v podaném dovolání tvrzen a odůvodněn konkrétními vadami.

Jak již bylo uvedeno, dovolatelka uplatnila dovolací důvody uvedené v § 265b odst. 1 písm. g) a *l*) tr. ř. Z logiky věci je zapotřebí zmínit nejprve druhý z nich, který je procesním dovolacím důvodem obsahujícím dvě alternativy. Podle **§ 265b odst. 1 písm.*l*) tr. ř.** lze totiž dovolání podat, jestliže bylo rozhodnuto o zamítnutí nebo odmítnutí řádného opravného prostředku proti rozsudku nebo usnesení uvedenému v § 265a odst. 2 písm. a) až g) tr. ř., aniž byly splněny procesní podmínky stanovené zákonem pro takové rozhodnutí nebo byl v řízení mu předcházejícím dán důvod dovolání uvedený v § 265b odst. 1 písm. a) až k) tr. ř.

Z obsahu podání je zřejmé, že tento dovolací důvod dovolatelka uplatnila v jeho druhé alternativě, neboť tvrdila, že v řízení, které předcházelo vydání napadeného rozhodnutí, byl dán důvod dovolání uvedený v § 265b odst. 1 písm. g) tr. ř. Tato alternativa by v dané věci mohla být naplněna pouze za předpokladu, že by napadené rozhodnutí a řízení mu předcházející bylo skutečně zatíženo hmotně právními vadami v citovaném důvodu dovolání předpokládanými.

Důvod dovolání podle **§ 265b odst. 1 písm. g) tr. ř.** je dán tehdy, jestliže rozhodnutí spočívá na nesprávném právním posouzení skutku nebo jiném nesprávném hmotně právním posouzení. V mezích uplatněného dovolacího důvodu lze namítat, že skutek, jak byl soudem zjištěn, byl nesprávně právně kvalifikován jako trestný čin, ačkoliv o trestný čin nejde nebo jde o jiný trestný čin, než kterým byl obviněný uznán vinným. Na podkladě tohoto dovolacího důvodu nelze proto přezkoumávat a hodnotit správnost a úplnost skutkových zjištění, na nichž je napadené rozhodnutí založeno, ani prověřovat úplnost provedeného dokazování a správnost hodnocení důkazů ve smyslu ustanovení § 2 odst. 5, 6 tr. ř., poněvadž tato činnost soudu spočívá v aplikaci ustanovení procesních, nikoliv hmotně právních. Vedle vad, které se týkají právního posouzení skutku, lze vytýkat též "jiné nesprávné hmotně právní posouzení". Rozumí se jím zhodnocení otázky, která nespočívá přímo v právní kvalifikaci skutku, ale v právním posouzení jiné skutkové okolnosti mající význam z hlediska hmotného práva.

Nejvyšší soud není další odvolací instancí, nemůže přezkoumávat a posuzovat postup hodnocení důkazů obou stupňů. V takovém případě by se totiž dostával do pozice soudu druhého stupně a suploval jeho činnost (k tomu srov. přiměřeně usnesení Ústavního soudu např. ve věcech sp. zn. I. ÚS 412/02, III. ÚS 732/02, III. ÚS 282/03, II. ÚS 651/02). Dovolací soud je naopak povinen vycházet ze skutkových zjištění soudů prvního (a event. druhého) stupně a teprve v návaznosti na jimi zjištěný skutkový stav může posuzovat hmotně právní posouzení skutku. V této souvislosti je také třeba připomenout, že z hlediska nápravy skutkových vad trestní řád obsahuje další mimořádné opravné prostředky, a to především obnovu řízení (§ 277 a násl. tr. ř.) a v určitém rozsahu i stížnost pro porušení zákona (§ 266 a násl. tr. ř.).

Nejvyšší soud shledal, že námitky vznesené dovolatelkou jsou z hlediska uplatněných dovolacích důvodů relevantní a opodstatněné. Jelikož současně neshledal důvody pro odmítnutí dovolání podle § 265i odst. 1 tr. ř., přezkoumal podle § 265i odst. 3 tr. ř. zákonnost a odůvodněnost výroků napadeného rozhodnutí, proti nimž bylo dovolání podáno, v rozsahu a z důvodů uvedených v dovolání, jakož i řízení napadenému rozhodnutí předcházející. K vadám výroků, které nebyly dovoláním napadeny, přihlížel, jen pokud by mohly mít vliv na správnost výroků, proti nimž bylo podáno dovolání.

Z důvodu přehlednosti a vymezení rozsahu své přezkumné činnosti Nejvyšší soud považuje za vhodné upozornit na to, že podané dovolání (a předtím ani odvolání státního zástupce) nesměřovalo proti právní kvalifikaci skutku popsaného pod bodem 3) rozsudku soudu prvního stupně, a proto tento výrok nepřezkoumával.

III

K řešené problematice je zapotřebí (toliko ve stručnosti a jen v obecné rovině) uvést, že trestného činu šíření pornografie podle § 205 odst. 2 písm. a) tr. zák. se dopustí ten, *kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě.*

Přečinu šíření pornografie podle § 191 odst. 1 trestního zákoníku se dopustí ten, *kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, v němž se projevuje násilí či neúcta k člověku, nebo které popisuje, zobrazuje nebo jinak znázorňuje pohlavní styk se zvířetem.*

Z hlediska subjektivní stránky je jak trestný čin šíření pornografie podle § 205 odst. 2 písm. a) tr. zák., tak i přečin šíření pornografie podle § 191 odst. 1 trestního zákoníku trestným činem úmyslným [srov. § 4 písm. a), b) tr. zák. a § 15 odst. 1, 2 v návaznosti na § 13 odst. 2 trestního zákoníku].

Podle tzv. právní věty odsuzujícího rozsudku obviněný jednak *"jinak jinému opatřil elektronické pornografické dílo, které zobrazuje nebo jinak využívá dítě"* [bod 1) rozsudku], jednak *"jinak jinému opatřil elektronické pornografické dílo, které zobrazuje pohlavní styk se zvířetem"* [bod 2) rozsudku].

Ze skutkových zjištění učiněných soudem prvního stupně a popsaných v tzv. skutkových větách jeho odsuzujícího rozsudku se přitom podává, že obviněný se uvedených trestných činů dopustil tím, že (zkráceně) *odeslal ze své e-mailové schránky na 24 jiných (v rozsudku specifikovaných) e-mailových adres nejméně 47 e-mailových zpráv s přílohami obsahujícími pornografické fotografie a videosoubory zobrazující nebo jinak využívající děti* [bod 1) rozsudku], resp. že *na 2 e-mailové adresy (uvedené v tzv. skutkové větě odsuzujícího rozsudku) nejméně 6 e-mailových zpráv s přílohami obsahujícími pornografické fotografie a videosoubory, které zobrazují pohlavní styk se zvířetem* [bod 2) rozsudku].

Takto zjištěná jednání soud prvního stupně právně kvalifikoval jako trestný čin šíření pornografie podle § 205 odst. 2 písm. a) tr. zák. [bod 1) rozsudku] a jako přečin šíření pornografie podle § 191 odst. 1 trestního zákoníku [bod 2) rozsudku]. Jelikož k naplnění zákonných znaků obou těchto trestných činů neměla nejvyšší státní zástupkyně naprosto žádných výhrad, v rámci dovolacího řízení není zapotřebí se k nim blíže vyjadřovat. Ostatně učiněná skutková zjištění jednoznačně svědčí o tom, že jednotlivé z těchto zákonných znaků (*jinak jinému opatřil; elektronické pornografické dílo; dílo, které zobrazuje nebo jinak využívá dítě; dílo, které zobrazuje pohlavní styk se zvířetem*) byly jednáním obviněného naplněny.

Nalézací soud však neakceptoval právní kvalifikaci použitou v podané obžalobě, podle níž se obviněný dopustil v obou případech jmenovaných trestných činů v jejich tzv. kvalifikované podobě, tedy podle § 205 odst. 2 písm. a), odst. 3 písm. b) tr. zák. a podle § 191 odst. 1, 3 písm. b) trestního zákoníku. V odůvodnění svého rozhodnutí na straně 5 k této problematice uvedl, že *"... je třeba vzít v potaz naplnění subjektivní stránky jednání obžalovaného, … už samotná podstata takto zasílaného "obsahově závadného" e-mailu a jeho zveřejnění je pro případného pachatele naprosto nežádoucí, neboť ten těžko může mít zájem na svém odhalení vzhledem k obsahu svého e-mailu … E-mailová komunikace je jako jakákoli jiná komunikace založená na vyměňování informací mezi jednotlivě určenými subjekty. Každý uživatel musí mít pro příjem zpráv svoji e-mailovou adresu, která identifikuje jeho elektronickou poštovní schránku … tato adresa je chráněná heslem, které si každý uživatel volí dle svého uvážení … Soud … nevidí příliš rozdílu mezi oběma typy komunikace, byť elektronická komunikace se může jevit daleko sofistikovanější a možnosti jak proniknout do obsahu této komunikace jsou zřejmě větší, … e-mailová komunikace je předmětem ochrany z hlediska obsahu, neboť i zde je chráněno tajemství dopravovaných zpráv ve smyslu čl. 13 Listiny základních práv a svobod, konečně i trestním právem … ve smyslu § 182 odst. 1 písm. b) trestního zákoníku. Stav, kdy stát garantuje na jedné straně ochranu tajemství takto dopravovaných zpráv, a na straně druhé by v zásadě kvalitu způsobu přenosu … prostřednictvím sítě elektronické komunikace ponížil na úroveň, kdy účastník, resp. odesílatel zpráv je nucen předpokládat, že taková ochrana bude porušena a zpráva zveřejněna, je zcela kontradiktorní …".*

K těmto závěrům soud druhého stupně bez bližšího zdůvodnění pouze paušálně uvedl, že se s nimi ztotožňuje a *"… odkazuje … na příslušnou část odůvodnění napadeného rozsudku, neboť s tímto odůvodněním se v plném rozsahu ztotožnil, zejména ve vztahu k otázce naplnění objektivních znaků pro přísnější právní kvalifikaci"* (srov. stranu 3 odůvodnění jeho usnesení).

Nejvyšší soud se s takovými (poměrně kategorickými) závěry nemohl bezezbytku identifikovat, neboť je přesvědčen, že žádný ze soudů nižších instancí dostatečně nezvážil povahu a účel, k němuž slouží jednak Internet, jednak e-mailová komunikace (jako zřejmě základní komunikační prostředek na Internetu) a v jejím rámci e-mailové adresy, jichž obviněný pro předávání fotografií a videosouborů s pornografickou tématikou jiným subjektům využíval. Hodnotit a pečlivěji zkoumat bylo zapotřebí zejména to, zda škodlivý obsah obviněným odeslaných e-mailových zpráv nebyl rozšířen prostředky a způsobem, které nevylučují, aby se s ním seznámil větší počet lidí než pouze okruh odesílatelem přesně vymezených a e-mailovými adresami definovaných adresátů.

K tomu je zapotřebí (opět jen ve stručnosti a v obecné rovině) zmínit, že trestného činu šíření pornografie podle § 205 odst. 3 písm. b) tr. zák. se pachatel dopustí, *spáchá-li čin uvedený v odstavci 1 nebo 2 tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem.*

Obdobně přečinu šíření pornografie podle § 191 odst. 1, 3 písm. b) trestního zákoníku se pachatel dopustí, *spáchá-li čin uvedený v odstavci 1 nebo 2 tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem.*

Bylo-li výše uvedeno, že u obou těchto trestných činů se po subjektivní stránce vyžaduje úmysl, je třeba dodat, že u šíření pornografie právě uvedenými způsoby se z povahy věci vyžaduje alespoň eventuální úmysl [srov. § 4 písm. b) tr.

zák., resp. § 15 odst. 1, 2 v návaznosti na § 13 odst. 2 a § 17 trestního zákoníku].

