

ACTA  
UNIVERSITATIS  
CAROLINAE

---

IURIDICA 4/2012



# KYBERNETICKÁ KRIMINALITA

UNIVERZITA KARLOVA V PRAZE  
NAKLADATELSTVÍ KAROLINUM  
2013

*Vědecký redaktor:* prof. JUDr. Jiří Jelínek, CSc.

*Recenzovali:* doc. JUDr. Tomáš Gřivna, Ph.D.  
doc. JUDr. Radim Polčák, Ph.D.

## OBSAH

<i>Kateřina Lukášov:</i> Škodliv obsah na internetu .....	7
<i>Lukš Bohuslav, Vladimr Pelc:</i> Trestn in porušení autorskho prva .....	23
<i>Lenka Pošíkov:</i> Ziskvání telekomunikanch dat jako nstroj v boji s internetovou kriminalitou .....	39
<i>Jiř Krupka:</i> Phishing a problmy s jeho trestnprvn kvalifikc v teorii a praxi .....	57
<i>Michaela Pobořilov:</i> Virtuln dtsk pornografie .....	75
<i>Michal Sykora:</i> Trestn postih cyberstalkingu .....	95
<i>Robert Kabt:</i> Virtuln vlastnictv – vlastnictv za as <i>ius downloadendi</i> .....	105

## AUTOŘI

JUDr. Lukáš Bohuslav  
Mgr. Robert Kabát  
JUDr. Jiří Krupička, Ph.D.  
Mgr. et Mgr. Kateřina Lukášová  
Mgr. Vladimír Pelc  
JUDr. Michaela Pobořilová  
Mgr. Lenka Pošíková  
Mgr. Michal Sýkora

## ŠKODLIVÝ OBSAH NA INTERNETU\*

KATEŘINA LUKÁŠOVÁ

Jedním z nejvýraznějších aspektů současné společnosti je rychlý vývoj informačních a telekomunikačních technologií, díky nimž lze snad dokonce označit stávající období za digitální věk neboli dobu digitální. Především je to celosvětová počítačová síť Internet,<sup>1</sup> co relativizuje prostorové i časové omezení komunikace a zároveň umožňuje v nebyvalé míře dostupnost informací v podobě přenášeného množství dat. Lze tak být v kontaktu prakticky s kýmkoliv a kdykoliv,<sup>2</sup> stejně tak jako získat cokoliv, co je převoditelné do podoby dat.

Ve výsledném nepřeborném množství takto přenášených (a za tím účelem ukládaných) dat lze samozřejmě nalézt i taková, která lze považovat za více či méně nežádoucí, a to na jedné straně v rovině morální, na straně druhé i v rovině právní. Předmětem tohoto článku jsou pak právě taková data a jejich trestněprávní charakteristika.

Stručný název „Škodlivý obsah na internetu“ odkazuje na poměrně rozsáhlou oblast. V užším pojetí se jedná zejména o problematiku pornografie (tvrdé, dětské, prosté a včetně jednání označitelného jako sexting) a extremismu, v širším pojetí pod škodlivý obsah na internetu můžeme zařadit i velmi široký okruh dalších jevů, zejména pak různé formy páchání trestné činnosti prostřednictvím kyberprostoru.

Po úvodu do problematiky se článek nejprve věnuje zevrubněji otázkám pornografie a extremismu, poté pokračuje dalšími formami škodlivého obsahu na internetu v širším pojetí (např. kybergroomingem) a zakončen je krátkým shrnutím. Není ambicí článek podat zevrubný výklad škodlivých jevů spojených s internetem, resp. kyberprostorem, ale naopak předložit určitý jejich přehled.

Pozastavím se nejprve nad samotným pojmem kyberprostoru, který používám jako označení virtuálního světa vytvářeného moderními informačními a komunikačními

\* Univerzita Karlova v Praze, Právnická fakulta. Na vznik tohoto článku byla Právnické fakultě Univerzity Karlovy v Praze poskytnuta institucionální podpora v rámci programu rozvoje vědních oblastí na Univerzitě Karlově (PRVŮUK) č. 04 – Institucionální a normativní proměny práva v evropském a globálním kontextu.

<sup>1</sup> Zde je použit výraz „Internet“ odkazující na konkrétní počítačovou síť (vzhledem k tomu, že počítačových sítí může být nepřeborné množství, např. lokální městské, firemní atp.), ovšem dále v textu používám již výraz „internet“ jakožto obecně ustálené spojení odkazující na tuto celosvětově využívanou veřejně přístupnou počítačovou síť.

<sup>2</sup> Za předpokladu, že dotyční mají přístup k internetu.

technologemi.<sup>3</sup> Na první pohled by se snad mohl zdát vhodnější výraz počítačový prostor, nicméně dnešní doba se vyznačuje stále výraznějším propojením různých médií, zejména počítačů (ať už ve formě klasických stolních počítačů, notebooků, tabletů atp.), internetu a mobilních telefonů.<sup>4</sup> Mnohdy je již prakticky nemožné zabývat se těmito médii odděleně, proto je nutno mít při otázce škodlivého obsahu na internetu na paměti nejen používání internetu prostřednictvím počítačů, ale v rámci kyberprostoru jako takového, a zejména pak včetně mobilních telefonů s přístupem k internetu.

Protože článek se zabývá škodlivým obsahem na internetu, i některé zdroje sloužící jako podklad k jeho vypracování se nachází právě na internetu (a v dalších, tradičních médiích), ostatní spočívají v různé formě odborné literatury a samozřejmě v aktuálním znění relevantních zákonů ve spojení s jejich výkladem. Dalším zdrojem (zejména v oblasti rizikového jednání spojeného s internetem ve vztahu k dětem) jsou pak zkušenosti převzaté prostřednictvím osobních rozhovorů především s pedagogy základních a středních škol, převážně pražských.

## 1. UŽIVATELÉ INTERNETU

Škodlivý obsah na internetu je dnes velmi aktuálním tématem, a to hned z několika důvodů. Tím nejmarkantnějším je soustavně stoupající počet uživatelů internetu nepochybně jdoucí ruku v ruce s rostoucím počtem uživatelských míst.<sup>5</sup> Např. oproti roku 2008, kdy bylo v České republice zhruba 54 % uživatelů internetu (starších šestnácti let), v roce 2010 činil jejich podíl již téměř 62 %.<sup>6</sup> Lze předpokládat, že číslo dále poroste – na jedné straně stále roste počet prvouživatelů starších šestnácti let,<sup>7</sup> na straně druhé se přes hranici šestnácti let dostávají ti, kdo používají internet již od útlého věku (jejichž procentuální zastoupení taktéž roste).

Dalším významným fenoménem je rostoucí počet dětských uživatelů spolu s tím, jak se počítač stává běžným vybavením domácnosti, resp. spíše lze říci, že naopak děti patří k příčinám růstu počtu domácností s připojením k internetu. Tento trend dokumentuje fakt, že při celkovém množství 56 % domácností s přístupem k internetu je poměr takových domácností bez dětí 47,2 %, zatímco domácností s dětmi majícími přístup k internetu je téměř 80 %.<sup>8</sup>

Spolu s počtem uživatelů se samozřejmě zároveň rozvíjí i samotný internet, zvláště co do dostupnosti informací a služeb i většího množství a závažnosti rizik s internetem spojených, včetně škodlivého obsahu, a to především s ohledem na zřejmě i klesající

<sup>3</sup> K pojmu „kyberprostor“ blíže viz GRÍVNA, T., POLČÁK, R. (ed.). *Kyberkriminalita a právo*. Praha: Auditorium, 2008, s. 32.

<sup>4</sup> Ještě ve spojení s dalšími tzv. rozhraními, např. webovou kamerou, tiskárnou s dálkovým přístupem atp.

<sup>5</sup> Uživatelskými místy míním např. vytváření různých internetových kaváren a dalších míst, která zpřístupňují internet blíže neurčenému počtu uživatelů, a zároveň stále dostupnější možnost přístupu na internet, zejména prostřednictvím mobilního telefonu.

<sup>6</sup> K uvedeným statistickým údajům viz informace uvedené na webu Českého statistického úřadu: Český statistický úřad. *Informační společnost v číslech 2011*. Dostupné na <http://www.czso.cz/csu/2011edicniplan.nsf/p/9705-11> [cit. 2012-09-20].

<sup>7</sup> Tedy osob, které se učí vůbec s počítači zacházet, zejména ze starších generací.

<sup>8</sup> Viz informace uvedené na webu Českého statistického úřadu: Český statistický úřad. *Informační společnost v číslech 2011*. Dostupné na <http://www.czso.cz/csu/2011edicniplan.nsf/p/9705-11> [cit. 2012-09-20].



věk prvo uživatelů internetu. Zejména mladiství pak navíc žijí svůj sociální život z velké části právě prostřednictvím internetu.

Přesto však nelze problematiku škodlivého obsahu na internetu vztahovat pouze k jeho dětským uživatelům, naopak např. projevy extremismu budou pravděpodobně cíleny spíše na mladistvé a zejména pak dospělé osoby.

Z těchto důvodů je zapotřebí přizpůsobovat výše uvedeným trendům úměrně i určitou ochranu a prevenci v rámci užívání internetu. Už jen samotný fakt, že na internet může de facto kdokoliv vkládat kdykoliv cokoliv, znamená jen obtížně kontrolovatelnou či regulovatelnou oblast, a proto hlavní váha ochrany spočívá na obezřetném jednání každého jedince, ať už dospělého či dítěte.<sup>9</sup>

Z hlediska práva je relevantních hned několik právních předpisů. Na národní úrovni se v první řadě nabízí samozřejmě Listina základních práv a svobod, dále pak trestní zákoník, občanský zákoník, autorský zákon, zákon o elektronických komunikacích, zákon o některých službách informační společnosti atd. Na mezinárodní úrovni pak zejména Úmluva o kyberkriminalitě.<sup>10</sup>

## 2. FORMA ŠKODLIVÉHO OBSAHU NA INTERNETU

Jak jsem již naznačila v úvodu, výraz „škodlivý obsah na internetu“ jen zdánlivě odkazuje na ucelenou, snadno vymežitelnou skupinu jevů. Pravdou je však opak, neboť pod tento pojem můžeme zahrnout poměrně širokou škálu jevů, postížitelých v rámci soukromého i veřejného práva. Vzhledem k překotnému vývoji internetu navíc nelze předpokládat, že bychom mohli být schopni jednoznačně určit i do budoucna, co je či naopak není škodlivým obsahem na internetu.