Z uvedených alternativ těchto kvalifikovaných skutkových podstat sice v dané věci nemají zásadní význam prvé čtyři znaky (spáchání činu *tiskem, filmem, rozhlasem či televizí*), neboť obviněný zjištěným jednáním žádný z nich nenaplnil, nelze však od nich zcela odhlížet, jelikož jsou jedním ze srovnávacích hledisek při výkladu znaku *jiným obdobně účinným způsobem.*

V prvé řadě je ovšem třeba zaměřit pozornost na výklad znaku *veřejně přístupná počítačová síť*. Tento pojem se Nejvyšší soud pokusil již minulosti v několika svých rozhodnutích vyložit. Zřejmě poprvé se tak stalo v jeho usnesení ze dne 29. 9. 2010, sp. zn. 6 Tdo 1135/2010, jímž ovšem dovolání obviněného odmítl podle § 265i odst. 1 písm. b) tr. ř. jako podané z jiného důvodu, než je uveden v § 265b tr. ř., takže jen stručně a s odkazem na starší komentované vydání trestního zákona uvedl, že *"… pod pojmem veřejně přístupnou počítačovou sítí se rozumí funkční propojení počítačů do sítí s cílem vytvořit informační systém pracující s tzv. dálkovým přístupem, jakým je především internet a jiné podobné informační systémy (Šámal, P., Púry, F., Rizman, S. Trestní zákon. Komentář. 4. vydání. Praha: C. H. Beck. 2001, str. 1231),*k čemuž dodal, že *"… v této souvislosti bylo prokázáno, že* (obviněný) *počítačovou sítí přeposílal do emailových schránek digitální fotografie s tématikou dětské pornografie".*

Obdobně vyznělo i odůvodnění rozsudku Nejvyššího soudu ze dne 27. 1. 2011, sp. zn. 4 Tz 79/2010, podle něhož obviněný tím, že *"… k páchání trestné činnosti využíval webového portálu Xchat, … se připojil do "místnosti" nazvané "báječný flirt", vyměňoval si e-mailové zprávy s tématikou dětské pornografie s dalšími pro něj anonymními osobami, … tímto způsobem činil e-mailové zprávy přístupné veřejnosti blíže neurčenému počtu osob. Přístup do oné "místnosti" tj. virtuálního prostoru, v němž probíhala komunikace mezi jednotlivými zájemci o dětskou pornografii, mohl ovšem obviněný získat výlučně prostřednictvím Internetu, tj. veřejně přístupné počítačové sítě. Je proto mimo pochybnost, že zaslání pornografického díla elektronickou poštou je uvedením do oběhu prostřednictvím veřejně přístupné počítačové sítě a toto jednání podle právní úpravy platné do 31. 12. 2009 naplňovalo skutkovou podstatu trestného činu šíření pornografie podle § 205 odst. 2 písm. a), odst. 3 písm. b) tr. zákona"*. K tomu je ovšem třeba dodat, že skutková zjištění tu byla přece jen poněkud odlišná jak od posuzované věci, tak od ostatních zmiňovaných věcí (srov. *"… poté, co … založil e-mailové schránky … za účelem výměny fotografií pornografického charakteru s ostatními uživateli webového portálu Xchat, pomocí těchto e-mailových schránek … přijímal e-mailové zprávy s tématikou dětské pornografie a … přeposílal ostatním uživatelům webového portálu Xchat …").*

V odůvodnění naposledy citovaného rozsudku Nejvyšší soud s odkazem na odbornou literaturu (Šámal, P. a kol., Trestní zákoník II, Komentář, I. vydání, Praha, C.H.Beck 2010, str. 1699 - 1700) rovněž uvedl, že *"… veřejně přístupnou počítačovou sítí se rozumí funkční propojení počítačů do sítí s cílem vytvořit informační systém pracující s tzv. dálkovým přístupem, jakým je především Internet a jiné podobné informační systémy. Z technického hlediska je veřejně přístupná počítačová síť soustavou serverů, datových komunikací a k nim připojených počítačů. Z organizačního hlediska jde o provozovatele jednotlivých sítí a podsítí, zprostředkovatele připojení i uživatele a další subjekty. Internet jako světová informační počítačová síť vznikl propojováním původně privátních, specializovaných a autonomních datových sítí (vojenské, školní, energetické apod.) a později již veřejných takovýchto sítí (přístupných většinou za úplatu každému zájemci) s postupnou změnou jejich charakteru (přechod na jednotný protokol řízení přenosu Transmission Control Protocol/Internet Protocol, budovaných na principu dobrovolných dohod atd.), včetně užívání zdarma. Rozhodujícím okamžikem byl vznik služby WWW (World Wide Web), která byla vytvořena v internetu na bázi počítačových serverů (části Internetu) ukazujících jeden k druhému s využitím tzv. hypertextových odkazů, podpory multimedií a integrování různých služeb. WWW stránka neboli webová stránka je elektronický dokument, který se nachází na určitém serveru, jeho obsah je připojen k síti (indexován) pomocí hypertextových odkazů na jiná místa tohoto dokumentu nebo v jiných dokumentech na tomto serveru nebo na zcela jiných serverech nacházejících se v síti Internetu. Veřejně přístupnou počítačovou sítí výslovně nejsou pouze uzavřené počítačové sítě některých právnických osob, státních orgánů nebo jiné organizace, které nesplňují podmínku veřejné přístupnosti"*. Odkázal tam i na dovolatelkou zmiňované usnesení Nejvyššího soudu ze dne 21. 5. 2009, sp. zn. 11 Tdo 349/2009 (to se však týkalo trestného činu porušování tajemství dopravovaných zpráv podle § 239 odst. 1 tr. zák.), podle něhož *"… není pochyb o tom, že elektronická pošta zasílaná prostřednictvím internetu, tzv. email, je jiným veřejným zařízením ve smyslu § 239 odst. 1 písm. b) tr. zák."*, a dále *"… naprostá většina providerů kopie všech e-mailových zpráv ukládá na svoje servery před doručením a tyto zálohy ponechává na serveru často po dobu i více měsíců po doručení zprávy, a to i v případech, že tyto zprávy jsou ve schránkách odesilatele i příjemce již vymazány, … zde k nim mohly mít přístup i jiné osoby, než ty, kterým byla zpráva určena. Ochrana dopravované e-mailové zprávě je totiž poskytována v době jejího "podávání", tedy v průběhu doručování. Konec tohoto procesu je nutno vnímat v okamžiku doručení do e-mailové schránky příjemce. Do schránky má příjemce zprávy přístup, který je zabezpečen pomocí hesla, může se přitom do schránky dostat z kteréhokoli počítače připojeného k Internetu, … V této souvislosti nelze pominout i problém virů, tj. krátkých počítačových programů určených k provedení úkonů nad rámec vůle uživatele, které mohou mít kromě vlivu na narušení nebo likvidaci instalovaných programů, také vliv i na odesílání uložených dat a programů uživatele bez jeho výslovného pokynu".*

V odůvodnění dalšího usnesení dne 12. ledna 2011, sp. zn. 8 Tdo 1467/2010, Nejvyšší soud podrobně shrnul problematiku řešenou i v posuzované věci a uvedl, že *"…enormní počet příjemců, jimž obviněný … soubory zaslal, bylo nutné hodnotit z hlediska možného naplnění znaku "spáchání činu veřejně" [§ 89 odst. 4 písm. a) tr. zák.], jenž vyjadřuje podstatu ustanovení § 205 odst. 3 písm. b) tr. zák. jako kvalifikované skutkové podstaty, a bylo nutné jej zkoumat ze všech s ním spojených a rozhodných hledisek. Uvedené skutečnosti bylo potřeba posuzovat kromě jiného i se zřetelem na podstatu a hlavní smysl tohoto znaku, jímž je vyjádřena vyšší škodlivost a nebezpečnost činu, jestliže je zakázaný nebo z jiných důvodů škodlivý obsah rozšířen prostředky a způsobem jež zajišťují, aby se s ním seznámil velký počet lidí. Ustanovení § 89 odst. 4 písm. a) tr. zák. za tyto způsoby označuje: obsah tiskoviny nebo rozšiřovaný spis, film, rozhlas, televizi nebo jiný obdobně účinný způsob. V ustanovení § 205 odst. 3 písm. b) tr. zák. byl vedle těchto forem vyjádřen i další samostatný způsob veřejně přístupnou počítačovou sítí"*. V rámci úvah o tomto zákonném znaku uvedl, že *"… za veřejně přístupnou počítačovou sítí se považuje funkční propojení počítačů do sítí s cílem vytvořit informační systém pracující s tzv. dálkovým přístupem, jakým je především Internet a jiné podobné informační systémy. Internet je informační a komunikační*

systém, který se skládá z různých subjektů a objektů právních vztahů. S ohledem na rozvoj počítačových informačních a komunikačních technologií má Internet kromě jiného i povahu prostředku, jehož prostřednictvím lze veřejně šířit informace. S ohledem na celosvětovou propojenost a rozšířenost počítačových médií je virtuální svět Internetu považován za veřejný prostředek, neboť lze již považovat za notorietu, že je používán právě pro zveřejňování a šíření informací (srov. Smejkal, V. a kol. Právo informačních a telekomunikačních systémů. 1. vydání. Praha: C. H. Beck, 2001), … Internet je počítačovou sítí, která funguje jako přenosové médium umožňující využívání určitých služeb, z nichž nejvýznamnější je přenos informací, tj. znalostí, které je možné jakoukoli formou sdělovat, a jde o poznatek týkající se jakýchkoliv objektů, fakt, událostí, věcí procesů, myšlenek, které mají v daném kontextu specifický význam (srov. Smejkal, V. a kol. Právo informačních a telekomunikačních systémů. 1. vydání. Praha: C. H. Beck, 2001, s. 39, 40). Za informační systém se považuje funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost. Každý informační systém zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, a dále nástroje umožňující výkon informačních činností [srov. § 2 písm. b) zák. č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů]. Jde o systém pro sběr, zpracování, ukládání a vyhledávání a šíření informací (Knapp, V., Právo a informace, Academia, Praha, 1988 s. 43), … E-mailová adresa pak představuje elektronickou službu spočívající v elektronické poště, která je (podle Všeobecné encyklopedie, Praha: Nakladatelský dům, 1996) definována jako "telekomunikační služba instalovaná převážně na standardních počítačových sítích, určena k přenosu zpráv mezi počítačovými pracovišti, k ukládání těchto zpráv do paměťových schránek, k třídění a předzpracování zpráv. Vyznačuje se efektivním a levným provozem" (srov. Smejkal, V. a kol. Právo informačních a telekomunikačních systémů. 1. vydání. Praha: C. H. Beck, 2001, s. 205).

S odkazem na uvedenou odbornou literaturu Nejvyšší soud v citovaném usnesení své úvahy uzavřel tím, že *"… s ohledem na všechny skutečnosti a parametry, kterých Internet coby významný a vysoce sofistikovaný fenomén současné doby dosahuje, není sporu o tom, že jde o veřejně přístupnou počítačovou síť …"*. Dále pak pokračoval, že *"… e-mail je nejznámějším druhem elektronické pošty, jíž je textová, hlasová nebo obrazová zpráva poslaná prostřednictvím veřejné sítě elektronických komunikací, která může být uložena v síti nebo koncovém zařízení uživatele, dokud ji uživatel nevyzvedne. Důvěrnost zpráv a s nimi spojené provozní a lokalizační údaje jsou chráněny podle § 89 a násl. zák. č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů (srov. Hendrych, D. a kol. Právnický slovník, 3. podstatně rozšířené vydání, Praha: C. H. Beck, 2009, s. 206)"*. Připomněl rovněž, že podle § 89 naposledy citovaného zákona *"… podnikatelé zajišťující veřejné komunikační sítě nebo poskytující veřejně dostupné služby elektronických komunikací jsou povinni zajistit technicky a organizačně důvěrnost zpráv a s nimi spojených provozních a lokalizačních údajů, které se přenášejí prostřednictvím jejich veřejné komunikační sítě a veřejně dostupných služeb elektronických komunikací. Zejména nepřipustí odposlech, ukládání zpráv nebo jiné druhy zachycení nebo sledování zpráv a s nimi spojených údajů osobami jinými, než jsou uživatelé, bez souhlasu dotčených uživatelů, pokud zákon nestanoví jinak. To nebrání technickému ukládání údajů, které je nezbytné pro přenos zpráv, aniž by byla dotčena zásada důvěrnosti"*, a že podle § 89 odst. 2 tohoto zákona *"… zprávou se rozumí jakákoli informace, která se vyměňuje nebo přenáší mezi konečným počtem účastníků nebo uživatelů prostřednictvím veřejně dostupné služby elektronických komunikací, s výjimkou informace přenášené jako součást veřejného rozhlasového nebo televizního vysílání sítí elektronických komunikací, nelze-li ji přiřadit k určitelnému účastníkovi nebo uživateli, který tuto informaci přijímá"*.

A aby byl odkaz na odůvodnění zmiňovaného usnesení co nejúplnější, je ještě třeba uvést tam obsažené shrnutí, že *"… ze všech těchto stručně vyjádřených základních pojmových znaků jak Internetu, tak i e-mailu, je zřejmé, že ochrana podle § 89 a násl. zák. č. 127/2005 Sb. přísluší obsahu elektronicky rozesílané zprávy, kdežto e-mailová adresa jako identifikační místo umožňující elektronickou službu spočívající v elektronické poště, tj. v elektronickém přenosu zpráv, uvedené ochrany nepožívá. Nepožívá však ani ochrany podle zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. E-mailovou adresu lze přidělit pouze určitému uživateli na základě smlouvy uzavřené s poskytovatelem připojení (providerem), u něhož je vytvořen a veden systém obsahující informace o osobách (náležitostí smlouvy jsou totiž osobní údaje - jméno, příjmení, adresa, rodné číslo apod.) Na něj se vztahují všechny povinnosti provozovatelů informačních systémů obsahujících osobní údaje občanů ve smyslu zákona č. 101/2000 Sb. Přiřadit konkrétní osobu k takové elektronické adrese může tedy pouze provider, a pokud by tak učinil někdo jiný, porušil by zákon on nebo ten, kdo by mu data poskytl. Existuje tedy sice propojení mezi adresou a identifikací osoby, a to ve smlouvě mezi uživatelem a poskytovatelem připojení, nicméně se nejedná o veřejně dostupný údaj. Bude-li mít někdo disponovat jakýmkoliv způsobem sestaveným souborem existujících e-mailových adres bez dalších údajů, zejména bez výše uvedeného propojení s určitou fyzickou osobou, nejedná se tedy zřejmě o soubor obsahující osobní údaje a nevztahuje se na něj žádná ochrana z hlediska zák. č. 101/2000 Sb. Samotná elektronická (e-mailová) adresa nebo jiný identifikátor používaný na Internetu není osobním údajem ve smyslu § 4 písm. a) zák. č. 101/2000 Sb. a nepoužívá ochrany při svém izolovaném výskytu (srov. Smejkal, V. a kol. Právo informačních a telekomunikačních systémů. 1. vydání. Praha: C. H. Beck, 2001, s. 428, 429)"*.

S touto podrobně rozvedenou argumentací je zapotřebí v zásadě souhlasit. Zároveň je ovšem třeba zdůraznit, že jakkoliv otázka výkladu pojmu spáchání činu *veřejně přístupnou počítačovou sítí* je otázkou právní, k jejímuž správnému vyřešení sice mohou napomoci jak shora zmíněná ustanovení jednotlivých zákonů, tak citované názory respektovaných autorů, nelze se obejít bez specifických odborných podkladů (rozhodně ale nelze vystačit s laickými a odborně nepodloženými úvahami ať už obou soudů nižších instancí, nebo dovolatelky).

Z obsahu spisového materiálu v posuzované věci je zřejmé, že této skutečnosti si byly vědomy již orgány přípravného řízení, a proto přibraly k podání odborného vyjádření RNDr. J. H., CSc., soudního znalce z oboru kriminalistiky, odvětví počítačové expertízy (srov. č. l. 36 spisu). Tento soudní znalec v písemném odborném vyjádření (srov. č. l. 39 až 48 spisu) sice zodpověděl všechny položené otázky, žádná z nich však nebyla zaměřena na problematiku e-mailové korespondence jako možného způsobu komunikace *veřejně přístupnou počítačovou sítí*. Vypracované odborné vyjádření soud prvního stupně v průběhu hlavního líčení pouze přečetl (srov. č. l. 292 a 293 spisu), aniž soudního znalce předvolal a k obsahu odborného vyjádření blíže vyslechl. Tento nedostatek dokazování neodstranil v průběhu veřejného zasedání (srov. č. l. 318 a 319 spisu) ani odvolací soud, v důsledku čehož si ani on nevytvořil dostatečné skutkové předpoklady pro náležité posouzení zmiňované právní otázky.

Především v důsledku toho oba soudy nižších stupňů neposuzovaly skutky obviněného popsané pod body 1) a 2) výroku odsuzujícího rozsudku ze všech shora naznačených hledisek, a aniž by všechny zmíněné skutečnosti hodnotily jak jednotlivě, tak v jejich souhrnu, přinejmenším předčasně vyloučily, že obviněný oba činy spáchal *veřejně přístupnou počítačovou sítí* [v návaznosti na to pak vyloučily i možnost tyto skutky právně kvalifikovat i podle odst. 3 písm. b) § 205 tr. zák., resp. odst. 3 písm. b) § 191 trestního zákoníku].

Současně oba soudy ani neuvažovaly o další nabízející se alternativě, a to o *jiném obdobně účinném způsobu spáchání* předmětných trestných činů. Za takový způsob (jako je tisk, rozhlas, televize nebo veřejně přístupná počítačová síť) zákon považuje takovou formu přenosu nebo jiného předání určité písemné, zvukové nebo hlasové informace, jestliže je zpřístupněna většímu počtu příjemců, tedy veřejnosti ve formě blíže neurčitého počtu lidí, přičemž nezávisí na tom, zda přístup veřejnosti je zcela volný, nebo je omezen například zaplacením určitých poplatků, tzv. klubovou příslušností apod. Dále sem lze zařadit i místní rozhlas, vysílací stanici apod. (srov. Šámal, P., Púry, F., Rizman, S. Trestní zákon. Komentář. II. díl. 6., doplněné a přepracované vydání. Praha: C. H. Beck, 2004, s. 1232).

Jestliže se ve smyslu uvedeného vymezení za znak *jiného obdobně účinného způsobu* považuje např. nahrávka na gramofonové desce, magnetofonovém pásku, magnetofonové kazetě, videokazetě, záznam na počítačové disketě apod., pak je nutné zvažovat, zda mezi ně nelze zahrnout i počítačové soubory subsumované pod e-mailovou adresu, jejímž prostřednictvím jsou dále předávány, tj. rozesílány dalším e-mailovým příjemcům. Nelze totiž odhlížet od skutečnosti, že stejně jako u osobně vytvořeného záznamu na magnetofonovém pásku nebo na vlastnoručně vyrobeném filmovém záznamu, jde i u počítačového souboru v e-mailové adrese o záznamy, které se vytvářejí soukromě a informace na nich uložená, pokud není nabízena, přenechávána nebo zpřístupňována osobě mladší osmnácti let [§ 205 odst. 2 písm. a) tr. zák.], nepožívá ochrany trestního zákona. Teprve tehdy, je-li nabízena, přenechávána nebo zpřístupňována osobě mladší osmnácti let, stává se trestnou. Obdobná situace jako u předání informace většímu počtu příjemců například tím, že se přehraje film nebo videozáznam apod., nastane i tehdy, když se počítačové soubory rozešlou prostřednictvím e-mailové pošty většímu počtu e-mailových adresátů. V takovém případě by bylo možno i elektronickou poštu reálně považovat za okolnost naplňující zákonný znak jiného obdobně účinného způsobu ve smyslu odst. 3 písm. b) § 205 tr. zák., resp. odst. 3 písm. b) § 191 trestního zákoníku (to v případě, že by odvolací soud, jemuž je věc přikazována k novému projednání a rozhodnutí, neshledal naplněným znak veřejně přístupnou počítačovou sítí).

Lze tak uzavřít, že oba soudy nižších stupňů při úvahách o právní kvalifikaci skutků, jimiž byl obviněný uznán vinným pod body 1) a 2) odsuzujícího rozsudku, bezezbytku nezvážily všechny výše naznačené možnosti a skutečnosti, které by eventuelně mohly zakládat důvod pro právní posouzení těchto skutků podle přísnějších (shora opakovaně uváděných) ustanovení trestního zákona, resp. trestního zákoníku.

Nejvyšší soud proto podle § 265k odst. 1 tr. ř. dovoláním nejvyšší státní zástupkyně napadené usnesení Krajského soudu v Brně ze dne 23. 9. 2010, sp. zn. 7 To 442/2010, zrušil. Současně podle § 265k odst. 2 tr. ř. zrušil také všechna další rozhodnutí na zrušené rozhodnutí obsahově navazující, pokud vzhledem ke změně, k níž došlo zrušením, pozbyla podkladu. Poté podle § 265l odst. 1 tr. ř. Krajskému soudu v Brně přikázal, aby věc v potřebném rozsahu znovu projednal a rozhodl. Bylo totiž v možnostech tohoto odvolacího soudu, aby jednoduchým doplněním dokazování si vytvořil náležité předpoklady pro vypořádání se s odvolacími námitkami především ze strany státního zástupce.

Po rozhodnutí Nejvyššího soudu se věc vrací do stadia řízení před soudem druhého stupně, na němž bude, aby po doplnění dokazování znaleckým posudkem z oboru kriminalistiky, odvětví počítačové expertízy, znovu a daleko pečlivěji, než se v jeho předchozím rozhodnutí stalo, zvážil všechny skutečnosti významné z hlediska možných způsobů rozhodnutí o vině obviněného. Zejména se bude muset detailněji zaměřit na určení povahy e-mailové komunikace jakožto prostředku elektronické pošty provozovaného v rámci internetových služeb, zvláště s ohledem na možnosti jejího zabezpečení a rizika úniku obsahu zpráv přepravovaných jejím prostřednictvím. Na základě takto upřesněných skutkových zjištění bude na něm, aby pečlivě posoudil, zda jednání obviněného naplňuje nejen základní, ale i kvalifikované znaky skutkových podstat obou trestných činů kladených mu za vinu. Je jen samozřejmé, že skutkové i právní závěry, které v tomto směru učiní, musí náležitě odůvodnit, aby odůvodnění jeho nového rozhodnutí odpovídalo požadavkům obsaženým v ustanovení § 125 odst. 1 tr. ř., resp. § 134 odst. 2 tr. ř. (odůvodnění jeho předchozího usnesení tyto požadavky rozhodně nesplňuje).

Současně Nejvyšší soud připomíná, že soud druhého stupně je při novém rozhodnutí ve věci vázán právním názorem vysloveným v tomto usnesení (srov. § 265s odst. 1 tr. ř.), a vzhledem k tomu, že napadené rozhodnutí bylo zrušeno v důsledku dovolání podaného nejvyšší státní zástupkyní v neprospěch obviněného, neplatí zákaz reformace in peius ve smyslu ustanovení § 265s odst. 2 tr. ř.

V souladu s ustanovením § 265r odst. 1 písm. b) tr. ř. Nejvyšší soud učinil toto rozhodnutí v neveřejném zasedání, neboť vady napadeného rozhodnutí vytknuté dovoláním a zjištěné Nejvyšším soudem nebylo možno odstranit v řízení o dovolání ve veřejném zasedání.

Poučení:

Proti rozhodnutí o dovolání není s výjimkou obnovy řízení opravný prostředek přípustný (§ 265n tr. ř.).

V Brně dne 27. dubna 2011

Předseda senátu:

JUDr. Jan Bláha

3 Tdo 414/2011-21

K tomu, že zaslání pornografického díla zobrazující nebo jinak využívající dítě mezi odesílatelem a příjemcem e-mailové zprávy nenaplňuje znak „veřejně přístupnou počítačovou sítí“

Zaslání pornografického díla elektronickou poštou je uvedením do oběhu prostřednictvím veřejně přístupné počítačové sítě a toto jednání naplňovalo skutkovou podstatu trestného činu šíření pornografie podle § 205 odst. 2 písm. a), odst. 3 písm. b) TZ [ve znění účinném do 31. 12. 2009, od 1. 1. 2010 zločin výroba a jiné nakládání s dětskou pornografií podle § 192 odst. 2 alinea první, odst. 3 písm. b) TZ].

Jestliže však k pornografickým dílům měli přístup toliko konkrétní adresáti e-mailových zpráv (tj. pachatel jako odesílatel zprávy a příjemce), a jednalo se tak o nikoli široký, předem nevymezený okruh osob, není naplněn znak „veřejně přístupnou počítačovou sítí“ ve smyslu § 205 odst. 3 písm. b) TZ [ve znění účinném do 31. 12. 2009, od 1. 1. 2010 ve smyslu § 192 odst. 3 písm. b) TZ]. V takovém případě je využití veřejně přístupné počítačové sítě k šíření pornografických děl způsob nikoli veřejně přístupný.

USNESENÍ

Nejvyšší soud

České republiky rozhodl v neveřejném zasedání konaném dne 4. května 2011 o dovolání nejvyššího státního zástupce podaném v neprospěch obviněného P. L. , proti rozsudku Krajského soudu v Brně, pobočka v Jihlavě, ze dne 24. 11. 2010, sp. zn. 42 To 355/2010, jako soudu odvolacího v trestní věci vedené u Okresního soudu ve Žďáru nad Sázavou pod sp. zn. 13 T 85/2010, takto:

Podle § 265i odst. 1 písm. e) tr. ř. se dovolání nejvyššího státního zástupce odmítá.

Odůvodnění:

I.**Rozsudkem Okresního soudu ve Žďáru nad Sázavou ze dne 3. 9. 2010, sp. zn. 13 T 85/2010**, byl obviněný P. L. uznán vinným trestným činem šíření pornografie podle § 205 odst. 2 písm. a) zákona č. 140/1961 Sb., trestního zákona, účinného do 31. 12. 2009 (dále jen "tr. zák."), a trestným činem přechovávání dětské pornografie podle § 205a tr. zák., jichž se dopustil tím, že "*nejméně v období od 13. 11. 2007 do 5. 3. 2009 v internetové kavárně v městské části P. v P., v místě svého bydliště na ul. S. ve Ž. n. S. nebo na přesně nezjištěném místě v P. za použití počítačů umístěných na výše uvedených místech prostřednictvím elektronické pošty používaje jednak přijal a nejméně do dne 10. 3. 2009 přechovával celkem nejméně 76 zpráv obsahujících soubory pornografických fotografií a videonahrávek, na kterých byly zachyceny děti při souloži s dospělými, orálním pohlavním styku s dospělými a jiných sexuálních praktikách nebo v různých sexuálně vyzývavých pozicích,*

a jednak přinejmenším v období od 27. 6. 2008 do 3. 3. 2009 některé z těchto zpráv, nejméně v pěti případech, odeslal na e-mailové adresy užívané dosud neznámými osobami, a to dne 27. 6. 2008 v 18.26 hodin a 18.31 hodin na e-mailovou adresu dne 10. 1. 2009 v 11.12 hodin na e-mailovou adresu dne 14. 1. 2009 v 11.45 hodin na e-mailovou adresu a dne 3. 3. 2009 na e-mailovou adresu".

Za to byl obviněný odsouzen podle § 205 odst. 2 za použití § 35 odst. 1 tr. zák. k trestu odnětí svobody v trvání 8 (osmi) měsíců, jehož výkon byl podle § 58 odst. 1 a § 59 odst. 1 tr. zák. podmíněně odložen na zkušební dobu v trvání 2 (dvou) let. Současně byl obviněnému uložen trest propadnutí věci nebo jiné majetkové hodnoty, a to 3 ks CD-R, které byly zajištěny dne 14. 10. 2009 při domovní prohlídce, a které jsou přílohou spisu.

Okresní soud ve Žďáru nad Sázavou plně převzal skutková tvrzení z obžaloby státního zástupce Okresního státního zastupitelství ve Žďáru nad Sázavou ze dne 1. 6. 2010, sp. zn. ZT 442/2009, neakceptoval však státním zástupcem navrhovanou právní kvalifikaci, pokud státní zástupce požadoval, aby byl obviněný P. L. uznán vinným trestným činem šíření pornografie spáchaným v kvalifikované skutkové podstatě podle § 205 odst. 2 písm. a), odst. 3 písm. b) tr. zák., tedy, že se činu dopustil veřejně přístupnou počítačovou sítí.

Proti rozsudku Okresního soudu ve Žďáru nad Sázavou podal státní zástupce Okresního státního zastupitelství

ve Žďáru nad Sázavou v neprospěch obviněného odvolání (č. l. 161 - 164), které zaměřil do výroků o vině i o trestu. Státní zástupce v odvolání uvedl, že trvá na tom, aby byl skutek právně posouzen jako trestný čin šíření pornografie spáchaný v kvalifikované skutkové podstatě podle § 205 odst. 2 písm. a), odst. 3 písm. b) tr. zák., neboť obviněný P. L. se svého jednání dopustil veřejně přístupnou počítačovou sítí.