Škodlivý obsah na internetu můžeme vnímat v širším nebo užším pojetí, přičemž k užšímu pojetí přiřazují zejména pornografii a projevy extremismu. V širším pojetí zahrnují problematiku porušování autorských práv a ochrany osobností a přidávají i další jevy jako sociální inženýrství, kyberšikanu, kybergrooming, násilný obsah.

Lze se setkat s obrázky, fotografiemi a zvukovými záznamy či audiovizuálními záznamy, které mají zřejmě nejvýraznější podíl na škodlivém obsahu na internetu. Jedná se v první řadě o pornografická díla<sup>11</sup> a dále různé obrázky, fotografie, zvukové záznamy, audiovizuální záznamy a různé formy textových souborů i texty samotné jako takové. K tomu nutno přiřadit protiprávní nakládání s obsahem, který sám o sobě protiprávní není.<sup>12</sup>

Specifickou oblast pak představuje používání skryté symboliky, která se objevuje v logách, obrázcích, vizuální podobě webových stránek, textech umístěných na webových stránkách i textech zvukových skladeb.<sup>13</sup> Symboliku využívají nejvíce pravděpo-

<sup>9</sup> Zvláště u dětských uživatelů hraje pak velkou roli výchova zaměřená na bezpečné užívání internetu, zprostředkovaná rodiči, školou, různými institucemi či i mezi vrstevníky navzájem.

<sup>10</sup> Českou republikou dosud sice neratifikována, nicméně vzata v potaz při tvorbě a úpravách současného trestního zákoníku (zák. č. 40/2009 Sb., trestní zákoník, ve znění účinném ke dni 1. ledna 2012, dále jen TZ).

<sup>11</sup> K tomu viz dále.

<sup>12</sup> Např. zasilání prosté pornografie dítěti.

<sup>13</sup> K tomu blíže viz např. CHMELÍK, J. *Extremismus*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2012.

dobně webové stránky obsahující obsah škodlivý z hlediska extremismu, nacházíme např. konkrétní používaný font písma, který běžnému návštěvníkovi může připadat pouze poněkud ojedinělý či nezvyklý, znalá, poučení osoba však již při pouhém prvním pohledu ví nebo tuší, jaké skryté poselství v textu hledat. Obdobně fungují různé symboly, např. číslo 88 odkazující mezi neonacisty na nacistický pozdrav Heil Hitler.<sup>14</sup>

Nelze opomenout ani porušování práva na ochranu osobnosti zveřejňováním fotografií a audiovizuálních záznamů osob bez jejich svolení, aniž by šlo o jednání v rámci některé ze zákonných licencí. Taktéž je časté zveřejňování nepravdivých údajů o konkrétních osobách s cílem je poškodit. Za tím účelem vznikají případně i samostatné webové stránky.

Za zvláštní formu škodlivého obsahu na internetu považují umístění odkazu na webové stránky obsahující škodlivý obsah na internetu.<sup>15</sup>

Osoby umísťující protiprávní obsah na internet se mnohdy snaží uniknout sankcionování svého jednání tím, že takový obsah ukládají na servery fyzicky umístěné v zahraničí, přičemž se domnívají, že tím dosáhnou vyloučení z působnosti zákonů České republiky. Trestní zákoník<sup>16</sup> však považuje za trestný čin spáchaný na území České republiky i takový, jímž pachatel v ČR porušil nebo ohrozil zájem chráněný trestním zákonem nebo měl-li alespoň zčásti takový následek v ČR nastat (ust. § 4 odst. 2 písm. b) TZ).<sup>17</sup> Domnívám se proto, že z hlediska místní působnosti lze zákon ČR co do trestnosti případného spáchaní trestného činu v případě webových stránek aplikovat vždy, je-li možné vyvolat<sup>18</sup> danou webovou stránku na území ČR. K tomu ovšem musí přistoupit záměr pachatele, aby webová stránka byla vyvolána právě v ČR, samotná pouhá možnost vyvolání jistě nebude dostačující.<sup>19</sup>

### 3. PORNOGRAFIE

Na internetu lze v současnosti nalézt obrovské množství pornografického materiálu. V prvé řadě se nabízí celé servery věnované pornografii, zpravidla komerčního typu – placené nejčastěji formou umístění reklamy a často také zasíláním hrazené SMS ze strany uživatelů na vybrané telefonní číslo. Objevuje se také požadavek registrace, včetně uvedení e-mailové adresy, na kterou se následně zasílají další reklamní sdělení, spamy atp. Nelze nicméně vynechat ani pornografii kolující mezi jednotlivými uživateli, ať už prostřednictvím sdílení<sup>20</sup> či přímým zasíláním.

<sup>14</sup> Viz EICHLER, P., VEDRAL, J. Neonacisté v Česku snadno koupí „to pravé“ oblečení. *iDNES*, 8. 10. 2006. Dostupné na [http://zpravy.idnes.cz/neonaciste-v-cesku-snadno-koupí-to-prave-obleceni-f7q-/domaci.aspx?c=A061006\\_150831\\_krimi\\_pei](http://zpravy.idnes.cz/neonaciste-v-cesku-snadno-koupí-to-prave-obleceni-f7q-/domaci.aspx?c=A061006_150831_krimi_pei) [cit. 2012-10-03].

<sup>15</sup> Zde pouze zmiňuji pro úplnost.

<sup>16</sup> Zák. č. 40/2009 Sb., trestní zákoník.

<sup>17</sup> K tomu viz např. judikatura k ust. § 4 TZ v ŠÁMAL, P. et al. *Trestní zákoník: komentář*. Praha: C. H. Beck, 2009, s. 59.

<sup>18</sup> Vyvoláním míním zobrazení webové stránky prostřednictvím zařízení přístupujícího k internetu na území České republiky – typicky např. zobrazení na monitoru počítače nebo displeji mobilního telefonu.

<sup>19</sup> Srov. POSPÍŠIL, M. Německo: Místní působnost trestních norem a Internet. *IT právo*, 17. 1. 2001. Dostupné na <http://www.itpravo.cz/index.shtml?x=61318> [cit. 2012-10-20].

<sup>20</sup> Sdílení lze nejsnadněji popsat jako podělení se s někým o příslušná data, aniž by tím byla data jakkoliv ovlivněna. Typicky dochází ke sdílení např. nahráním dat do úložiště dostupného prostřednictvím inter-

Umístění jakéhokoliv pornografického díla na internet či jeho rozeslání, přeposlání nebo vůbec stažení ještě samo o sobě nemusí být protiprávní, nepřistoupí-li k tomu další okolnosti. Nejprve je nutné vymezit pornografické dílo jako takové, resp. jednotlivé druhy pornografie z hlediska trestního zákona, neboť ne každá pornografie se považuje za společensky nežádoucí.<sup>21</sup>

V druhé řadě stojí za zmínku zpřístupňování jakékoliv pornografie dětem, resp. osobám mladším 18 let, a možné způsoby řešení této otázky.

Pornografické dílo<sup>22</sup> není v současnosti v trestním zákoně definováno, lze tedy pouze dovozovat, co jím je a co není, a to i s ohledem na určitou hladinu morálního vývoje uznávanou společností a na to, co ještě společnost považuje za přijatelné. Posuzujeme dílo jako takové, nikoliv ve vztahu k jeho „uživatelům“ či adresátům. Odborná veřejnost se shoduje na tom, že „pornografické dílo lze charakterizovat tím, že zvláště intenzivním a vtíravým způsobem zasahuje a podněcuje sexuální pud, překračuje podle převládajících názorů ve společnosti uznávané hranice sexuální slušnosti, uráží neakceptovatelným způsobem cit pro sexuální slušnost, vyvolává pocit studu“.<sup>23</sup> Zjednodušeně řečeno: „Za pornografické dílo se považuje takové dílo, jehož jediným účelem je vyvolat (zvyšovat) sexuální vzrušení.“<sup>24</sup> Zobrazení nahého těla či těl jako takové, včetně zobrazení sexuálního aktu vůbec, ještě samo o sobě nemusí být považováno z hlediska trestního práva za pornografii.

Při rozlišování pornografického díla se uvádí tzv. pornografie tvrdá, dětská a prostá. Tvrdá pornografie zobrazuje násilí či neúctu k člověku<sup>25</sup> nebo popisuje, zobrazuje či jinak znázorňuje pohlavní styk se zvířetem. Dětská pornografie (z hlediska českého trestního práva) zobrazuje nebo jinak využívá dítě, tedy osobu mladší 18 let, nebo osobu, jež se jeví být dítětem. Zde je patrný vliv dosud v ČR neratifikované Úmluvy o počítačové kriminalitě, která zavádí pojem dětské pornografie jako „pornografický materiál, který vizuálně zobrazuje nezletilého při zjevném sexuálním chování nebo osobu, která se jeví jako nezletilá při zjevném sexuálním chování či realistické obrázky ukazující nezletilého při zjevném sexuálním chování“.<sup>26</sup> ČR se vydala cestou rozšíření pojmu dětská pornografie o pornografická díla vizuálně zobrazující viditelný sexuální akt osoby, jež pouze vyhlíží jako nezletilá, změnou trestního zákoníku provedenou zákonem č. 330/2011 Sb. s účinností ke dni 1. prosince 2011.<sup>27</sup> Až do 30. listopadu 2011 dětská pornografie odkazovala pouze na takovou pornografii, která zobrazuje nebo jinak vyu-

---

netu, kam mají přístup kromě nahravatele další osoby dle jeho zadaných kritérií (např. uživatel konkrétní e-mailové adresy nebo naopak třeba kdokoliv, kdo zná adresu uložení).