Krajský soud v Brně, pobočka v Jihlavě, na podkladě podaného odvolání **rozsudkem ze dne 24. 11. 2010, sp. zn. 42 To 355/2010**, zrušil podle § 258 odst. 1 písm. b), d) tr. ř. napadený rozsudek soudu prvního stupně, a to ve výroku o trestu propadnutí věci nebo jiné majetkové hodnoty. Současně podle § 259 odst. 3 písm. a) tr. ř. odvolací soud sám znovu rozhodl tak, že obviněnému uložil podle § 55 odst. 1 písm. a) tr. zák. trest propadnutí věci a jiné majetkové hodnoty, a to CD-R č. 2/95, CD-R č. 2/98, CD-R č. 2/101, obsahující dětskou pornografii. Podle § 101 odst. 1 písm. c) tr. zák. odvolací soud dále vyslovil zabrání 1 ks pevného disku Western Digital WD1600JS 160GB-SATA, a 1 ks paměťové karty San disk o kapacitě 2GB, z PC AT Computers, zajištěných při domovní prohlídce dne 9. 10. 2009.

Nutno upozornit, že takto byl rozsudek odvolacího soudu vyhlášen podle protokolu na č. 1. 176 spisu, když v písemném vyhotovení rozsudku odvolacího soudu je pouze uvedeno, že "se napadený rozsudek zrušuje".

II.

Proti usnesení krajského soudu podal **nejvyšší státní zástupce** *dovolání v neprospěch obviněného*, a to z důvodu uvedeného v **§ 265b odst. 1 písm. g) tr. ř.,** neboť má za to, že napadené rozhodnutí spočívá na nesprávném právním posouzení skutku.

Poté, co nejvyšší státní zástupce zrekapituloval dosavadní průběh řízení a argumenty soudů obou stupňů, kteréžto vedly k výroku o vině obviněného, uvedl, že nelze souhlasit se závěry soudů obou stupňů, podle kterých nebyl naplněn znak spáchání činu "veřejně přístupnou počítačovou sítí", čímž by byla naplněna skutková podstata trestného činu šíření pornografie spáchaného v kvalifikované skutkové podstatě podle § 205 odst. 2 písm. a), odst. 3 písm. b) tr. zák. Uvedl, že veřejně přístupnou počítačovou sítí se rozumí funkční propojení počítačů do sítí s cílem vytvořit informační systém pracující s tzv. dálkovým přístupem. Veřejně přístupnou počítačovou sítí je především Internet jako světová informační počítačová síť a jiné podobné informační systémy. Namítl, že dle vymezení skutku ve výroku o vině vyplývá, že obviněný P. L. nejméně v pěti případech odeslal na e-mailové adresy užívané dosud neznámými osobami zprávy obsahující soubory fotografií a videonahrávek s tematikou dětské pornografie. Již z této skutečnosti jednoznačně vyplývá, že šlo o spáchání činu veřejně přístupnou počítačovou sítí. Ustanovení § 205 odst. 3 písm. b) tr. zák. postihuje takové způsoby šíření pornografie, které pachateli umožňují, aby s pornografickým dílem v krátkém čase seznámil velké množství osob; jeho formálním znakem však není zveřejnění díla ve smyslu jeho zpřístupnění komukoli. Znak "činí veřejně přístupným" je obsažen toliko v § 205 odst. 2 písm. a) tr. zák., a to alternativně jako jeden z řady dalších forem jednání, kterým může být uvedená skutková podstata naplněna. Nejvyšší státní zástupce vyslovil přesvědčení, že mimořádná účinnost elektronické komunikace, kterážto je do značné míry i anonymní, zřejmě vedla zákonodárce k tomu, aby šíření pornografických děl prostřednictvím veřejně přístupné počítačové sítě učinil přísněji trestným nežli "prosté" šíření pornografie. Poukázal také na judikaturu Nejvyššího soudu České republiky (ve věci sp. zn. 6 Tdo 1135/2010).

Nejvyšší státní zástupce namítl, že argumentace soudů obou stupňů, která se soustředila na skutečnost, že k pornografickým dílům měli přístup pouze jejich konkrétní adresáti, nikoli široký, předem nevymezený okruh osob, proto do značné míry není rozhodná z hlediska naplnění znaku spáchání činu prostřednictvím veřejně přístupné počítačové sítě. Argumentace soudů plně nepřihlíží k některým specifikům e-mailové komunikace. Rozdíl mezi e-mailovou komunikací, která je základním komunikačním prostředkem na Internetu, a komunikací formou klasické poštovní zásilky (dopisu, balíku) zasílané prostřednictvím veřejného přepravce konkrétnímu adresátovi spočívá nejen v tom, že e-mailové zprávy musí projít cizími počítači v síti před tím, než dosáhnou cílový počítač, což výrazně zjednodušuje možnost obsah zprávy zachytit a přečíst ji. Jde též o to, že naprostá většina providerů kopie všech e-mailových zpráv ukládá (zálohuje) na svoje servery před doručením a tyto zálohy často ponechává na serveru řadu měsíců po doručení zprávy, a to i v případě, že ve schránkách odesílatele i příjemce jsou již vymazány. Samotní uživatelé taktéž často ponechávají e-mailové zprávy uložené ve svých schránkách, což ostatně nepochybně činil i obviněný P. L., jehož trestná činnost spočívala m. j. v přechovávání 76 zpráv obsahujících pornografická díla. Zde k nim pak mohou získat přístup i jiné osoby než ty, kterým byly určeny. V této souvislosti nejvyšší státní zástupce poukázal na rozhodnutí Nejvyššího soudu ČR ve věci, sp. zn. 11 Tdo 349/2008, ze kterého vyplývá, že po doručení do e-mailové schránky již elektronická pošta nepožívá ochrany tajemství dopravovaných zpráv ve smyslu tehdy platného § 239 odst. 1 tr. zák.

S ohledem na uvedený právní názor se nejvyšší státní zástupce domnívá, že souzený skutek vylíčený ve výroku o vině měl být právně kvalifikován jako trestný čin šíření pornografie podle § 205 odst. 2 písm. a), odst. 3 písm. b) tr. zák.

V petitu svého dovolání nejvyšší státní zástupce navrhl, aby Nejvyšší soud podle § 265k odst. 1, odst. 2 tr. ř. zrušil napadený rozsudek Krajského soudu v Brně, pobočka v Jihlavě, jakož i všechna další rozhodnutí na toto rozhodnutí obsahově navazující, pokud v důsledku zrušení pozbyla podkladu. Dále navrhl, aby Nejvyšší soud podle § 265l odst. 1 tr. ř. věc přikázal odvolacímu soudu k novému projednání a rozhodnutí.

Opis dovolání nejvyššího státního zástupce byl za podmínek § 265h odst. 2 tr. ř. zaslán k vyjádření **obviněnému a jeho právnímu zástupci**, kteří jej shodně obdrželi dne 24. 3. 2011. Obviněný se vyjádřil v tom smyslu, že podané dovolání nepovažuje za důvodné. Právní úvahy soudů obou stupňů považuje za věcně správné, neboť zasílání e-mailových zpráv v omezeném počtu konkrétním adresátům nelze posuzovat jako veřejné zpřístupňování prostřednictvím počítačové sítě ve smyslu § 205 odst. 3 písm. b) tr. zák. E-mailová korespondence je zcela soukromá, určená vždy konkrétnímu adresátovi. Uživatel si e-mailovou schránku pořizuje s dobrou vírou v ochranu přepravovaných zpráv, přinejmenším v tom rozsahu, že se k obsahu žádný jiný uživatel nedostane. Útoky počítačových virů pak sice nelze vyloučit, nicméně takovou

eventualitu, pokud skutečně nastane, nelze klást za vinu běžnému uživateli.

Obviněný s ohledem na výše uvedené vyjádření navrhl, aby Nejvyšší soud dovolání nejvyššího státního zástupce jako nedůvodné zamítl.**III.Nejvyšší soud** jako soud dovolací nejdříve ověřil, že dovolání je *přípustné,* bylo podáno *oprávněnou osobou*, v *zákonné lhůtě* a na *předepsaném místě.*

Nejvyšší soud se proto dále zabýval otázkou opodstatněnosti dovolatelem uplatněných dovolacích důvodů.

Protože dovolání je možné učinit pouze z důvodů uvedených v § 265b tr. ř., bylo nutno posoudit, zda nejvyšším státním zástupcem vznesené námitky naplňují jím uplatněné zákonem stanovené dovolací důvody.

Důvod dovolání vymezený ustanovením § 265b odst. 1 písm. g) tr. ř. je dán tehdy, pokud rozhodnutí spočívá na nesprávném právním posouzení skutku nebo jiném nesprávném hmotně právním posouzení. V jeho mezích lze namítat mylnou právní kvalifikaci skutku - tedy otázku nesprávné právní kvalifikace a dále vadu jiného hmotně právního posouzení - která spočívá v nesprávném posouzení některé další otázky, s právní kvalifikací skutku přímo nesouvisející, ale významnou v posuzování jiné skutkové okolnosti, např. z hlediska hmotného práva trestního (popř. i jiného právního odvětví). Tento dovolací důvod tedy neumožňuje napadnout postup podle procesních předpisů, ale je zaměřen výlučně proti nesprávnému hmotně právnímu posouzení (viz usnesení Ústavního soudu ze dne 1. září 2004, sp. zn. II. ÚS 279/03).

Dovolatel daný dovolací důvod uplatnil s tím, že jím namítané nesprávné právní posouzení spočívá v tom, že Okresní soud ve Žďáru nad Sázavou posoudil souzený skutek pouze podle základní skutkové podstaty trestného činu šíření pornografie uvedené v ustanovení § 205 odst. 2 písm. a) tr. zák., a nepřihlédl k tomu, že čin byl spáchán veřejně přístupnou počítačovou sítí ve smyslu ustanovení § 205 odst. 3 písm. b) tr. zák. Stejnou vadou pak bylo zatíženo i napadené rozhodnutí odvolacího soudu, který k odvolání okresního státního zástupce sice rozhodnutí soudu prvního stupně částečně změnil, výrok o vině však ponechal beze změny.

Trestného činu šíření pornografie se v základní skutkové podstatě **podle § 205 odst. 2 písm. a) tr. zák.**se dopustí ten, kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě.

V kvalifikované skutkové podstatě **podle § 205 odst. 3 písm. b) tr. zák.** se tohoto trestného činu dopustí ten, kdo čin uvedený v odst. 2 spáchá tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem.

Pokud se týká dosavadního řízení, soud prvního stupně na rozdíl od podané obžaloby nekvalifikoval jednání obviněného P. L. jako spáchané v kvalifikované skutkové podstatě podle § 205 odst. 3 písm. b) tr. zák., tedy tak, že obviněný činy spáchal veřejně přístupnou počítačovou sítí. Dospěl k závěru, že znak "veřejně přístupnou počítačovou sítí" nebyl naplněn.

Odvolací soud pak v rámci přezkumu rozsudku nalézacího soudu dospěl k závěru, že nalézací soud v právní kvalifikaci skutku nijak nepochybil. Konstatoval, že e-mailové zprávy byly odesílány ze soukromé schránky obviněného P. L., kterážto byla chráněna heslem, do soukromých schránek konkrétních příjemců, které byly taktéž chráněny heslem, bez jehož znalosti nelze obsah e-mailové schránky zpřístupnit. Uvedl, že formu e-mailové korespondence je možné přirovnat ke korespondenci ve formě dopisu, který je určen konkrétnímu adresátovi. Ačkoli je tedy internet veřejně přístupnou počítačovou sítí, e-mailové zprávy a jejich obsah posílaný prostřednictvím internetu nejsou veřejně přístupné. Odvolací soud dále vyslovil názor, že předmětný skutek nelze považovat za čin spáchaný veřejně přístupnou počítačovou sítí, jak vyžaduje skutková podstata § 205 odst. 3 písm. b) tr. zák., a současně se ztotožnil s názorem nalézacího soudu v tom směru, že jako spáchané veřejně přístupnou počítačovou sítí by bylo možno posoudit jednání obviněného pouze tehdy, kdyby materiály umístil na webové stránky, které jsou běžně přípustné blíže neurčenému a neomezenému okruhu uživatelů internetu.

Při výkladu jednotlivých právních pojmů, jež citovaná ustanovení trestního zákona zmiňují, je především třeba vycházet z jejich vymezení. Je-li zmiňováno *dítě*, rozumí se, že jde o osobu mladší osmnácti let. *Pornografickým dílem*je jakýkoli předmět, který je-li pozorován ať přímo nebo prostřednictvím technického zařízení, zvláště intenzivním a vtíravým způsobem zasahuje a podněcuje samotný sexuální pud. Současně takové dílo podle převládajících názorů většiny členů společnosti hrubě porušuje uznávané morální normy dané společnosti a vyvolává v nich pocit studu. Pro pornografický charakter je rozhodující obsah celého díla, nikoli jen jeho určitá část, výseč, kapitola nebo úryvek apod.

Pod pojmem *uvádí do oběhu*se rozumí jednání pachatele, kterým se má předmět dostat postupně do rukou více lidí, ať již v originále, nebo v kopiích; nešlo by o oběh, pokud by se měl s pornografickým předmětem seznámit jen úzký okruh lidí, uzavřená společnost apod., avšak na druhé straně není třeba, aby se s ním skutečně širší okruh lidí seznámil, postačí pouhé uvádění do běhu, tedy počátek tohoto oběhu. Pod znakem *rozšiřování*je třeba chápat šíření zejména pomocí veřejných sdělovacích prostředků, tedy tiskem, rozhlasem, televizí, jakož i jakákoli jiná distribuce po živnostensku (srov. též Šámal, P., Púry, F., Rizman, S. Trestní zákon. Komentář. 4. vydání. Praha: C. H. Beck. 2001, str. 1228 - 1229).