<sup>21</sup> Tím zde samozřejmě netvrdím, že některý typ pornografie je přímo žádoucí.

<sup>22</sup> Výraz „dílo“ je z hlediska trestního zákona širší než přesně vymezené dílo autorské dle autorského zákona.  
<sup>23</sup> Srov. NOVOTNÝ, O., VOKOUN, R. et al. *Trestní právo hmotné II. Zvláštní část*. Praha: ASPI, 2007, s. 275.

<sup>24</sup> Viz JELÍNEK, J. et al. *Trestní zákon a trestní řád s poznámkami a judikaturou a předpisy související, zákon o soudnictví ve věcech mládeže, zákon o Policii ČR, zákon o výkonu vazby, zákon o výkonu trestu odnětí svobody, zákon o Probační a mediační službě, advokátní tarif, v úplném znění: podle stavu k 1. 10. 2008, se zapracováním změn účinných od 1. 1. 2009*. Praha: Linde, 2008, s. 249.

<sup>25</sup> Skutečně, nikoliv předstírané násilí či neúctu.

<sup>26</sup> Viz GRÍVNA, T., POLČÁK, R. (ed.). *Kyberkriminalita a právo*. Praha: Auditorium, 2008, s. 154.

<sup>27</sup> Zůstává zde ovšem stále určitý prostor pro případné použití jakési „quasidětské“ pornografie (tedy takové, která pouze realisticky zobrazuje dítě – např. animovaná pornografie), a to zejména ve vztahu k léčbě pedofilů, nebo spíše ve vztahu k tlumení jejich sexuálních potřeb. K tomu viz např. JILKOVÁ, M. Povolme animované dětské porno, říká sexuolog Weiss. *iDNES.cz/Zprávy*, 9. 10. 2007. Dostupné na [http://zpravy.idnes.cz/povolme-animovane-detske-porno-rika-sexuolog-weiss-fhs-domaci.aspx?c=A071009\\_115203\\_](http://zpravy.idnes.cz/povolme-animovane-detske-porno-rika-sexuolog-weiss-fhs-domaci.aspx?c=A071009_115203_)

živá dítě, ale nikoliv již osobu jako dítě pouze vypadající. Z hlediska českého právního řádu pak veškerá ostatní pornografická díla zařazujeme mezi pornografii prostou.

Pornografické dílo může dle trestního zákoníku nabývat podobu písemnou, fotografickou, filmovou, počítačovou, elektronickou (např. soubor obsahující pornografii, která tak není vnímatelná jinak než za použití zobrazovacího přístroje, např. počítače ve spojení s monitorem) nebo jinou.

K pornografii jako projevu škodlivého obsahu na internetu (nebo k protiprávnímu nakládání s ní) se pojí zejména trestný čin šíření pornografie (ust. § 191 TZ zahrnuje hned dvě základní skutkové podstaty), dále pak trestný čin výroby a jiného nakládání s dětskou pornografií (ust. § 192 TZ, taktéž zahrnuje dvě základní skutkové podstaty).

Trestného činu šíření pornografie (ust. § 191 odst. 1 TZ) se dopustí, kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří tvrdé pornografické dílo (v případě internetového prostředí připadá v úvahu zejména tvrdé pornografické dílo v elektronické podobě). Stává se tak typicky např. umístěním tvrdé pornografie na webové stránky. Dalšími formami trestného činu šíření pornografie v rámci škodlivého obsahu na internetu pak bude zejména uvedení tvrdé pornografie do oběhu, tedy například rozesílání prostřednictvím sociální sítě, a dále pak zprostředkování, prodej nebo jiné opatření jinému tvrdé pornografie (např. zaslání e-mailem).

Druhá základní skutková podstata trestného činu šíření pornografie (ust. § 191 odst. 2 TZ) zahrnuje nabídnutí, přenechání nebo zpřístupnění dítěti (tedy osobě mladší 18 let)<sup>28</sup> jakékoliv pornografie, nebo zpřístupnění či jiné vystavení jakékoliv pornografie na místě dětem přístupném. V případě internetu tak půjde typicky o zpřístupnění a umístění na místě dětem přístupném prostřednictvím pornografických serverů a různých pop-up oken. Servery s pornografickým materiálem mnohdy vyvíjejí určitou snahu zamezit přístupu dětí, a to obvykle prostřednictvím vstupní stránky dotazující se na věk návštěvníka a zamítnutím zobrazení dalšího obsahu v případě, že dotyčný se sám dobrovolně označí za osobu mladší 18 let. K tomu se eventuálně přidává poskytnutí informace o tom, že má být zobrazen pornografický materiál, spolu s výzvou adresovanou osobám mladším 18 let, aby dané stránky opustily. Domnívám se, že v tomto směru činí majitelé těchto webů z právního hlediska dostatek opatření, aby jejich webové stránky nebyly „místem dětem přístupným“, neboť takové místo je definované např. jako „kterékoli místo, kde je umožněn přístup osobám mladším 18 let, resp. které je obvykle dětmi navštěvováno, ale nejen výlučně jimi. Nejde tedy o místa, do kterých mají děti zakázán přístup (sexshopy, pornografická kina)“.<sup>29</sup> Tím ovšem není dotčena případná odpovědnost za zpřístupňování pornografie dětem. To je definováno např. jako „jednání, kterým je umožněno, aby se s pornografickým dílem mohly seznámit děti“,<sup>30</sup> je proto klíčové, zda úmysl případného pachatele kryje i tuto skutečnost. Tedy zda případný pachatel chtěl, aby bylo pornografické dílo zpřístupňováno dětem, nebo věděl, že se tak může stát, a pro ten případ s tím byl srozuměn (ust. § 15 TZ).

---

domaci\_nad [cit. 2012-08-12] nebo HERCZEG, J. Virtuální dětská pornografie: Zločin bez oběti? In: VANDŮCHOVÁ, M., GRÍVNA, T. (ed.) *Pocta Otovi Novotnému k 80. narozeninám*. Praha: ASPI, 2008.

<sup>28</sup> Viz ust. § 126 TZ.

<sup>29</sup> Viz ŠÁMAL, P. et al. *Trestní zákoník: komentář*. Praha: C. H. Beck, 2009, s. 1699.

<sup>30</sup> Viz tamtéž.

Trestný čin výroby a jiného nakládání s dětskou pornografií v základní skutkové podstatě dle ust. § 192 odst. 1 TZ není z hlediska škodlivého obsahu na internetu příliš relevantním (postihuje přechovávání dětské pornografie). Zato však jeho druhá základní skutková podstata (ust. § 192 odst. 2 TZ) již zahrnuje např. nabídnutí, činění veřejně přístupným, zprostředkování, uvedení do oběhu, prodej nebo jiné opatření jinému dětské pornografie.<sup>31</sup>

### 3.1 SEXTING

V rámci šíření pornografie považují za vhodné upozornit na praxi mladistvých v současnosti se rozmáhající, a to i u dětí mladších 15 let, zvanou sexting.<sup>32</sup> Termín sexting nejprve označoval zasílání sexuálně laděných obrázků prostřednictvím mobilních telefonů,<sup>33</sup> ovšem s ohledem na rozvoj informačních a komunikačních technologií se v současnosti pod sexting řadí i zasílání krátkých podobně laděných videí. Tyto materiály (často vznikající v rámci partnerských vztahů) s sebou vždy nesou riziko, že např. jeden partner z nejrůznějších pohnutek zveřejní fotografie či videa svého partnera. K tomu zbývá doplnit, že se jedná zpravidla o fotografie či videa zachycující odesílatele, od portrétů po pornografická díla.

Sexting je pro mládež lákavý hned z několika důvodů, zejména však ze dvou: na straně jedné stojí touha po sebezpřetaci a kladné odezvě okolí,<sup>34</sup> která výrazně nabývá na intenzitě v období dospívání především. Druhým častým důvodem je snaha o drobný přivýdělek, zvláště v podobě kreditu do mobilního telefonu atp. výměnou za zaslání vlastní fotografie či krátkého videa. Nelze ovšem pominout ani výrazný vliv vrstevnické skupiny a normy chování v ní respektované – zjednodušeně řečeno, čím více vrstevníků sexting provozuje, tím menší jsou sociální zábrany k jeho provozování pro kohokoliv dalšího v jejich okolí.

Na první pohled by se snad sexting mohl zdát jako neškodné flirtování s větší kapkou lehkomyšlnosti, což bohužel může být zcela mylnou představou na hony vzdálenou pravdě, a to zvláště v případech, kde lze takové fotografie či videa považovat za pornografická díla. Z hlediska trestního práva se nabízí hned několik možných skutkových podstat, pod které lze jednat v rámci sextingu podřadit.

Vezměme v úvahu nejprve zasílání pornografických fotografií či videí<sup>35</sup> osobě mladší 18 let. Toto jednání lze podřadit pod skutkovou podstatu trestného činu šíření pornografie podle ust. § 191 odst. 2 písm. a) TZ, neboť pachatel buď nabízí, nebo přímo přenechává pornografické dílo dítěti. Výraz „přenechává“ je totiž definovaný např. tak, že „přenecháváním se již pornografické dílo skutečně dostává do rukou dítěte, které se

<sup>31</sup> K tomu viz výše.

<sup>32</sup> K tomu blíže viz např. LIVINGSTONE, S., HADDON, L., GÖRZIG, A., ÓLAFSSON, K. *EU Kids Online final report*. The London School of Economics and Political Science, 2011.

<sup>33</sup> Viz např. BARKACS, L., BARKACS, C. B. Do you think I'm sexy? Minors and sexting: teenage fad or child pornography? *Journal of Legal, Ethical & Regulatory Issues*, 2010, roč. 13, č. 2, s. 23.

<sup>34</sup> Vzhledem k tomu, že ti, kdo tyto materiály pořizují, tak činí s úmyslem se jejich prostřednictvím prezentovat, „posílají do světa“ jen takové, na kterých vypadají dle svého názoru skutečně dobře, přinejmenším z hlediska jejich referenční skupiny (tj. takové, se kterou se ztotožňují či chtějí ztotožnit). Kladná odezva okolí, resp. jejich referenční skupiny je proto vcelku pravděpodobná.

<sup>35</sup> Takového charakteru, že je lze považovat za pornografické dílo z hlediska trestního zákona.

tak může s pornografickým dílem seznámit.<sup>36</sup> Jestliže pachatel „pouze“ zašle osobě mladší 18 let soubor s pornografickým dílem, který je k jeho vnímání nutno nejprve otevřít (tedy vyvinout určitou aktivitu ze strany dítěte), lze takové jednání posoudit jako nabídnutí pornografického díla dítěti („nabídka je jakékoli předložení pornografického díla, které má za cíl, aby si jej jiný převzal“).<sup>37</sup> Při rozlišení znaku „přenechává“ a „nabízí“ tak v současnosti u sextingu připadá v úvahu<sup>38</sup> zejména varianta zaslání MMS<sup>39</sup> (zde půjde o nabízení, neboť k zobrazení obsahu MMS je nezbytná aktivita ze strany uživatele směřující k jejímu zobrazení). Může ovšem dojít i k naplnění znaku přenechávání namísto nabízení – např. u zaslání e-mailu s přílohou, kdy je tato příloha automaticky zobrazena jako jeho součást.<sup>40</sup> O trestný čin se ovšem jedná samozřejmě za předpokladu, že jednání pachatele dosáhlo natolik významného stupně společenské škodlivosti, že postih podle jiných právních předpisů není postačující, a je proto nutné použít jakožto ultima ratio prostředky trestního práva.<sup>41</sup>

Mladistvý se může dopustit také trestného činu výroby a jiného nakládání s dětskou pornografií. Nikoliv však tím, že vyrobí dětskou pornografii, jejímž bude jediným aktérem, vzhledem k obecné právní zásadě, že „nemůže být trestná osoba, k jejíž ochraně je příslušné trestněprávní ustanovení určeno“,<sup>42</sup> ve spojení s tím, že „objektem trestného činu výroby a jiného nakládání s dětskou pornografií je zájem společnosti na ochraně mravního vývoje dětí a jejich ochraně před sexuálním zneužíváním“.<sup>43</sup> Kdokoliv, včetně mladistvého se nicméně může dopustit trestného činu výroby a jiného nakládání s dětskou pornografií podle ust. § 192 odst. 2 alinea 1 TZ tím, že rozesílá dětskou pornografii, neboť jednání spočívající v rozesílání dětské pornografie můžeme podřadit pod nabídnutí, případně zprostředkování dětské pornografie jinému – za předpokladu, že objektem trestného činu výroby a jiného nakládání s dětskou pornografií podle ust. § 192 odst. 2 alinea 1 TZ je kromě zájmu společnosti na ochraně mravního vývoje dětí a jejich ochraně před sexuálním zneužíváním zároveň zájem na mravních hodnotách společnosti, která dětskou pornografii považuje za škodlivou.

Trestného činu šíření pornografie i výroby a jiného nakládání s dětskou pornografií se lze dopustit v jednočinném souběhu s ohrožováním výchovy dítěte podle ust. § 201 odst. 1 písm. a) TZ. „Objektem trestného činu ohrožování výchovy dítěte je zájem na řádné výchově dětí, která má být vedena v souladu se zásadami morálky občanské společnosti tak, aby byl zaručen jejich řádný rozumový, mravní a citový vývoj.“<sup>44</sup> K ohrožení rozumového, citového nebo mravního vývoje dítěte pak dojde zejména teh-

<sup>36</sup> Viz ŠÁMAL, P. et al. *Trestní zákoník: komentář*. Praha: C. H. Beck, 2009, s. 1699.

<sup>37</sup> Viz tamtéž, s. 1697.

<sup>38</sup> Vzhledem k vývoji informačních a komunikačních technologií lze předpokládat, že z technického hlediska přibudou další varianty.

<sup>39</sup> MMS (z anglického Multimedia Message Service) neboli tzv. multimediální zpráva, tedy taková, která kombinuje různá média, typicky psaný text spolu s obrázkem, videem či zvukem, včetně variací těchto kombinací.

<sup>40</sup> K zamyšlení pokládám otázku, zda automatické zobrazení přílohy po otevření e-mailu spadá pod znak „přenechává“ nebo „nabízí“, neboť zobrazení vyžaduje aktivitu ze strany uživatele, avšak aktivitu směřující k otevření e-mailu, nikoliv zobrazení přílohy.

<sup>41</sup> Pozornost otázce společenské škodlivosti je pochopitelně třeba věnovat vždy při posuzování všech jednání zde uvedených.

<sup>42</sup> Viz ŠÁMAL, P. et al. *Trestní zákoník: komentář*. Praha: C. H. Beck, 2009, s. 1481.

<sup>43</sup> Viz NOVOTNÝ, O. et al. *Trestní právo hmotné: Zvláštní část*. Praha: Wolters Kluwer ČR, 2010, s. 130.

<sup>44</sup> Viz ŠÁMAL, P. et al. *Trestní zákoník: komentář*. Praha: C. H. Beck, 2009, s. 1762.

dy, jestliže jednání pachatele vede ke vzniku reálného nebezpečí např. pohlavní nevázanosti, promiskuity, osvojení si takových návyků dítětem, které vedou „k jeho morálnímu úpadku a k neschopnosti usměrňovat způsob svého života v souladu s obecnými morálními zásadami občanské společnosti“.<sup>45</sup> Výjimečně by se tak mohlo stát i v případě sextingu, pokud by jeho provozování a obsah ze strany konkrétního odesílatele ve vztahu ke konkrétnímu adresátovi – dítěti – přesáhly určitou míru.<sup>46</sup> Trestného činu ohrožování výchovy dítěte podle ust. § 201 odst. 1 písm. b) nebo c) nebo d) TZ se mohou dopustit např. i rodiče dítěte, jestliže k porušení jejich rodičovské zodpovědnosti dojde v takové míře, že umožní vést dítěti v tomto případě nemravný život nebo závažným způsobem poruší svou povinnost o ně pečovat či jinou svou důležitou povinnost vyplývající z rodičovské zodpovědnosti.

Sexting může být spojen i s trestným činem zneužití dítěte k výrobě pornografie podle ust. § 193 odst. 1 TZ, kterého se dopustí ten, kdo přiměje, zjedná, najme, zláká, svede nebo zneužije dítě k výrobě pornografického díla nebo kořistí z účasti dítěte na takovém pornografickém díle. Půjde především o najmutí, a to tehdy, když se pachatel s dítětem dohodne na tom, že dítě samo vyrobí a zašle mu pornografický materiál zahrnující toto dítě výměnou za kredit do mobilního telefonu či jinou obdobnou protislužbu či protihodnotu (např. koupě herního času pro hraní počítačové hry). Předpokladem je, že dítě tento materiál vyrobilo až na základě takové dohody s pachatelem. Skutková podstata trestného činu zneužití dítěte k výrobě pornografie podle ust. § 193 odst. 1 TZ může být ovšem naplněna i zlákaním nebo svedením zvláště v případě partnerských vztahů mládeže, v jejichž rámci jeden partner přesvědčí druhého k výrobě dětské pornografie.

Kromě trestněprávních důsledků může mít sexting samozřejmě také dopady v psychosociální rovině. Na straně jedné může působit pozitivně na vnímání vlastní sexuality a sebepojetí, na straně druhé je může naopak deformovat. Kromě toho jsou jeho aktéři ohroženi i do budoucna tím, že si nemohou nikdy být zcela jisti, kdo získal přístup k je zobrazujícímu pornografickému dílu (třeba i po letech) a jak s ním hodlá nakládat.

#### 4. EXTREMISMUS

Na internet lze svým způsobem nahlížet jako na Janusovu tvář. Na jedné straně nabízí určitou formu veřejného prostoru, kde se mohou svobodně realizovat mnohé názorové proudy, stejně tak jako různé skupiny. De facto každý jedinec i skupina tak mohou touto cestou vyjádřit své názory i potřeby a např. usilovat o jejich naplnění prostřednictvím získávání podpory jiných osob či skupin. Internet tak jednoznačně podporuje názorovou i kulturní rozmanitost.<sup>47</sup>

<sup>45</sup> Viz tamtéž, s. 1763.

<sup>46</sup> Míru ospravedlnitelnou např. touhou experimentovat s vlastní sexualitou nebo vyhledávat zážitkové podněty. Zlomový bod se pak bude nalézat někde mezi jednorázovým pokusem (nebo občasnými pokusy) a způsobem života vyznačujícím se obchodováním s využitím svého těla.

<sup>47</sup> K názorové a kulturní rozmanitosti se nerozlučně pojí riziko přílišné relativizace hodnot, jež může vést až k anomii, což ovšem není tématem tohoto článku; uvádím tuto poznámku pouze pro úplnost.