*Veřejně přístupnou počítačovou sítí*se rozumí funkční propojení počítačů do sítí s cílem vytvořit informační systém pracující s tzv. dálkovým přístupem, jakým je především internet a jiné podobné informační systémy. Z technického hlediska je veřejně přístupná počítačová síť soustavou serverů, datových komunikací a k nim připojených počítačů. Z organizačního hlediska jde o provozovatele jednotlivých sítí a podsítí, zprostředkovatele připojení i uživatele a další subjekty. Internet jako světová informační počítačová síť vznikl propojováním původně privátních, specializovaných a autonomních datových sítí (vojenské, školní, energetické apod.) a později již veřejných takovýchto sítí (přístupných většinou za úplatu každému zájemci) s postupnou změnou jejich charakteru (přechod na jednotný protokol řízení přenosu Transmission Control

Protocol/Internet Protocol, budovaných na principu dobrovolných dohod atd.), včetně užívání zdarma. Rozhodujícím okamžikem byl vznik služby WWW (World Wide Web), která byla vytvořena v internetu na bázi počítačových serverů (části Internetu) ukazujících jeden k druhému s využitím tzv. hypertextových odkazů, podpory multimédií a integrování různých služeb. Veřejně přístupnou počítačovou sítí výslovně nejsou pouze uzavřené počítačové sítě některých právnických osob, státních orgánů nebo jiné organizace, které nesplňují podmínku veřejné přístupnosti (srov. též Šámal, P., Púry, F., Rizman, S. Trestní zákon. Komentář. 4. vydání. Praha: C. H. Beck. 2001, str. 1231 - 1232).

Z hlediska zachovávání dopravovaných e-mailových zpráv lze říci, že naprostá většina providerů kopie všech e-mailových zpráv ukládá na svoje servery před jejich doručením a tyto zálohy následně ponechává na serveru, a to často po dobu i více měsíců po samotném doručení zprávy, a to i v případech, že tyto zprávy jsou již ve schránkách odesílatele i příjemce vymazány. Ochrana dopravované e-mailové zprávě je tak poskytována v době jejího "podávání", tedy v průběhu doručování. Konec tohoto procesu je nutno vnímat v okamžiku doručení do e-mailové schránky příjemce. Do schránky má příjemce zprávy přístup, který je zabezpečen pomocí hesla, může se přitom do schránky dostat z kteréhokoli počítače připojeného k Internetu (srov. také usnesení NS ČR ze dne 21. 5. 2009, sp. zn. 11 Tdo 349/2009). V této souvislosti nelze pominout i problém virů, tj. krátkých počítačových programů určených k provedení úkonů nad rámec vůle uživatele, které mohou mít kromě vlivu na narušení nebo likvidaci instalovaných programů, také vliv i na odesílání uložených dat a programů uživatele bez jeho výslovného pokynu (srov. rozsudek Nejvyššího soudu ze dne 27. 1. 2011, sp. zn. 4 Tz 79/2010).

Lze souhlasit s nejvyšším státním zástupcem v tom, že e-mailová komunikace umožňuje, aby pachatel neporovnatelně jednodušším a rychlejším způsobem nežli v případě šíření pornografických děl v hmotné podobě, např. cestou "klasické" poštovní zásilky, rozesílal elektronická pornografická díla velkému počtu subjektů; pouhou manipulací na počítači lze takováto díla v minimálním časovém úseku dopravit na prakticky neomezenou vzdálenost, kdy jde současně o komunikaci do značné míry anonymní, když pachateli postačuje znalost e-mailové adresy a nemusí znát fyzickou totožnost příjemce.

S ohledem na výše uvedené je zaslání pornografického díla elektronickou poštou uvedením do oběhu prostřednictvím veřejně přístupné počítačové sítě a toto jednání podle právní úpravy platné do 31. 12. 2009 naplňovalo skutkovou podstatu trestného činu šíření pornografie podle § 205 odst. 2 písm. a), odst. 3 písm. b) tr. zák.

Nejvyšší soud však má za to, že v projednávaném případě nebyl znak "veřejně přístupnou počítačovou sítí" naplněn. Přestože obviněný využil k šíření pornografických děl e-mailových zpráv zasílaných prostřednictvím sítě internet, z povahy těchto zpráv vyplývá, že k jejich obsahu si mohou legálně zjednat přístup pouze odesílatel a příjemce, popřípadě snad omezený okruh osob činných pro poskytovatele připojení, resp. že k pornografickým dílům měli přístup toliko konkrétní adresáti e-mailových zpráv, nikoli široký, předem nevymezený okruh osob, jak by tomu bylo v případě, že byl skutek spáchán např. televizí, filmem nebo vystavením takového pornografického díla na veřejně přístupných stránkách internetu. Obviněný tak využil k šíření pornografických děl veřejně přístupnou počítačovou síť ovšem způsobem nikoli veřejně přístupným.

Nad rámec výše uvedeného je potřeba zmínit, že trestného činu šíření pornografie podle § 205 odst. 3 písm. b) tr. zák. se dopustí ten, kdo takový čin spáchá tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo

jiným obdobně účinným způsobem

.

Za jiný obdobně účinný způsob jako je tisk, rozhlas, televize nebo veřejně přístupná počítačová síť, se považuje taková forma přenosu nebo jiného předání určité písemné, zvukové nebo hlasové informace, jestliže je zpřístupněna většímu počtu příjemců, tedy veřejnosti ve formě blíže neurčitého počtu lidí, přičemž nezávisí na tom, zda přístup veřejnosti je zcela volný, nebo je omezen např. zaplacením určitých poplatků, tzv. klubovou příslušností apod. Dále sem lze zařadit i místní rozhlas, vysílací stanici apod. (viz Šámal, P., Púry, F., Rizman, S. Trestní zákon. Komentář. II. díl. 6., doplněné a přepracované vydání. Praha: C. H. Beck, 2004, s. 1232).

Pokud se za znak jiného obdobně účinného způsobu považuje např. nahrávka na gramofonové desce, magnetofonovém pásku, magnetofonové kazetě, t. j. druh záznamové techniky, pak je nutné zvažovat, zda mezi ně nelze zahrnout i počítačové soubory (vytvořené, zachycené, nebo jinak získané) do e-mailové adresy a jejím prostřednictvím předávané, když stejně jako u osobně vytvořeného záznamu na magnetofonovém pásku jde i u počítačového souboru v e-mailové adrese o záznamy, které se vytvářejí soukromě a informace na nich uložená, pokud není nabízena, přenechávána nebo zpřístupňována osobě mladší osmnácti let [§ 205 odst. 2 písm. a) tr. zák.], nepožívá ochrany trestního zákona. Teprve tehdy, je-li nabízena, přenechávána nebo zpřístupňována osobě mladší osmnácti let, se stává trestnou. Stejná situace jako u předání předmětné informace většímu počtu příjemců např. přehráním filmu nebo videozáznamu apod. nastane, jestliže se počítačové soubory rozešlou prostřednictvím e-mailové pošty **většímu počtu e-mailových adresátů**. V takové situaci by bylo možno i elektronickou poštu považovat za okolnost naplňující znak jiného obdobně účinného způsobu ve smyslu § 205 odst. 3 písm. b) tr. zák.

V projednávaném případě se však obviněný trestné činnosti dopustil tím, že "***v pěti případech**, odeslal na e-mailové adresy užívané dosud neznámými osobami, a to dne 27. 6. 2008 v 18.26 hodin a 18.31 hodin na e-mailovou adresu, dne 10. 1. 2009 v 11.12 hodin na e-mailovou adresu dne 14. 1. 2009 v 11.45 hodin na e-mailovou adresu a dne 3. 3. 2009 na e-mailovou adresu*". Zde je třeba poukázat na to, že se jednalo pouze **o pět** prokázaných případů přeposlání e-mailové zprávy, kdy adresáti těchto zpráv nebyli identifikováni, resp. totožnost osob, jimž byly zprávy určeny, nebyla zjištěna. Přestože by bylo možno hovořit o tom, že v obecné rovině jednání obviněného znaky skutkové podstaty podle § 205 odst. 3 písm. b) tr. zák. naplňuje, s ohledem na počet e-mailových adres, na které byly zprávy zasílány, nelze dospět k

závěru, že jeho jednání současně vykazuje takovou hromadnou účinnost, jakou má na mysli ustanovení § 205 odst. 3 písm. b) tr. zák.

V projednávaném případě nelze dospět k závěru, že by počítačové soubory byly rozeslány prostřednictvím e-mailové pošty **většímu počtu e-mailových adresátů.** S ohledem na rozsah spáchané činnosti tak nebyla naplněna podmínka pro přísnější právní kvalifikaci dle kvalifikované skutkové podstaty podle § 205 odst. 3 písm. b) tr. zák.

S ohledem na skutečnosti rozvedené v předcházejících odstavcích Nejvyšší soud neshledal, že by napadené rozhodnutí odvolacího soudu bylo zatíženo vytýkanými vadami.

IV.

Podle § 265i odst. 1 písm. e) tr. ř. **Nejvyšší soud dovolání odmítne**, jde-li o dovolání zjevně neopodstatněné. S ohledem na shora stručně (§ 265i odst. 2 tr. ř.) uvedené důvody Nejvyšší soud v souladu s citovaným ustanovením zákona dovolání obviněného P. L. odmítl. Za podmínek § 265r odst. 1 písm. a) tr. ř. učinil toto rozhodnutí v neveřejném zasedání.

Poučení:

Proti rozhodnutí o dovolání není s výjimkou obnovy řízení opravný prostředek přípustný (§ 265n tr. ř.).

V Brně dne 4. května 2011

Předseda senátu:

JUDr. Petr Šabata

3 Tdo 669/2011-17

K výkladu znaku jiným obdobně účinným způsobem u trestného šíření pornografie

Znak „jiným obdobně účinným způsobem“ obsažený ve skutkové podstatě trestného činu šíření pornografie podle § 205 odst. 3 písm. b) TZ [ve znění účinném do 31. 12. 2009, od 1. 1. 2010 přečin šíření pornografie podle § 191 odst. 3 písm. b) TZ] je srovnatelný se znakem šíření tiskem, filmem, rozhlasem, televizí a veřejně přístupnou počítačovou sítí uvedeným v citovaném ustanovení. Přitom se musí jednat o takové množství případů, kdy se předávaný závadný obsah (např. prostřednictvím e-mailové pošty) dostane k většímu množství konečných příjemců.

USNESENÍ

Nejvyšší soud

České republiky rozhodl v neveřejném zasedání konaném dne 1. června 2011 o dovolání nejvyššího státního zástupce podaném v neprospěch obviněného A. Š. , proti usnesení Krajského soudu v Brně ze dne 19. 1. 2011, sp. zn. 5 To 10/2011, jako soudu odvolacího v trestní věci vedené u Okresního soudu v Břeclavi pod sp. zn. 21 T 178/2010, takto:

Podle § 265i odst. 1 písm. e) tr. ř. se dovolání nejvyššího státního zástupce odmítá.

Odůvodnění:

I.**Rozsudkem Okresního soudu v Břeclavi ze dne 23. 11. 2010, sp. zn. 21 T 178/2010**, byl obviněný A. Š. uznán vinným trestným činem šíření pornografie podle § 205 odst. 2 písm. a) zákona č. 140/1961 Sb., trestního zákona, účinného do 31. 12. 2009 (dále jen "tr. zák."), a trestným činem přechovávání dětské pornografie podle § 205a tr. zák., jichž se dopustil tím, že:

1. "*v období od 17. 10. 2008 nejméně do 9. 3. 2009 v místě svého trvalého bydliště v B., jakožto uživatel e-mailové schránky s názvem po zadání hesla opakovaně přistupoval prostřednictvím sítě internet z IP adres dynamicky přidělovaných společností T-Mobile Czech Republic, a. s., jako mobilní připojení k tel. č. obžalovaného do této e-mailové schránky a prostřednictvím internetu odeslal dalším adresátům z této e-mailové schránky 32 elektronických zpráv obsahujících obrazové soubory a videosoubory s tzv. dětskou pornografií, tedy obrazové soubory a videosoubory zobrazující obnažené dívky a chlapce zjevně mladší 18 let situované v polohách vyzývavě předvádějících obnažené pohlavní orgány za účelem sexuálního uspokojení, dále pak snímky dívek a chlapců zjevně mladších 18 let zachycujících je v polohách skutečného či předstíraného sexuálního styku s nimi a jiné obdobně sexuálně dráždivé snímky dětí mladších 18 let, čehož si byl plně vědom;*

2. od přesně nezjistitelného data nejméně však od 17. 10. 2008 do 14. 10. 2009 v místě svého trvalého bydliště v B., prostřednictvím sítě internet přistupoval z IP adres dynamicky přidělovaných společností T-Mobile Czech Republic, a. s., jako mobilní připojení k tel. č. obžalovaného, do e-mailové schránky s názvem, v níž k datu 9. 3. 2009 přechovával celkem 39 e-mailových zpráv obsahujících obrazové soubory a videosoubory s tzv. dětskou pornografií, tedy obrazové soubory a videosoubory zobrazující obnažené dívky a chlapce zjevně mladší 18 let situované v polohách vyzývavě předvádějících obnažené pohlavní orgány za účelem sexuálního uspokojení, dále pak snímky dívek a chlapců zjevně mladších 18 let zachycujících je v polohách skutečného či předstíraného sexuálního styku s nimi a jiné obdobně sexuálně dráždivé snímky dětí mladších 18 let, přičemž dne 14. 10. 2009 byla při domovní prohlídce zajištěna výpočetní technika a přenosné nosiče dat CD/DVD, patřící obžalovanému, kdy odborným zkoumáním bylo zjištěno, že v době nejméně od 1. 12. 2007 do 14. 10. 2009 na pevných discích všech počítačů a na 15 ks CD-R a DVD-R přechovával značné množství (řádově tisíce) obrazových a videosouborů s tématikou tzv. dětské pornografie, čehož si byl plně vědom".