Na druhé straně internet skýtá stejným způsobem prostor i pro projevy nesnášenlivosti a netolerance. Jakmile dosáhnou tyto společensky nežádoucí jevy určité míry, mohou již začít naplňovat znaky skutkové podstaty trestného činu, a to zejména trestného činu založení, podpory a propagace hnutí směřujícího k potlačení práv a svobod člověka<sup>48</sup> (např. tvorba webové stránky zaměřené na hlásání neonacistické ideologie), trestného činu projevu sympatií k hnutí směřujícímu k potlačení práv a svobod člověka<sup>49</sup> (pachatel zde hnutí přímo nepropaguje, ale např. vyjadřuje k němu veřejně<sup>50</sup> obdiv bez úmyslu získávat tomuto hnutí další přívržence či jinak posilovat jeho pozici)<sup>51</sup> a eventuálně i trestného činu popírání, zpochybňování, schvalování a ospravedlňování genocidia.<sup>52</sup>

Zároveň můžeme do oblasti projevů extremismu zařadit i tzv. hate crimes, neboli trestné činy z nenávisti. Jedná se o trestné činy motivované společenskými předsudky, ať už se tyto vztahují např. k rase, etnické skupině, náboženství, politické orientaci, sexuální orientaci aj.<sup>53</sup> V prostředí České republiky sem proto zařazujeme zejména trestný čin hanobení národa, rasy, etnické nebo jiné skupiny osob<sup>54</sup> („hanobením se rozumí subjektivní, hrubě urážlivý projev směřující k hrubému znevážení“),<sup>55</sup> trestný čin podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod<sup>56</sup> a případně i trestný čin násilí proti skupině obyvatelů a proti jednotlivci.<sup>57</sup> V ostatních případech, kdy nelze škodlivé jednání kvalifikovat jako některý ze zde uvedených trestných činů, ale zároveň přesto nese znaky trestného činu z nenávisti, soud k takové motivaci přihlídně jako k přitěžující okolnosti spočívající v tom, že pachatel spáchal trestný čin z národnostní, rasové, etnické, náboženské, třídní či jiné podobné nenávisti nebo z jiné zvláště zavrženíhodné pohnutky<sup>58</sup> (nejedná-li se o okolnost podmiňující použití vyšší trestní sazby).<sup>59</sup>

## 5. PORUŠOVÁNÍ AUTORSKÝCH PRÁV A PRÁVA NA OCHRANU OSOBNOSTI

V úvodu jsem zahrнула do širšího pojetí škodlivého obsahu na internetu i některé trestné činy páchané prostřednictvím internetu. Největší kategorií v této oblasti tvoří nepochybně porušování autorských práv. Specifikum zde spočívá ve skutečnosti, že samotný obsah umístěný na internetu škodlivý není, ale je s ním nakládáno protiprávním způsobem, nejčastěji ve formě neoprávněného užití díla jeho sdělováním veřejnosti

<sup>48</sup> Ust. § 403 odst. 1, 2 písm. a) TZ.

<sup>49</sup> Viz ust. § 404 TZ.

<sup>50</sup> Tedy např. veřejnou počítačovou sítí, viz ust. § 117 písm. a) TZ.

<sup>51</sup> Viz ŠÁMAL, P. et al. *Trestní zákoník: komentář*. Praha: C. H. Beck, 2009, s. 3208.

<sup>52</sup> Viz ust. § 405 TZ.

<sup>53</sup> K tomu viz např. JACOBS, J. B., POTTER, K. *Hate Crimes: Criminal Law and Identity Politics*. Cary, NC, USA: Oxford University Press, 2000, s. 11.

<sup>54</sup> Viz ust. § 355 odst. 1 písm. a) nebo b), odst. 2 písm. b) TZ.

<sup>55</sup> Viz Rt 11/2007 (2. část). *Profiprávo*, 4. 9. 2007. Dostupné na [http://profipravo.cz/index.php?page=article&id\\_category=168&id\\_article=248934&csum=835c8427](http://profipravo.cz/index.php?page=article&id_category=168&id_article=248934&csum=835c8427) [cit. 2012-08-12].

<sup>56</sup> Viz ust. § 356 odst. 1, 3 písm. a) TZ.

<sup>57</sup> Viz ust. § 352 odst. 2, 3 písm. b) TZ.

<sup>58</sup> Viz ust. § 42 písm. b) TZ.

<sup>59</sup> Viz ust. § 17 písm. b) TZ.



prostřednictvím veřejně přístupné počítačové sítě. Pachatel se tak může dopustit trestného činu porušení autorského práva, práv souvisejících s právem autorským a práv k databázi (ust. § 270 TZ). Chráněno je zde autorské dílo, umělecký výkon, zvukový či zvukově obrazový záznam, rozhlasové nebo televizní vysílání nebo databáze. Proti-právní jednání spočívá obvykle v neoprávněném zhotovení rozmnoženiny díla a jeho rozšiřování prostřednictvím veřejné počítačové sítě.<sup>60</sup>

V prostředí internetu dochází často také ke zveřejňování osobních údajů bez svolení jejich subjektu. Jestliže se jedná o osobní údaje shromážděné v souvislosti s výkonem veřejné moci, pachatel se může dopustit trestného činu neoprávněného nakládání s osobními údaji dle ust. § 180 odst. 1 TZ. Jestliže zveřejněním osobních údajů získaných v souvislosti s výkonem povolání, zaměstnání nebo funkce pachatele tento poruší státem uloženou nebo uznanou povinnost mlčenlivosti a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají, pachatel se dopustí trestného činu neoprávněného nakládání s osobními údaji dle ust. § 180 odst. 2 TZ.

Velká část škodlivého obsahu na internetu v širším pojetí spočívá ve zveřejňování různých nelichotivých či přímo zesměšňujících, ponižujících fotografií a videí druhých osob. Obvykle lze takové jednání kvalifikovat nanejvýše jako přestupek proti občanskému soužití,<sup>61</sup> jeho dopady v psychické rovině napadeného jedince mohou však být značné. Na místě jsou proto alespoň občanskoprávní prostředky ochrany.<sup>62</sup>

## 6. NĚKTERÉ DALŠÍ ŠKODLIVÉ JEVY V PROSTŘEDÍ INTERNETU

Ke škodlivým jevům na internetu v širším pojetí patří i další problematiky než výše uvedené. Vzhledem k omezenému prostoru článku je zmiňuji více méně pouze ve stručnosti, byť každé z uvedených témat zasluhuje samostatné zamyšlení.

Velkou skupinu zde tvoří oblast sociálního inženýrství, kde škodlivý obsah spočívá velmi často v malwaru.<sup>63</sup> Jiná jednání zakládající škodlivý obsah na internetu, jako např. kyberšikana nebo kybergrooming, mívají zejména písemnou podobu ve formě textů na chatech a sociálních sítích. Obvykle ve formě videí pak můžeme na internetu nalézt různý násilný obsah.

Svým způsobem lze ke škodlivému obsahu na internetu zařadit i podněcování k trestnému činu (ust. § 364 TZ)<sup>64</sup> a schvalování trestného činu (ust. § 365 TZ), dopouští-li se jich pachatel veřejně, tedy v tomto případě veřejně přístupnou počítačovou sítí,<sup>65</sup> tzn. např. prostřednictvím příspěvků na svém profilu v sociální síti.

<sup>60</sup> Srov. např. judikaturu k ust. § 270 TZ v PROUZA, D. et al. *Trestní zákoník s judikaturou*. Praha: C. H. Beck, 2010, s. 974.

<sup>61</sup> Viz ust. § 49 odst. 1 písm. a) zák. č. 200/1990 Sb., zákon České národní rady o přestupcích.

<sup>62</sup> Zápůřčí žaloba, žalobní nárok restituční, satisfakční (morální zadostiučinění, náhrada nemajetkové újmy v penězích) aj. (např. právo domáhat se určení, že neoprávněným zásahem došlo k porušení práva na ochranu osobnosti).

<sup>63</sup> Malware je škodlivý software sloužící na jedné straně k poškození počítače či jiného zařízení nebo poškození počítačové sítě, na straně druhé je využíván i k získání různých dat z napadeného zařízení (ať už se jedná např. o hesla uživatele atp. nebo blíže specifikované soubory aj.).

<sup>64</sup> „Podněcovat lze i k individuálně neurčeným trestným činům a podněcování může být adresováno neurčitému okruhu osob,“ viz ŠAMAL, P. et al. *Trestní zákoník: komentář*. Praha: C. H. Beck, 2009, s. 3062.

<sup>65</sup> Viz ust. § 117 písm. a) TZ.

## 6.1 SOCIÁLNÍ INŽENÝRSTVÍ

Sociální inženýrství lze obecně definovat jako určitý způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace.<sup>66</sup> Pod jednoduchou definicí se skrývá pestrá škála různých technik, jak se neoprávněně dostat k citlivým datům nebo tato data ještě dále využít. Jmenovat lze např. phishing,<sup>67</sup> trojské koně,<sup>68</sup> spoofing,<sup>69</sup> DoS a DDoS,<sup>70</sup> malware. V případě malwaru (podobně jako i u jiných uvede- ných technik) je škodlivým obsahem samotný text programu způsobilý vyvolat změny v počítačovém systému příjemce. Autor malwaru se tak může dopustit např. trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací dle ust. § 230 odst. 2 písm. a) (v případě, že neoprávněně užije data uložená v napadeném počítači) nebo d)<sup>71</sup> a eventuálně i odst. 3 písm. a) či b) (případně obojí) TZ.

## 6.2 KYBERŠIKANÁ

Zvláštní oblast představuje jednání v rámci kyberšikaný.<sup>72</sup> Ta probíhá často formou vytváření různých webů zesměšňujících oběť nebo pomlouváním na sociálních sítích (trestný čin pomluvy dle ust. § 184 odst. 1, 2 TZ), opatřením si hesla k počítači poškozeného za účelem spáchání trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací dle ust. § 231 odst. 1 písm. b) TZ nebo prolomením počítačového hesla (trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací dle ust. § 230 odst. 1 TZ) a např. i následnou manipulací s profilem oběti na sociální síti atp. (trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací dle ust. § 230 odst. 2 písm. b) nebo c), odst. 3 písm. a) TZ). Škodlivý obsah na internetu zde má zejména písemnou formu spočívající v samotných textech, ovšem nabývá i podoby obrázků, fotografií a videí (zpravidla použitých bez souhlasu zobrazené osoby, a tudíž porušujících její právo na ochranu osobnosti).

<sup>66</sup> K sociálnímu inženýrství blíže viz např. BAMNOTE, G., PATIL, G., SHEJOLE, A. Social Networking-Another Breach In The Wall. *AIP Conference Proceedings*; 11/6/2010, č. 1, s. 151.

<sup>67</sup> Tedy podvodné e-mailové aj. útoky snažící se vylákat z uživatele citlivé údaje (typicky např. v podobě odpovědi na dotaz ze strany zdánlivě důvěryhodné osoby či instituce nebo přístupu na falešné webové stránky).

<sup>68</sup> Obvykle počítačový program vpravený do zařízení uživatele bez jeho vědomí (např. při stahování dat z internetu může být trojský kůň jejich skrytou součástí), obsahovat může např. tzv. keylogger (software monitorující úhozy do klávesnice, který zasílá zprávy o tom svému původci).

<sup>69</sup> Typ útoku využívající tzv. doménový překladač (ten „překládá“ číslo IP adresy do podoby např. www.wikipedia.cz a zpět) – např. přesměruje uživatele na falešnou webovou stránku nebo umožní přístup k webové stránce neoprávněnému uživateli.

<sup>70</sup> Tzv. odepření služby (Denial-of-Service) a distribuované odmítnutí služby (Distributed-Denial-of-Service), kdy je zjednodušeně řečeno napadený server zahlcen takovým množstvím přístupů, že v důsledku toho přestane fungovat.

<sup>71</sup> Případně dle ust. § 230 odst. 2 písm. a) i d) TZ.

<sup>72</sup> Blíže ke kyberšikaně viz např. SHARIF, S. *Confronting cyber-bullying: what schools need to know to control misconduct and avoid legal consequences*. Cambridge: Cambridge University Press, 2009; KO-LÁR, M. *Nová cesta k léčbě šikaný*. Praha: Portál, 2011; LIVINGSTONE, S., HADDON, L., GÖRZIG, A., ÓLAFSSON, K. *EU Kids Online final report*. The London School of Economics and Political Science, 2011.

Zvláštní skupinu tvoří jev zvaný kybergrooming, tedy psychická manipulace oběti zpravidla za účelem jejího sexuálního zneužití. Obětí, a tedy i následným poškozeným bývá nejčastěji dítě, vzhledem k přirozené naivitě a snazšímu vzbuzení důvěry, avšak objevují se i případy dospělých osob, obvykle hledajících spřízněnou duši prostřednictvím internetových seznamek, chatů a sociálních sítí. Podstata kybergroomingu spočívá ve vyhlédnutí oběti pachatelem, vytvoření falešné identity pachatele tak, aby odpovídala předpokládané představě oběti o důvěryhodné osobě a následný kontakt udržovaný i měsíce s úmyslem vybudovat její důvěru (již to může zakládat např. trestný čin znásilnění dle ust. § 185 odst. 1, 2 písm. b), eventuálně odst. 1, 3 písm. a) TZ spáchaný ve stadiu přípravy). V průběhu tohoto období pachatel mámi z oběti citlivé informace a může se tím dopustit např. trestného činu poškození cizích práv dle ust. § 181 TZ. Vzhledem k tomu, že se stoupající důvěrou oběti si s ní pachatel obvykle začne vyměňovat pornografické fotografie či videa a mnohdy i vyláká z oběti její vlastní fotografie (zpravidla vybízí oběť k sextingu),<sup>73</sup> může svým jednáním naplnit skutkovou podstatu trestného činu ohrožování výchovy dítěte, šíření pornografie, výroby a jiného nakládání s dětskou pornografií a trestného činu zneužití dítěte k výrobě pornografie spočívajícího např. ve zlákáni dítěte k výrobě pornografie.<sup>74</sup>

To vše činí kybergroomer s cílem vylákat oběť na osobní schůzku. Pokud oběť odmítá, kybergroomer se často uchýlí k trestnému činu vydírání dle ust. § 175 TZ. (např. hrozí zveřejněním získaných kompromitujících materiálů). Na osobní schůzce dojde obvykle k různým formám sexuálních praktik.<sup>75</sup> Pokud se pachatel při osobní schůzce dopustí nějakého trestného činu, nejčastěji jde o trestný čin znásilnění (ust. § 185 TZ), sexuálního nátlaku (ust. § 186 TZ), pohlavního zneužití (ust. § 187 TZ), svádění k pohlavnímu styku (ust. § 202 TZ), ale také zneužití dítěte k výrobě pornografie (ust. § 193 TZ) ve spojení s výrobou a jiným nakládáním s dětskou pornografií (ust. § 192 TZ), poškození cizích práv (ust. § 181 TZ), ohrožování výchovy dítěte (ust. § 201 TZ), obchodování s lidmi (ust. § 168 TZ), zbavení (ust. § 170 TZ) nebo omezování osobní svobody (ust. § 171 TZ), vydírání (ust. § 175 TZ), útisku (ust. § 177 TZ).

V médiích<sup>76</sup> se lze setkat i s širším pojetím kybergroomingu, za který je někdy obecně považována jakákoliv komunikace mezi vzájemně se neznajícím dospělým a dítětem na sexuální téma – typicky dospělý navštíví internetovou seznamku, osloví některé z přítomných dětí a záhy stočí rozhovor na sexuální téma. V takových případech mnohdy ani neskrývá svůj věk, motivaci atp. a vyhledává pouze jednorázové pobavení se, nespolupracující dítě dále neobtěžuje. Jde tak nepochybně o výrazně méně závažné jednání – dítě není skrytě manipulováno, není lákáno k osobní schůzce, nemusí ani dojít k vybitení k výrobě a zaslání dětské pornografie – přesto ale není takové jednání zcela bez závad. Především může být ohrožen mravní vývoj dítěte, ať už takový dospělý

<sup>73</sup> K tomu viz kap. Sexting.

<sup>74</sup> K tomu viz výše.

<sup>75</sup> Druhým možným cílem kybergroomera může být i přesvědčení oběti k provedení teroristického útoku, nicméně varianta sexuálního nátlaku v našich zeměpisných šířkách zdaleka převažuje.

<sup>76</sup> Viz např. dopolední vysílání ČR 1 Radiožurnálu dne 2. března 2012 s tématem internetu jako rizikového prostředí pro děti.

naplní znaky trestného činu ohrožování výchovy dítěte dle ust. § 201 odst. 1 písm. a) TZ (a případně i jeho kvalifikované skutkové podstaty) nebo nikoliv – i v takovém případě může sexuálně laděná komunikace mezi ním a dítětem pokřivit dítěti pohled na vlastní sexualitu a její využívání v rámci mezilidských vztahů.

#### 6.4 NÁSILNÝ AJ. ŠKODLIVÝ OBSAH

Na vývoj psychiky dítěte může mít výrazný dopad také násilný obsah, s nímž se lze na internetu setkat. Již uvedený výčet škodlivého obsahu na internetu zbývá proto doplnit o násilná videa či fotografie zachycující týrání zvířat – v těchto případech se trýznitel může stát pachatelem trestného činu týrání zvířat dle ust. § 302 odst. 1 písm. b) TZ, jedná-li např. s úmyslem zveřejnit záznam svého jednání na internetu.

Z hlediska trestněprávně relevantního jednání nesmí být dítěti zpřístupněn škodlivý obsah (vč. násilného) s úmyslem svést ho k zahálčivému nebo nemravnému životu (např. k morálnímu úpadku, trvalému záškoláctví, alkoholismu, promiskuitě, opakovanému páchání trestných činů – např. právě trestného činu týrání zvířat).

Ostatní případy zveřejňování násilného obsahu (vyjma těch zde již uvedených jako týrání zvířat, tvrdé pornografie, podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod aj.) mohou být sice protiprávní (např. zveřejnění záznamu útoku na na záznamu rozpoznatelnou oběť šikany bez jejího souhlasu), nikoliv však trestné. Jen pro úplnost uvádím ještě samostatnou kapitolu jevů zpravidla nikoliv protiprávních, které ale lze do jisté míry považovat za společensky škodlivé. Tvoří ji různé weby zaměřené na sebepoškozování, namátkou pouze zmíním weby sdružující osoby trpící poruchami příjmu potravy (mentální anorexii atp.), které de facto fungují jako platforma vzájemné podpory v daném životním stylu.<sup>77</sup>

### 7. TRESTNÍ ODPOVĚDNOST PRÁVNICKÝCH OSOB

1. ledna 2012 vstoupil v účinnost zákon č. 418/2011 Sb. ze dne 27. října 2011, o trestní odpovědnosti právnických osob a řízení proti nim, který upravuje mimo jiné podmínky trestní odpovědnosti právnických osob. Vzhledem k tomu, že některé z vybraných trestných činů, jejichž spáchání lze tzv. přičítat právnické osobě, se vztahují i ke škodlivému obsahu na internetu, je možné za takové jednání trestněprávně postihnout nejen konkrétní fyzickou osobu, ale i právnickou osobu (přičemž trestní odpovědnost právnické osoby není závislá na trestní odpovědnosti jednajících fyzické osoby a naopak).<sup>78</sup>

V souvislosti se škodlivým obsahem na internetu, jak je nastíněn výše, přichází v případě trestní odpovědnosti právnické osoby odpovědnost zejména za spáchání trestného činu obchodování s lidmi, vydírání, porušení tajemství dopravovaných zpráv, sexuálního nátlaku, pohlavního zneužití, kuplířství, výroby a jiného nakládání s dětskou pornografií,

<sup>77</sup> „Životním stylu“ z úhlu pohledu osob trpících mentální anorexií.

<sup>78</sup> Vyloučena je ovšem trestní odpovědnost České republiky a územních samosprávných celků při výkonu veřejné moci.

zneužití dítěte k výrobě pornografie, ohrožování výchovy dítěte, svádění k pohlavnímu styku, neoprávněného přístupu k počítačovému systému a nosiči informací, opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat, poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti, porušení autorského práva, práv souvisejících s právem autorským a právem k databázi, hanobení národa, rasy, etnické nebo jiné skupiny osob, podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod, podněcování k trestnému činu, projev sympatií k hnutí směřujícímu k potlačení práv a svobod člověka a popírání, zpochybňování, schvalování a ospravedlňování genocidia.