Za to byl obviněný odsouzen podle § 205 odst. 2 za použití § 35 odst. 1 tr. zák. k úhrnnému trestu odnětí svobody v trvání 2 (dvou) let, jehož výkon byl podle § 58 odst. 1 tr. zák. a § 59 odst. 1 tr. zák. podmíněně odložen na zkušební dobu v trvání 4 (čtyř) let. Současně byl obviněnému uložen trest propadnutí věci nebo jiné majetkové hodnoty, a to 15 ks CD/DVD tvořících přílohu spisu, 1 ks paměťové karty zn. FujiFilm 1 GB, 1 ks osobního počítače zn. HP, černé barvy, 1 ks osobního počítače zn. ALI VO, šedé barvy, 1 ks osobního počítače zn. CELERON, šedé barvy, 1 ks notebook zn. ACER, s příslušenstvím.

Okresní soud dále obviněného A. Š. a P. Š., dříve S., podle § 226 písm. a) tr. ř. zprostil v bodě 3) obžaloby

Okresního státního zastupitelství v Břeclavi ze dne 26. 10. 2010, sp. zn. ZT 307/2010, pro skutek, že "*v době od 26. 7. 2009 do 9. 8. 2009 v době dovolené v P., v B. pořizovali na hotelovém pokoji, kde byli ubytováni, vzájemně své fotografie v erotických a pornografických polohách, které zachycovaly jejich obnažené intimní partie, přičemž tomuto fotografování byl přítomen syn obžalované P. Š., dříve S., která je manželkou, dříve družkou obžalovaného A. Š., nezletilý, žijící spolu s obžalovanými ve společné domácnosti, který je taktéž na těchto fotografiích zachycen zcela svlečený, jak zcela evidentně fotografování sleduje, a dále se oba obžalovaní nechali od nezletilého fotografovat na nudistické pláži v takových pózách, že tyto fotografie lze označit za pornografické, tedy v pózách zobrazujících vyzývavým způsobem jejich intimní partie*", čímž měli spáchat trestný čin ohrožování výchovy mládeže podle § 217 odst. 1 písm. a) tr. zák. účinného do 31. 12. 2009, neboť nebylo prokázáno, že se stal skutek, pro nějž byli obvinění A. Š. a P. Š., dříve S., stíháni.

Okresní soud v Břeclavi plně převzal skutková tvrzení z obžaloby státního zástupce Okresního státního zastupitelství v Břeclavi ze dne 22. 10. 2010, sp. zn. ZT 307/2010, neakceptoval však státním zástupcem navrhovanou právní kvalifikaci, pokud státní zástupce požadoval, aby byl obviněný A. Š. uznán vinným trestným činem šíření pornografie spáchaným v kvalifikované skutkové podstatě podle § 205 odst. 2 písm. a), odst. 3 písm. b) tr. zák., tedy, že se činu dopustil veřejně přístupnou počítačovou sítí.

Proti rozsudku Okresního soudu v Břeclavi podal státní zástupce Okresního státního zastupitelství v Břeclavi v neprospěch obviněného odvolání (č. l. 310 - 311), které zaměřil do výroků o vině i o trestu. Státní zástupce v odvolání uvedl, že trvá na tom, aby byl skutek právně posouzen jako trestný čin šíření pornografie spáchaný v kvalifikované skutkové podstatě podle § 205 odst. 2 písm. a), odst. 3 písm. b) tr. zák., neboť obviněný A. Š. se svého jednání dopustil veřejně přístupnou počítačovou sítí.

Krajský soud v Brněo podaném odvolání rozhodl **rozsudkem ze dne 19. 1. 2011, sp. zn. 5 To 10/2011**, a to tak, že odvolání státního zástupce podle § 256 tr. ř. zamítl.

II.

Proti usnesení krajského soudu podal **nejvyšší státní zástupce** *dovolání v neprospěch obviněného,* a to z důvodu uvedeného v **§ 265b odst. 1 písm. g) tr. ř.,** neboť má za to, že napadené rozhodnutí spočívá na nesprávném právním posouzení skutku.

Poté, co nejvyšší státní zástupce zrekapituloval dosavadní průběh řízení a argumenty soudů obou stupňů, kteréžto vedly k výroku o vině obviněného, uvedl, že nelze souhlasit se závěry soudů obou stupňů, podle kterých nebyl naplněn znak spáchání činu "veřejně přístupnou počítačovou sítí", čímž by byla naplněna skutková podstata trestného činu šíření pornografie spáchaného v kvalifikované skutkové podstatě podle § 205 odst. 2 písm. a), odst. 3 písm. b) tr. zák. Uvedl, že veřejně přístupnou počítačovou sítí se rozumí funkční propojení počítačů do sítí s cílem vytvořit informační systém pracující s tzv. dálkovým přístupem. Veřejně přístupnou počítačovou sítí je především Internet jako světová informační počítačová síť a jiné podobné informační systémy. Namítl, že dle vymezení skutku ve výroku o vině vyplývá, že obviněný A. Š. nejméně v 32 případech odeslal na e-mailové adresy zprávy obsahující soubory fotografií a videonahrávek s tematikou dětské pornografie. Již z této skutečnosti jednoznačně vyplývá, že šlo o spáchání činu veřejně přístupnou počítačovou sítí. Nejvyšší státní zástupce namítl, že argumentace soudů obou stupňů, která se soustředila na skutečnost, že k pornografickým dílům měli přístup pouze jejich konkrétní adresáti, nikoli široký, předem nevymezený okruh osob, proto do značné míry není rozhodná z hlediska naplnění znaku spáchání činu prostřednictvím veřejně přístupné počítačové sítě. Rozdíl mezi dřívějším komunikačním prostředkem cestou klasického dopisu, svěřeného k přepravě veřejnému přepravci od odesílatele k adresátovi, spočívá v tom, že e-mailové zprávy musí projít cizími počítači v síti předtím, než dosáhnou cílový počítač. Takový způsob distribuce zpráv jejich adresátům však výrazně napomáhá snadné možnosti obsah zprávy zachytit a přečíst. V naprosté většině případů jsou kopie e-mailových zpráv zálohovány na serverech před doručením a tyto zálohy často bývají na serveru řadu měsíců ponechávány i po doručení zprávy, a to i v případě, že ve schránkách odesílatele i příjemce jsou již vymazány. V tomto směru pak nelze pominout ani problém virů, kdy se v podstatě jedná o krátké počítačové programy, určené k provedení úkonů nad rámec vůle uživatele, přičemž nepůsobí pouze tak, že mohou narušovat instalované programy, nebo je likvidovat, ale mohou být naprogramovány též tak, že bez vědomí uživatele odesílají z jeho počítače uložená data a dokumenty.

S ohledem na uvedený právní názor se nejvyšší státní zástupce domnívá, že souzený skutek vylíčený ve výroku o vině měl být právně kvalifikován jako trestný čin šíření pornografie podle § 205 odst. 2 písm. a), odst. 3 písm. b) tr. zák.

V petitu svého dovolání nejvyšší státní zástupce navrhl, aby Nejvyšší soud podle § 265k odst. 1, odst. 2 tr. ř. zrušil napadené usnesení Krajského soudu v Brně ze dne 19. 1. 2011, sp. zn. 5 To 10/2011, jakož i všechna další rozhodnutí na toto rozhodnutí obsahově navazující, pokud v důsledku zrušení pozbyla podkladu. Dále navrhl, aby Nejvyšší soud podle § 265l odst. 1 tr. ř. věc přikázal odvolacímu soudu k novému projednání a rozhodnutí.

Opis dovolání nejvyššího státního zástupce byl za podmínek § 265h odst. 2 tr. ř. zaslán k vyjádření **obviněnému a jeho právnímu zástupci**, kteří jej shodně obdrželi dne 4. 5. 2011. Obviněný se vyjádřil v tom smyslu, že podané dovolání nepovažuje za důvodné. Právní úvahy soudů obou stupňů považuje za věcně správné, neboť přenos závadového obsahu elektronické pošty prostřednictvím šifrovaných paketů z jedné IP adresy, navíc chráněné přístupovým heslem, na druhou IP adresu, rovněž chráněnou jiným heslem, nelze v žádném případě považovat za veřejně přístupný způsob přepravy, k němuž by měl přístup jakýkoli jiný účastník internetové sítě. Je přesvědčen, že pokud nejvyšší státní zástupce nesprávně zdůvodňuje své dovolání tvrzením, že veřejně přístupnou počítačovou sítí se rozumí pouze propojení vzdálených PC do sítě k dálkovému přístupu, tedy sítí internetu, pak se zabývá pouze povrchně existencí takové sítě, avšak již naprosto opomíjí technická opatření, zajišťující znemožnění přístupu jiného, anonymního uživatele, k obsahu přenášených paketů.

Obviněný s ohledem na výše uvedené vyjádření navrhl, aby Nejvyšší soud dovolání nejvyššího státního zástupce

jako nedůvodné zamítl.

III.Nejvyšší soud jako soud dovolací nejdříve ověřil, že dovolání je *přípustné,* bylo podáno *oprávněnou osobou*, v *zákonné lhůtě* a na *předepsaném místě.*

Nejvyšší soud se proto dále zabýval otázkou opodstatněnosti dovolatelem uplatněných dovolacích důvodů.

Protože dovolání je možné učinit pouze z důvodů uvedených v § 265b tr. ř., bylo nutno posoudit, zda nejvyšším státním zástupcem vznesené námitky naplňují jím uplatněné zákonem stanovené dovolací důvody.

Důvod dovolání vymezený ustanovením § 265b odst. 1 písm. g) tr. ř. je dán tehdy, pokud rozhodnutí spočívá na nesprávném právním posouzení skutku nebo jiném nesprávném hmotně právním posouzení. V jeho mezích lze namítat mylnou právní kvalifikaci skutku - tedy otázku nesprávné právní kvalifikace a dále vadu jiného hmotně právního posouzení - která spočívá v nesprávném posouzení některé další otázky, s právní kvalifikací skutku přímo nesouvisející, ale významnou v posuzování jiné skutkové okolnosti, např. z hlediska hmotného práva trestního (popř. i jiného právního odvětví). Tento dovolací důvod tedy neumožňuje napadnout postup podle procesních předpisů, ale je zaměřen výlučně proti nesprávnému hmotně právnímu posouzení (viz usnesení Ústavního soudu ze dne 1. září 2004, sp. zn. II. ÚS 279/03).

Dovolatel daný dovolací důvod uplatnil s tím, že jím namítané nesprávné právní posouzení spočívá v tom, že Okresní soud v Břeclavi posoudil souzený skutek pouze podle základní skutkové podstaty trestného činu šíření pornografie uvedené v ustanovení § 205 odst. 2 písm. a) tr. zák., a nepřihlédl k tomu, že čin byl spáchán veřejně přístupnou počítačovou sítí ve smyslu ustanovení § 205 odst. 3 písm. b) tr. zák. Stejnou vadou pak bylo zatíženo i napadené rozhodnutí odvolacího soudu, který odvolání okresního státního zástupce jako nedůvodné zamítl.

Trestného činu šíření pornografie se v základní skutkové podstatě **podle § 205 odst. 2 písm. a) tr. zák.**dopustí ten, kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě.

V kvalifikované skutkové podstatě **podle § 205 odst. 3 písm. b) tr. zák.** se tohoto trestného činu dopustí ten, kdo čin uvedený v odst. 2 spáchá tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem.

Pokud se týká dosavadního řízení, soud prvního stupně na rozdíl od podané obžaloby nekvalifikoval jednání obviněného A. Š. jako spáchané v kvalifikované skutkové podstatě podle § 205 odst. 3 písm. b) tr. zák., tedy tak, že obviněný činy spáchal veřejně přístupnou počítačovou sítí. Dospěl k závěru, že znak "veřejně přístupnou počítačovou sítí" nebyl naplněn.

Odvolací soud pak v rámci přezkumu rozsudku nalézacího soudu dospěl k závěru, že nalézací soud v právní kvalifikaci skutku nijak nepochybil a odkázal na odůvodnění nalézacího soudu s tím, že je nadbytečné jej znovu opakovat. Nalézací soud konstatoval, že posílání e-mailů není zpřístupňování veřejně přístupnou počítačovou sítí ve smyslu citovaného ustanovení, když každá e-mailová schránka je především chráněna jedinečným heslem a samotné e-maily jsou uchovávány včetně příloh na serverech, ke kterým nemají neoprávněné osoby přístup. E-mailová komunikace tak probíhá mezi subjekty, které mají předmětnou e-mailovou adresu, jinak daný typ komunikace možný není. "*Tato adresa je chráněna heslem, které si každý uživatel volí dle svého uvážení. Je pravdou, že e-mailová zpráva prochází cizími počítači předtím, než dosáhne počítač cílový, nicméně pouze z této skutečnosti dovodit, že e-mailová zpráva by měla představovat formu jakési veřejné komunikace, tj. komunikace, jež není vymezena konkrétními předem určenými subjekty, je dle názoru soudu naprosto zcestná, a to již vzhledem k úvahám soudu týkající se naplnění subjektivní stránky trestného činu*" (str. 5 rozsudku soudu prvního stupně). Postavil se tak na stanovisko, že obviněný poslal závadové e-maily s dětskou pornografií prostřednictvím internetu, který sice má povahu veřejně přístupné sítě, ale že e-mailové zprávy, takto prostřednictvím internetu posílané a tím ani jejich obsah, nejsou v daném případě veřejně přístupné. Soud uvedl, že pokud obviněný "*posílal zprávy do jednotlivých individualizovaných e-mailových schránek, nelze tento jeho čin srovnávat s tím, jakoby byl spáchán tiskem, filmem, rozhlasem, televizí nebo obdobně účinným způsobem*" (str. 6 rozsudku soudu prvního stupně). Jako spáchané veřejně přístupnou počítačovou sítí by bylo možno posoudit jednání obviněného pouze tehdy, kdyby materiály umístil na webové stránky, které jsou běžně přípustné blíže neurčenému a neomezenému okruhu uživatelů internetu.