## 8. SHRnutí

Škodlivý obsah na internetu zahrnuje poměrně pestrou škálu různých jevů. Zde uvedený výčet není a ani nemůže být vyčerpávající, zejména s ohledem na překotný rozvoj informačních a komunikačních technologií včetně internetu a s tím se proměňujícím způsobem jejich využívání a na měnící se věkovou skladbu jejich uživatelů. Specifickou otázkou je také například problematika odpovědnosti poskytovatelů volného prostoru na internetu za cizí obsah a problematika odkazování na webové stránky obsahující protiprávní obsah.

Podobu nabývá škodlivý obsah na internetu různou, objevuje se např. ve formě písemné, ve formě obrázků či fotografií, zvukových záznamů, audiovizuálních záznamů i jako určité grafické zpracování.

Velmi často bývá škodlivý obsah na internetu spojen s pornografií, zpravidla ve formě obrázků či audiovizuálních záznamů. K nejzávažnějším škodlivým jednáním patří zpřístupňování dětské a tvrdé pornografie, ale i šíření prosté aj. pornografie směrem k dětem a zvláště pak mezi dětmi navzájem ve formě sextingu.

Další nezanedbatelnou oblast tvoří různé projevy extremismu spočívající na jedné straně nejčastěji v propagaci a projevech sympatií k hnutí směřujících k potlačování práv a svobod člověka, na druhé straně v samotných nenávistných projevech směřujících vůči určitým skupinám a v podněcování k nenávisti k nim.

Do širší kategorie škodlivého obsahu na internetu pak spadá dále např. porušování autorských práv (ponejvíce formou neoprávněného rozmnožování a zpřístupňování autorských děl) a porušování práva na ochranu osobnosti.

Zvláštní skupinu pak tvoří některé další škodlivé jevy související s kyberprostorem jako je sociální inženýrství a dále jednání související s kyberšikanou a kybergroomingem.

Takový je tedy velmi obecný přehled škodlivého obsahu na internetu. Jednotlivé uvedené jevy jsou zde pouze velmi obecně nastíněny, avšak každý z nich zasluhuje bližší zkoumání, a to hned v několika směrech: koho zasahuje, do jaké míry je daný jev pocíťován jako škodlivý, jak se od doby prvních výskytů proměňuje a jak se proměňuje s ohledem na rostoucí počet uživatelů internetu a nové technologické možnosti, a samozřejmě v neposlední řadě také jakým způsobem na něj pohlíží právní řád České republiky, jak lze proti němu účinně postupovat a jak mu předcházet.

## HARMFUL CONTENT ON THE INTERNET

### Summary

The article deals with the various forms of harmful content on the Internet. It briefly introduces its various forms, pornography (including sexting), extremist manifestations, copyright and rights of privacy infringement and certain other undesirable phenomena in cyberspace: social engineering, cyberbullying, cybergrooming, display of violence. It mentions crimes in connection with harmful content on the Internet, which can be committed by a legal person.

*Key words:* harmful content, cyberspace, criminal law

*Klíčová slova:* škodlivý obsah, kyberprostor, trestní právo

# TRESTNÝ ČIN PORUŠENÍ AUTORSKÉHO PRÁVA

LUKÁŠ BOHUSLAV, VLADIMÍR PELC

## 1. MEZINÁRODNÍ A EVROPSKÉ PRAMENY AUTORSKÉHO PRÁVA

### 1.1 MEZINÁRODNÍ PRAMENY PRÁVA AUTORSKÉHO

V oblasti autorského práva platí na základě čl. 10 Ústavy České republiky (dále též „Ústava“) klasická aplikační přednost mezinárodních smluv před vnitrostátními právními předpisy, tedy „*vyhlášené mezinárodní smlouvy, k jejichž ratifikaci dal Parlament souhlas a jimiž je Česká republika vázána, jsou součástí právního řádu; stanoví-li mezinárodní smlouva něco jiného než zákon, použije se mezinárodní smlouva*“. Česká republika podle čl. 1 odst. 2 Ústavy respektuje závazky, které pro ni vyplývají z mezinárodního práva. V úvodu výkladu je tak nutné zmínit mezinárodněprávní základ problematiky autorského práva tak, jak vychází z následujících mezinárodních úmluv.

- 1) Úmluva o zřízení Světové organizace duševního vlastnictví, podepsaná ve Stockholmu dne 14. července 1967. Úmluva byla vyhlášena pod číslem 69/1975 Sb., ve znění vyhlášky č. 80/1985 Sb. Jak vyplývá již z názvu Úmluvy, byla touto zřízena Světová organizace duševního vlastnictví (World Intellectual Property Organization).
- 2) Bernská úmluva o ochraně literárních a uměleckých děl, která byla uzavřena dne 9. září 1986 v Bernu. Úmluva byla uveřejněna vyhláškou č. 133/1980 Sb., ve znění vyhlášky č. 19/1985 Sb. Bernská úmluva byla mnohokrát novelizována, naposledy pak v Paříži roku 1971. Stanovuje minimální standardy ochrany autorského práva.
- 3) Všeobecná úmluva o autorském právu, která byla dohodnuta a podepsána dne 6. září 1952 ve švýcarské Ženevě. Do českého právního řádu byla implementována vyhláškou č. 2/1960 Sb., ve znění vyhlášky č. 134/1980.
- 4) Mezinárodní úmluva o ochraně výkonných umělců, výrobců zvukových záznamů a rozhlasových organizací ze dne 26. října 1961 vyhlášená pod č. 192/1964 Sb.
- 5) Úmluva o ochraně výrobců zvukových záznamů proti nedovolenému rozmnožování jejich zvukových záznamů, která byla sjednána dne 29. října 1971 v Ženevě. Tato úmluva byla vyhlášená v českém právním řádu pod č. 32/1985 Sb.

- 6) Dohoda o obchodních aspektech práv k duševnímu vlastnictví známá též pod zkratkou „TRIPS“, jež je součástí sdělení Ministerstva zahraničních věcí č. 191/1995 Sb., inkorporujícího Dohodu o zřízení Světové obchodní organizace (WTO).
- 7) Smlouva Světové organizace duševního vlastnictví o právu autorském ze dne 20. prosince 1996, přijatá v Ženevě. Smlouva vyšla ve Sbírce mezinárodních smluv jako sdělení Ministerstva zahraničních věcí č. 33/2002 Sb. m. s.
- 8) Smlouva Světové organizace duševního vlastnictví o výkonech výkonných umělců a o zvukových záznamech, přijatá taktéž 20. prosince 1996 v Ženevě, vyhlášená jako sdělení Ministerstva zahraničních věcí č. 48/2002 Sb. m. s.
- 9) Úmluvou se značným trestněprávním dosahem je *Úmluva Rady Evropy o boji proti internetové kriminalitě* (Convention on Cybercrime), uzavřená dne 23. listopadu 2001 v Budapešti. Úmluva vstoupila v účinnost dne 1. července 2004 a je prvním dokumentem trestněprávní povahy stran autorského práva. Ostatní výše zmíněné úmluvy se trestněprávními aspekty práva autorského nezabývaly. Úmluva jako první upravuje trestné činy spáchané přes internet a zabývá se mj. porušením autorského práva (dalšími oblastmi úpravy Úmluvy jsou podvody spáchané prostřednictvím počítače, dětská pornografie a narušování počítačové bezpečnosti). Úmluva se trestnými činy proti autorskému právu zabývá v čl. 10, přičemž každá smluvní strana Úmluvy je povinna přijmout opatření, kterými stanoví trestnost porušení autorského práva podle vnitrostátního práva (čl. 10 odst. 1 Úmluvy) a práv souvisejících s autorským právem (čl. 10 odst. 2 Úmluvy). Za splnění určitých podmínek smluvní strana nemusí trestní odpovědnost za jednání proti právu autorskému a právům souvisejícím s právem autorským stanovit (čl. 10 odst. 3 Úmluvy). Článek 12 Úmluvy stanoví trestní odpovědnost právnických osob. Česká republika Úmluvu podepsala, ale dosud neratifikovala. K Úmluvě byl připojen Protokol zabývající se kriminalizací činů rasistické a xenofobní povahy spáchaných za pomoci počítačových systémů, který je účinný od března roku 2006.

## 1.2 EVROPSKÁ UNIE

Předpisů Evropské unie upravujících oblast autorského práva je značné množství, proto autoři tohoto textu neaspírají na jejich kompletní výčet, přesto je vhodné alespoň nejdůležitější z nich uvést:

- 1) směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. 5. 2001 o harmonizaci některých aspektů práva autorského a práv s ním souvisejících v informační společnosti, tzv. směrnice o informační společnosti,
- 2) směrnice Evropského parlamentu a Rady 2004/48/ES ze dne 29. 4. 2004 o dodržování práv duševního vlastnictví,
- 3) směrnice Evropského parlamentu a Rady 2006/115/ES ze dne 12. 12. 2006 o právu na pronájem a půjčování a o některých právech v oblasti duševního vlastnictví souvisejících s autorským právem v oblasti duševního vlastnictví,
- 4) směrnice Evropského parlamentu a Rady 2006/116/ES ze dne 12. 12. 2006 o době ochrany autorského práva a určitých práv s ním souvisejících ve znění směrnice Evropského parlamentu a rady 2011/77/EU ze dne 27. 9. 2011.