Při výkladu jednotlivých právních pojmů, jež citovaná ustanovení trestního zákona zmiňují, je především třeba vycházet z jejich vymezení. Je-li zmiňováno *dítě*, rozumí se, že jde o osobu mladší osmnácti let. *Pornografickým dílem*je jakýkoli předmět, který je-li pozorován ať přímo nebo prostřednictvím technického zařízení, zvláště intenzivním a vtíravým způsobem zasahuje a podněcuje samotný sexuální pud. Současně takové dílo podle převládajících názorů většiny členů společnosti hrubě porušuje uznávané morální normy dané společnosti a vyvolává v nich pocit studu. Pro pornografický charakter je rozhodující obsah celého díla, nikoli jen jeho určitá část, výseč, kapitola nebo úryvek apod.

Pod pojmem *uvádí do oběhu*se rozumí jednání pachatele, kterým se má předmět dostat postupně do rukou více lidí, ať již v originále, nebo v kopiích; nešlo by o oběh, pokud by se měl s pornografickým předmětem seznámit jen úzký okruh lidí, uzavřená společnost apod., avšak na druhé straně není třeba, aby se s ním skutečně širší okruh lidí seznámil, postačí pouhé uvádění do běhu, tedy počátek tohoto oběhu. Pod znakem rozšiřování je třeba chápat šíření zejména pomocí veřejných sdělovacích prostředků, tedy tiskem, rozhlasem, televizí, jakož i jakákoli jiná distribuce po živnostensku (srov. též Šámal, P., Púry, F., Rizman, S. Trestní zákon. Komentář. 4. vydání. Praha: C. H. Beck. 2001, str. 1228 - 1229).

*Veřejně přístupnou počítačovou sítí*se rozumí funkční propojení počítačů do sítí s cílem vytvořit informační systém pracující s tzv. dálkovým přístupem, jakým je především internet a jiné podobné informační systémy. Z technického hlediska je veřejně přístupná počítačová síť soustavou serverů, datových komunikací a k nim připojených počítačů. Z organizačního

hlediska jde o provozovatele jednotlivých sítí a podsítí, zprostředkovatele připojení i uživatele a další subjekty. Internet jako světová informační počítačová síť vznikl propojováním původně privátních, specializovaných a autonomních datových sítí (vojenské, školní, energetické apod.) a později již veřejných takovýchto sítí (přístupných většinou za úplatu každému zájemci) s postupnou změnou jejich charakteru (přechod na jednotný protokol řízení přenosu Transmission Control Protocol/Internet Protocol, budovaných na principu dobrovolných dohod atd.), včetně užívání zdarma. Rozhodujícím okamžikem byl vznik služby WWW (World Wide Web), která byla vytvořena v internetu na bázi počítačových serverů (části Internetu) ukazujících jeden k druhému s využitím tzv. hypertextových odkazů, podpory multimedií a integrování různých služeb. Veřejně přístupnou počítačovou sítí výslovně nejsou pouze uzavřené počítačové sítě některých právnických osob, státních orgánů nebo jiné organizace, které nesplňují podmínku veřejné přístupnosti (srov. též Šámal, P., Púry, F., Rizman, S. Trestní zákon. Komentář. 4. vydání. Praha: C. H. Beck. 2001, str. 1231 - 1232).

Z hlediska zachovávání dopravovaných e-mailových zpráv lze říci, že naprostá většina providerů kopie všech e-mailových zpráv ukládá na svoje servery před jejich doručením a tyto zálohy následně ponechává na serveru, a to často po dobu i více měsíců po samotném doručení zprávy, a to i v případech, že tyto zprávy jsou již ve schránkách odesílatele i příjemce vymazány. Ochrana dopravované e-mailové zprávě je tak poskytována v době jejího "podávání", tedy v průběhu doručování. Konec tohoto procesu je nutno vnímat v okamžiku doručení do e-mailové schránky příjemce. Do schránky má příjemce zprávy přístup, který je zabezpečen pomocí hesla, může se přitom do schránky dostat z kteréhokoli počítače připojeného k Internetu (srov. také usnesení NS ČR ze dne 21. 5. 2009, sp. zn. 11 Tdo 349/2009).

Lze souhlasit s nejvyšším státním zástupcem v tom, že e-mailová komunikace umožňuje, aby pachatel neporovnatelně jednodušším a rychlejším způsobem nežli v případě šíření pornografických děl v hmotné podobě, např. cestou "klasické" poštovní zásilky, rozesílal elektronická pornografická díla velkému počtu subjektů; pouhou manipulací na počítači lze takováto díla v minimálním časovém úseku dopravit na prakticky neomezenou vzdálenost, kdy jde současně o komunikaci do značné míry anonymní, když pachateli postačuje znalost e-mailové adresy a nemusí znát fyzickou totožnost příjemce.

S ohledem na výše uvedené je zaslání pornografického díla elektronickou poštou uvedením do oběhu prostřednictvím veřejně přístupné počítačové sítě a toto jednání podle právní úpravy platné do 31. 12. 2009 naplňovalo skutkovou podstatu trestného činu šíření pornografie podle § 205 odst. 2 písm. a), odst. 3 písm. b) tr. zák.

Nejvyšší soud však má za to, že v projednávaném případě nebyl znak "veřejně přístupnou počítačovou sítí" naplněn. Přestože obviněný využil k šíření pornografických děl e-mailových zpráv zasílaných prostřednictvím sítě internet, z povahy těchto zpráv vyplývá, že k jejich obsahu si mohou legálně zjednat přístup pouze odesílatel a příjemce, popřípadě snad omezený okruh osob činných pro poskytovatele připojení, resp. že k pornografickým dílům měli přístup toliko konkrétní adresáti e-mailových zpráv, nikoli široký, předem nevymezený okruh osob, jak by tomu bylo v případě, že byl skutek spáchán např. televizí, filmem nebo vystavením takového pornografického díla na veřejně přístupných stránkách internetu. Obviněný tak využil k šíření pornografických děl veřejně přístupnou počítačovou síť ovšem způsobem nikoli veřejně přístupným.

Nad rámec výše uvedeného je potřeba zmínit, že trestného činu šíření pornografie podle § 205 odst. 3 písm. b) tr. zák. se dopustí ten, kdo takový čin spáchá tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo

jiným obdobně účinným způsobem

.

Za jiný obdobně účinný způsob jako je tisk, rozhlas, televize nebo veřejně přístupná počítačová síť, se považuje taková forma přenosu nebo jiného předání určité písemné, zvukové nebo hlasové informace, jestliže je zpřístupněna většímu počtu příjemců, tedy veřejnosti ve formě blíže neurčitého počtu lidí, přičemž nezávisí na tom, zda přístup veřejnosti je zcela volný, nebo je omezen např. zaplacením určitých poplatků, tzv. klubovou příslušností apod. Dále sem lze zařadit i místní rozhlas, vysílací stanici apod. (viz Šámal, P., Púry, F., Rizman, S. Trestní zákon. Komentář. II. díl. 6., doplněné a přepracované vydání. Praha: C. H. Beck, 2004, s. 1232).

Pokud se za znak jiného obdobně účinného způsobu považuje např. nahrávka na gramofonové desce, magnetofonovém pásku, magnetofonové kazetě, tj. druh záznamové techniky, pak je nutné zvažovat, zda mezi ně nelze zahrnout i počítačové soubory (vytvořené, zachycené, nebo jinak získané) do e-mailové adresy a jejím prostřednictvím předávané, když stejně jako u osobně vytvořeného záznamu na magnetofonovém pásku jde i u počítačového souboru v e-mailové adrese o záznamy, které se vytvářejí soukromě a informace na nich uložená, pokud není nabízena, přenechávána nebo zpřístupňována osobě mladší osmnácti let [§ 205 odst. 2 písm. a) tr. zák.], nepožívá ochrany trestního zákona. Teprve tehdy, je-li nabízena, přenechávána nebo zpřístupňována osobě mladší osmnácti let, se stává trestnou. Stejná situace jako u předání předmětné informace většímu počtu příjemců např. přehráním filmu nebo videozáznamu apod. nastane, jestliže se počítačové soubory rozešlou prostřednictvím e-mailové pošty **většímu počtu e-mailových adresátů**. V takové situaci by bylo možno i elektronickou poštu považovat za okolnost naplňující znak jiného obdobně účinného způsobu ve smyslu § 205 odst. 3 písm. b) tr. zák.

V projednávaném případě se však obviněný trestné činnosti dopustil tím, že "*prostřednictvím internetu odeslal dalším adresátům z této e-mailové schránky**32 elektronických zpráv** obsahujících obrazové soubory a videosoubory s tzv. dětskou pornografií*".

Ustanovení § 205 odst. 3 písm. b) tr. zák. stanovuje, že daného jednání je možno se dopustit

jiným obdobně účinným způsobem

, tedy obdobně účinným způsobem jako je šíření tiskem, filmem, rozhlasem, televizí a veřejně přístupnou počítačovou sítí. Hranice toho, co lze pod dané ustanovení podřadit je nejasná. Nejvyšší soud je však toho názoru, že se musí jednat o takové množství případů, kdy se předávaný obsah dostane k ekvivalentnímu množství konečných příjemců.

Zde je třeba poukázat na to, že se jednalo toliko **o 32** prokázaných případů přeposlání e-mailové zprávy, a to na 18 odlišných e-mailových adres (zpráva na č. l. 81 - 82). Přestože by bylo možno hovořit o tom, že v obecné rovině jednání obviněného znaky skutkové podstaty podle § 205 odst. 3 písm. b) tr. zák. naplňuje, s ohledem na počet e-mailových adres, na které byly zprávy zasílány nelze dospět k závěru, že jeho jednání současně vykazuje takovou hromadnou účinnost, jakou má na mysli ustanovení § 205 odst. 3 písm. b) tr. zák.

V projednávaném případě nelze dospět k závěru, že by počítačové soubory byly rozeslány prostřednictvím e-mailové pošty **většímu počtu e-mailových adresátů.** S ohledem na rozsah spáchané činnosti tak nebyla naplněna podmínka pro přísnější právní kvalifikaci dle kvalifikované skutkové podstaty podle § 205 odst. 3 písm. b) tr. zák.

S ohledem na skutečnosti rozvedené v předcházejících odstavcích Nejvyšší soud neshledal, že by napadené rozhodnutí odvolacího soudu bylo zatíženo vytýkanými vadami.

IV.

Podle § 265i odst. 1 písm. e) tr. ř. **Nejvyšší soud dovolání odmítne**, jde-li o dovolání zjevně neopodstatněné. S ohledem na shora stručně (§ 265i odst. 2 tr. ř.) uvedené důvody Nejvyšší soud v souladu s citovaným ustanovením zákona dovolání obviněného A. Š. odmítl. Za podmínek § 265r odst. 1 písm. a) tr. ř. učinil toto rozhodnutí v neveřejném zasedání.

Poučení:

Proti rozhodnutí o dovolání není s výjimkou obnovy řízení opravný prostředek přípustný (§ 265n tr. ř.).

V Brně dne 1. června 2010

Předseda senátu:

JUDr. Petr Šabata

7 Tdo 687/2011 - 21

K posouzení § 88 odst. 1 TZ (ve znění účinném do 31. 12. 2009) u trestného činu šíření pornografie, který pachatel spáchal odesláním závadových pornografických videosouborů

Trestný čin šíření pornografie obsahuje v ustanovení § 205 odst. 2 TZ (ve znění účinném do 31. 12. 2009, od 1. 1. 2010 přečin šíření pornografie podle § 191 odst. 2 TZ) různé formy opatření pornografického díla jinému. Forma opatření díla zde spočívá v jeho veřejném zpřístupnění a uvedení do oběhu a sama o sobě zahrnuje požadavek vyšší míry zveřejnění takového díla a tím i jeho zpřístupnění většímu počtu osob.

Za intenzivnější míru zpřístupnění díla lze pak považovat ty alternativy, které jsou obsaženy v § 205 odst. 3 písm. b) [ve znění účinném do 31. 12. 2009, od 1. 1. 2010 podle § 191 odst. 3 písm. b) TZ], tedy spáchání citovaného trestného činu tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí, nebo jiným obdobně účinným způsobem. Pro posouzení materiální podmínky podmiňující použití vyšší trestní sazby podle § 88 odst. 1 TZ (ve znění účinném do 31. 12. 2009) k citovanému ustanovení je třeba rovněž zvážit časový rozsah zasílaných závadových souborů.

Jestliže totiž film jako dílo zabírá svým rozsahem zpravidla několik desítek minut až hodin, pak k e-mailu připojené videosoubory (videoklipy) trvají obvykle několik vteřin či minut. Zpřístupnění díla formou připojeného videosouboru může být tedy svojí intenzitou srovnatelné se zpřístupněním díla filmem jen tehdy, pokud pachatel odeslal výrazně větší počet závadových pornografických videosouborů prostřednictvím veřejně přístupné počítačové sítě. V případě menšího počtu takto odeslaných videosouborů nelze dospět k závěru, že jednání pachatele spočívající v opatření pornografického díla jinému veřejně přístupnou počítačovou sítí podle § 205 odst. 3 písm. b) TZ [ve znění účinném do 31. 12. 2009, od 1. 1. 2010 podle § 191 odst. 3 písm. b) TZ], podstatně zvyšuje stupeň nebezpečnosti činu pro společnost ve smyslu ustanovení § 88 odst. 1 TZ (ve znění účinném do 31. 12. 2009).

USNESENÍ

Nejvyšší soud

České republiky rozhodl dne 13. července 2011 v neveřejném zasedání o dovolání nejvyššího státního zástupce v neprospěch obviněného V. B. proti usnesení Krajského soudu v Brně ze dne 3. 2. 2011, sp. zn. 7 To 11/2011, v trestní věci vedené u Okresního soudu v Břeclavi pod sp. zn. 21 T 167/2010, takto:

Podle § 265j tr. ř. sedovolání zamítá .

Odůvodnění:

Rozsudkem Okresního soudu v Břeclavi ze dne 18. 11. 2010, sp. zn. 21 T 167/2010, byl obviněný uznán vinným trestnými činy přechovávání dětské pornografie podle § 205a tr. zákona (ad 1. výroku o vině) a šíření pornografie podle § 205 odst. 2 písm. a), c), tr. zákona (ad 2. výroku o vině). Za tyto trestné činy byl odsouzen podle § 205 odst. 2 a § 35 odst. 1 tr. zákona k úhrnnému trestu odnětí svobody v trvání 12 měsíců, jehož výkon byl podle § 58 odst. 1 a § 59 odst. 1 tr. zákona podmíněně odložen na zkušební dobu v trvání 2 let. Podle § 55 odst. 1 písm. a) tr. zákona mu byl uložen také trest propadnutí věci (1 ks osobního počítače).

Proti rozsudku soudu I. stupně podal státní zástupce v neprospěch obviněného odvolání, které bylo usnesením Krajského soudu v Brně ze dne 3. 2. 2011, sp. zn. 7 To 11/2011, zamítnuto podle § 256 tr. ř. jako nedůvodné. Odvoláním se státní zástupce domáhal posouzení jednání obviněného v bodě 2) výroku o vině i podle odst. 3 písm. b) ustanovení § 205 tr.

zákona tj., že čin spáchal veřejně přístupnou počítačovou sítí.

Usnesení odvolacího soudu napadl nejvyšší státní zástupce řádně a včas podaným dovoláním v neprospěch obviněného, ve kterém uplatnil důvody dovolání podle § 265b odst. 1 písm. g) a l) tr. ř. Dovolání směřuje proti právnímu posouzení skutku v bodě 2. výroku o vině rozsudku soudu I. stupně, kterým podle soudů obou stupňů obviněný spáchal trestný čin šíření pornografie podle § 205 odst. 2 písm. a), c) tr. zákona. Podle názoru odvolatele mělo být jednání obviněného právně posouzeno i podle odst. 3 písm. b) tohoto zákonného ustanovení, tj. že čin spáchal veřejně přístupnou počítačovou sítí. Dovolatel uvedl, že veřejně přístupnou počítačovou sítí se rozumí funkční propojení počítačů do sítí s cílem vytvořit informační systém s tzv. dálkovým přístupem, jakým je především internet. Z technického hlediska je veřejně přístupná počítačová síť soustavou serverů, datových komunikací a k nim připojených počítačů. Takovou počítačovou sítí naopak není např. uzavřená počítačová síť některé právnické osoby, státního orgánu nebo jiné organizace, protože nesplňuje podmínku veřejné přístupnosti. Dovolatel poukázal s odkazem na odbornou literaturu (Trestní zákoník II., 1. vydání C. H. Beck), že za jiný obdobně účinný způsob jako je tisk, film, rozhlas, televize nebo veřejně přístupná počítačová síť se považuje např. nahrávka na gramofonové desce, počítačové disketě, magnetofonovém pásku nebo videokazetě, jestliže jsou zpřístupněny většímu počtu osob, tedy veřejnosti ve formě blíže neurčeného počtu lidí, přičemž nezáleží na tom, zda je přístup veřejnosti zcela volný, nebo je omezen zaplacením určitých poplatků, tzv. klubovou příslušností apod. Elektronická pošta, jako základní komunikační prostředek na internetu, je svou podstatou síťový e-mail a je tedy v obecném měřítku funkční v rámci celé internetové sítě, nikoliv pouze ve smyslu datové komunikační sítě s omezeným rozsahem tak, aby ji bylo možné označit nad uvedený rámec za uzavřenou. Elektronická pošta při své jednoduchosti a dostupnosti použití umožňuje s vysokou mírou rychlosti a efektivity zasílat zprávy s textem, fotografie, videosoubory apod. bez nutnosti ukládat jejich obsah na hmotný substrát a dále s ním nakládat způsobem odpovídajícím požadavkům klasické poštovní přepravy. Prostřednictvím elektronické pošty jsou tak některé zprávy způsobilé šířit se geometrickou řadou mezi obrovské množství adresátů, a to bez nutnosti znát jejich pravou identitu či kontaktní adresu. Absence potřeby znát pravé jméno či adresu adresáta byla využita i v tomto případě, kdy trestní stíhání obviněného bylo zahájeno na základě rozkrytí celé sítě uživatelů, kteří si navzájem zasílali zprávy se závadným obsahem, aniž by se museli osobně znát.

Přitom e-mailové zprávy musí před dosažením cílového počítače projít cizími počítači v síti, což napomáhá možnosti obsah zprávy zachytit a přečíst, navíc kopie e-mailových zpráv mohou být před doručením zálohovány na serverech i po doručení zprávy, a to i když ve schránkách odesílatele i příjemce jsou již vymazány a tyto kopie elektronických zpráv mohou být přístupné i jiným neurčeným osobám.

Proto nejvyšší státní zástupce považuje předávání zpráv elektronickou poštou za šíření zpráv veřejně přístupnou počítačovou sítí, když elektronická pošta umožňuje jednoduchou distribuci předmětného obsahu mezi členy e-mailově propojené skupiny, která navíc není zcela uzavřená, neboť obvykle je prostřednictvím některých svých členů napojena také na jiné skupiny. Poukázal také na rozhodnutí Nejvyššího soudu ČR (6 Tdo 1135/2010, 8 Tdo 1467/2010 a 4 Tz 79/2010), ze kterých vyplývá shodný právní závěr. V závěru dovolání proto navrhl, aby Nejvyšší soud zrušil napadené usnesení podle § 265k odst. 1, 2 tr. ř. a přikázal odvolacímu soudu, aby věc v potřebném rozsahu znovu projednal a rozhodl.

Obviněný v písemném vyjádření k dovolání vyjádřil nesouhlas s argumentací nejvyššího státního zástupce s tím, že přeposílal e-mailové soubory konkrétním adresátům do jejich soukromých chráněných schránek a odeslání 11 e-mailových zpráv nemá ani znaky masového šíření. Navrhl, aby bylo dovolání odmítnuto podle § 265i odst. 1 písm. e) tr. ř., nebo zamítnuto podle § 265j tr. ř. v neveřejném zasedání.

Nejvyšší soud zjistil, že námitky nejvyššího státního zástupce odpovídají uplatněnému dovolacímu důvodu dovolání podle § 265b odst. 1 písm. g) tr. ř., když směřují proti právnímu posouzení jednání obviněného v bodě 2) výroku o vině rozsudku soudu I. stupně. V tomto bodě byl obviněný uznán vinným trestným činem šíření pornografie podle § 205 odst. 2 písm. a), c) tr. zákona, a to za jednání spočívající ve své podstatě v tom, že v období nejméně od 27. 4. do 16. 5. 2009 ze své e-mailové schránky odeslal dalším adresátům celkem 11 e-mailových zpráv s připojenými obrazovými a videosoubory, na nichž byly zobrazovány svlečené děti zjevně mladší než 18 let, předvádějící své pohlavní orgány ve vyzývavých sexuálních pozicích, nebo provozující různé sexuální praktiky, nebo zobrazující sexuální styk dětí nebo s dětmi, a dále odeslal dalším adresátům celkem 7 e-mailových zpráv obsahujících připojené obrazové a videosoubory, znázorňující pohlavní styk se zvířaty.

Nejvyšší státní zástupce nesouhlasí s názorem soudů, že jednání obviněného spočívající v zasílání e-mailů s uvedenými připojenými soubory do e-mailových schránek individuálně přesně určeným subjektům, není spácháním činu veřejně přístupnou počítačovou sítí ve smyslu § 205 odst. 3 písm. b) tr. zákona.

Trestného činu šíření pornografie podle § 205 odst. 2 písm. a), c) tr. zákona se dopustí ten, kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě, a které zobrazuje nebo jinak znázorňuje pohlavní styk se zvířetem.

Pachatelem kvalifikované skutkové podstaty tohoto trestného činu podle § 205 odst. 3 písm. b) tr. zákona je ten, kdo čin uvedený v odstavci 2 spáchá tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem.

Námitky nejvyššího státního zástupce, kterými odůvodňuje názor, že obviněným zasílané soubory prostřednictvím elektronické pošty je nutno posoudit jako šíření veřejně přístupnou počítačovou sítí ve smyslu výše uvedeného ustanovení § 205 odst. 3 písm. b) tr. zákona, korespondující s názorem vysloveným Nejvyšším soudem již opakovaně v rozhodnutích sp. zn. 6 Tdo 1135/2010, 8 Tdo 1467/2010 a 4 Tz 79/2010, na která nejvyšší státní zástupce také přímo odkazuje. Ve všech uvedených trestních věcech se jednalo rovněž o pachatele, kteří na jiné e-mailové adresy odesílali (resp. přeposílali) e-maily obsahující dětskou pornografii a Nejvyšší soud toto jejich jednání, spočívající v zasílání pornografického díla elektronickou poštou, shodně považoval za uvedení do oběhu prostřednictvím veřejně přístupné počítačové sítě podle §

205 odst. 2 písm. a), resp. také písm. c), odst. 3 písm. b) tr. zákona účinného do 31. 12. 2009.

V souladu s dosavadní judikaturou Nejvyššího soudu je i v tomto případě shodného způsobu jednání obviněného V. B. zřejmé, že zasílání daného pornografického díla elektronickou poštou je formálně uvedením do oběhu prostřednictvím veřejně přístupné počítačové sítě podle § 205 odst. 3 písm. b) tr. zákona. Současně se ale jedná o okolnost, která podmiňuje použití vyšší trestní sazby, ke které se podle § 88 odst. 1 tr. zákona přihlédne jen tehdy, jestliže pro svou závažnost podstatně zvyšuje stupeň nebezpečnosti činu pro společnost.

Ve všech výše uvedených předchozích trestních věcech, ve kterých Nejvyšší soud shledal naplnění znaku "spáchání činu veřejně přístupnou počítačovou sítí", se jednalo o pachatele, kteří po dlouhou dobu odesílali e-mailové zprávy s daným obsahem velkému počtu jiných osob. Tak ve věci sp. zn. 8 Tdo 1467/2010 pachatel za dobu dva a půl roku odeslal různým adresátům 164 takových e-mailových zpráv, ve věci sp. zn. 4 Tz 79/2010 pachatel za dobu 10 měsíců přeposlal jiným adresátům 128 takových e-mailových zpráv a ve věci sp. zn. 6 Tdo 1135/2010 pachatel po dobu 14 měsíců až ze čtyř e-mailových schránek přeposílal takové e-mailové zprávy nezjištěným osobám. Oproti těmto jiným pachatelům, kteří dlouhodobě posílali velkému počtu adresátů e-maily se závadným obsahem, je jednání obviněného V. B. výrazně menšího rozsahu, když podle zjištění soudu I. stupně za dobu necelých 3 týdnů odeslal dalším adresátům celkem 18 e-mailů se závadným obsahem. Vzhledem k tomuto mnohonásobně menšímu rozsahu jednání obviněného co do počtu e-mailů a připojených závadových souborů i délky jejich trvání, je Nejvyšší soud toho názoru, že není v daném případě splněna podmínka spočívající podle § 88 odst. 1 tr. zákona v tom, že by spáchání činu veřejně přístupnou počítačovou sítí podstatně zvyšovalo stupeň nebezpečnosti činu obviněného pro společnost. Trestný čin šíření pornografie již v ustanovení § 205 odst. 2 tr. zákona obsahoval různé formy (alternativně) opatření pornografického díla jinému, která z hlediska svého významu pro opatření tohoto díla jinému mají být srovnatelná. Je - li mezi těmito formami opatření díla také jeho učinění veřejně přístupným a jeho uvedení do oběhu, je již v tomto ustanovení vyjádřen požadavek vyšší míry zveřejnění takovéhoto díla a tím jeho zpřístupnění většímu počtu osob. Mnohem intenzivnější míru zpřístupnění díla pak představují formy jeho opatření jinému uvedené v ustanovení § 205 odst. 3 písm. b) tr. zákona (tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí, jiným obdobně účinným způsobem), které musí být z hlediska svého významu pro opatření díla rovněž srovnatelné. Je - li film jako dílo svým rozsahem z časového hlediska v rozsahu desítek minut až několika hodin, jsou k e-mailu připojené videosoubory (videoklipy) záležitostí několika vteřin nebo nanejvýš minut. Aby se zpřístupnění díla formou připojeného videosouboru svojí intenzitou vyrovnalo zpřístupnění díla filmem, musí se jednat o výrazně větší počet veřejně přístupnou počítačovou sítí odeslaných videosouborů, což o to víc platí v případě opatření fotografického díla. Není - li tomu tak, nelze podle názoru Nejvyššího soudu dospět k závěru, že jednání spočívající byť v opatření pornografického díla jinému veřejně přístupnou počítačovou sítí podle § 205 odst. 3 písm. b) tr. zákona, podstatně zvyšuje stupeň nebezpečnosti činu pro společnost ve smyslu ustanovení § 88 odst. 1 tr. zákona.

Proto Nejvyšší soud, i když shledal námitky nejvyššího státního zástupce za souladné s judikaturou Nejvyššího soudu, nedospěl k závěru, že by napadené rozhodnutí spočívalo na nesprávném právním posouzení skutku ve smyslu ustanovení § 265b odst. 1 písm. g) tr. ř., jak bylo namítáno v dovolání. Tím ve věci není dán ani druhý uplatněný důvod dovolání podle § 265b odst. 1 písm. l) tr. ř. Proto bylo dovolání jako nedůvodné zamítnuto podle § 265j tr. ř. v neveřejném zasedání, a to v souladu s ustanovením § 265r odst. 1 písm. c) tr. ř.

Poučení:

Proti tomuto usnesení není opravný prostředek přípustný.

V Brně dne 13. července 2011

Předseda senátu:

JUDr. Michal Mikláš