### 1.3 OBCHODNÍ DOHODA PROTI PADĚLATELSTVÍ (ANTI-COUNTERFEITING TRADE AGREEMENT, TZV. ACTA)

V současné době je velmi aktuálním a kontroverzním tématem výše uvedená dohoda proti padělatelství, tzv. ACTA, která má vytvořit nový rámec ochrany autorských práv a jejich vynucování. ACTA by si vděk procesu svému přijímání a závažnému obsahu zaslouhovala vlastní zpracování, což vzhledem k zaměření a rozsahu článku není možné. Považujeme však za nutné seznámit čtenáře alespoň základním způsobem s trestněprávními aspekty této Obchodní dohody proti padělatelství (dále jen „Dohoda“). ACTA byla schválena dne 1. října 2011 v Tokiu 8 smluvními stranami této dohody. V České republice je v současné chvíli proces ratifikace této Dohody pozastaven. Dohoda je první mezinárodněprávní úmluvou stanovící trestněprávní prosazování v případech úmyslného padělání ochranné známky nebo porušení autorského práva nebo práv s ním souvisejících v komerčním měřítku a požadující zavedení trestního řízení a trestů (čl. 23 odst. 1 Dohody). Dohoda též požaduje ve svém čl. 23 odst. 5 trestní odpovědnost právnických osob za výše uvedená jednání. Smluvní strana je povinna stanovit tresty, které budou zahrnovat odnětí svobody a také peněžní tresty dostatečně vysoké, aby působily jako odrazující prostředek proti budoucímu porušování, a které budou odpovídat výši trestů za trestné činy odpovídající závažnosti (čl. 24). V čl. 25 Dohody je pak upraveno zabavení, konfiskace a zničení příslušných materiálů a zboží. Dohoda rovněž ukládá povinnost, aby každá smluvní strana ve svém právním řádu zajistila možnost účinných kroků vůči jakémukoli porušování práv k duševnímu vlastnictví, k němuž dojde v digitálním prostředí, včetně urychlených nápravných opatření (čl. 27 odst. 1 Dohody). Ustanovením budícím vážně je čl. 33 odst. 2 Dohody zakotvující, aby za účelem boje proti porušování práv k duševnímu vlastnictví smluvní strany v případě potřeby *podporovaly spolupráci mezi jejich příslušnými orgány odpovědnými za prosazování práv k duševnímu vlastnictví včetně trestněprávní prosazování a opatření na hranicích*, na něž se vztahuje Dohoda.

## 2. TRESTNĚPRÁVNÍ ÚPRAVA

Současný trestní zákoník upravuje dva trestné činy, které se přímo týkají porušování autorských a příbuzných práv. Jde o trestný čin porušení autorského práva, práv souvisejících s právem autorským a práv k databázi podle ustanovení § 270 (dále též „trestný čin porušení autorského práva“) zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů (dále též „TrZ“), a trestný čin padělání a napodobení díla výtvarného umění podle ustanovení § 271 trestního zákoníku. Zákon č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů, účinný do 31. 12. 2009, upravoval v ustanovení § 152 pouze první ze jmenovaných trestných činů. Oproti předešlému trestnímu kodexu obsahuje ten současný tedy speciální trestný čin padělání a napodobení díla výtvarného umění. Páchání tohoto trestného činu není přímo závislé na existenci kyberprostoru, nelze jej podřadit pod pojem kyberkriminality, a proto se jím nebudeme v tomto článku zabývat.

V zahraničí se můžeme z hlediska legislativně technického setkat s různými, někdy odlišnými koncepcemi trestněprávní ochrany autorských a příbuzných práv. Například italská a švýcarská právní úprava vymezují trestné činy přímo v autorském zákoně.<sup>1</sup> Tímto způsobem dochází k tříštění trestněprávní úpravy. Za přínos lze považovat, že zákonodárce neužije blanketní dispozice, ačkoliv její zřetelnou výhodou je, že při každé změně autorského zákona nemusí současně docházet k novelizaci trestního zákoníku. Zkoumané zahraniční úpravy se vyznačují někdy také větší propracovaností skutkových podstat a odstupňováním jednotlivých jednání ohrožujících nebo porušujících autorská práva z hlediska míry závažnosti protiprávního jednání. *Ipsa facto* tím dochází k omezení volného uvážení soudce, což lépe vyhovuje formálnímu pojetí trestného činu a zásadě zákonnosti. U blanketních dispozic může úprava narážet na požadavek určitosti trestněprávní normy (*nullum crimen sine lege certa*), což může být i případ autorskoprávní ochrany v trestním zákoníku.<sup>2</sup> Stejně řešení jako český zákonodárce přijal i zákonodárce slovenský, který v ustanovení § 283 zákona č. 300/2005 Z. z., trestný zákon, upravuje trestný čin „porušovanie autorského práva“. Trestněprávní ochranu autorských práv obsahuje v trestním kodexu např. i úprava španělská (viz čl. 270–272 španělského trestního zákoníku).<sup>3</sup>

## 2.1 TRESTNÝ ČIN PORUŠENÍ AUTORSKÉHO PŘÁVA

Skutkovou podstatu trestného činu porušení autorského práva obsahoval i předešlý trestní kodex v ustanovení § 152, jak jsme již uvedli výše. Oproti dřívější právní úpravě došlo ke změně rubriky trestného činu tak, že slovo „porušování“ bylo správně nahrazeno dokonavým tvarem tohoto slovesa („porušení“). K naplnění předmětné skutkové podstaty totiž stačí i pouhé jedno porušení autorského zákona.

Úprava ustanovení § 152 odst. 1 předešlého trestního zákona byla přejata s drobnými změnami. Na první pohled je odlišná formulace základní skutkové podstaty, kde se nově výslovně požaduje, aby zásah do zákonem chráněných práv byl větší než nepatrný (srov. „Kdo neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv [...]“). S ohledem na opuštění formálně-materiální či materiálně-formální definice trestného činu (srov. § 3 odst. 2 zákona č. 141/1961 Sb.) a její nahrazení definicí formální (viz § 13 odst. 1 TrZ), která je doplněna explicitním vyjádření zásady subsidiarity trestní represe (viz § 12 odst. 2 TrZ) je otázkou, zda přijetím nového trestního zákoníku došlo či nedošlo k částečné dekriminalizaci protiprávního jednání, které zasahuje do autorských práv, práv souvisejících s právem autorským a práv k databázi. Zodpovězení této otázky má praktický význam v případě, že by bylo v současné době z hlediska trestnosti posuzováno protiprávní jednání, které se pachatel trestného činu dopustil

<sup>1</sup> Italská úprava je obsažena v čl. 170 až 174 – *quienques* zákona o ochraně autorských práv a práv souvisejících s právem autorským (Protezione del diritto d'autore e di altri diritti connessi al suo esercizio) ze dne 22. dubna 1941, vyhlášeném ve sbírce zákonů dne 16. července 1941 pod č. 166 (G. U. n. 166 del 16 luglio 1941) – text dostupný na [http://www.interlex.it/testi/141\\_633.htm](http://www.interlex.it/testi/141_633.htm). Švýcarská úprava je obsažena v čl. 67 až 73 zákona o právu autorském a právech příbuzných ze dne 9. října 1992, účinný od 1. července 1993. Text dostupný na <http://www.admin.ch>.

<sup>2</sup> K tomu srov. rozhodnutí Ústavního soudu ČR ze dne 12. října 2006, sp. zn. I. ÚS 69/06.

<sup>3</sup> Ústavní zákon č. 10/1995 ze dne 22. listopadu 1995, trestní zákoník (Código penal), dostupný např. na <http://www.congreso.es>.

do 31. prosince 2009. Trestní právo je totiž postaveno na zásadě, kdy trestnost činu se posuzuje podle zákona účinného v době, kdy byl čin spáchán; pouze v případě, že pozdější zákon je pro pachatele příznivější, postupuje se podle zákona pozdějšího (viz § 2 odst. 1 TrZ). Podle názoru Nejvyššího soudu České republiky (dále též „NS ČR“) není ustanovení § 270 odst. 1 TrZ pro pachatele příznivější než ustanovení § 152 odst. 1 zákona č. 140/1961 Sb., byť základní skutková podstata je formulována odlišným způsobem a vyžaduje pro posouzení trestnosti zásah do zákonem chráněných práv v nikoli nepatrném rozsahu. Důvodem je prý skutečnost, že dřívější trestní kodex obsahoval ustanovení § 3 odst. 2, podle něhož za trestný čin nebylo možno považovat čin, jehož stupeň nebezpečnosti pro společnost je nepatrný, a je tak třeba dospět k závěru, že ve svém důsledku jde o ustanovení, která trestnost určitého jednání posuzují ve výsledku stejně.<sup>4</sup> Nejvyšší soud tak popsanou změnu vnímá pouze jako reakci na ústup zákonodárce od dřívějšího formálně-materiálního či materiálně-formálního pojetí trestného činu, které bylo nahrazeno ne zcela jasnou koncepcí založenou na formální definici trestného činu. Podle našeho názoru však nelze k uvedenému problému přistupovat takto scholasticky a výklad, který by u trestného činu *de facto* vylučoval použití zásady subsidiarity trestní represe, jak ji vyjadřuje § 12 odst. 2 TrZ, je nutné per *argumentum ad absurdum* odmítnout. Náš názor podporuje také skutečnost, že rozsah zásahu do autorských práv nemusí být v konkrétním případě shodný se stupněm společenské škodlivosti (nebezpečnosti). Stupeň společenské škodlivosti je totiž určován např. i způsobem provedení činu, mírou zavinění pachatele, pohnutkou, cílem. Podle našeho názoru je tedy teoreticky možné, aby zásah do autorských práv byl větší než nepatrný, ale vzhledem k dalším okolnostem, rozhodným pro určení společenské škodlivosti, se nejednalo o čin společensky škodlivý. Pokud by navíc v konkrétním případě postačovalo uplatnění odpovědnosti podle jiného (mimotrestního) právního předpisu, trestní odpovědnost pachatele by se neuplatnila (srov. § 12 odst. 2 TrZ).<sup>5</sup>

Další změnou u trestného činu porušení autorského práva je stanovení dalších zvlášť přitěžujících okolností v odstavci 2, kterými jsou „způsobení značné škody jinému“ a okolnost, že „čin vykazuje znaky obchodní činnosti nebo jiného podnikání“, a vytvoření nové kvalifikované skutkové podstaty, kde okolnostmi podmiňujícími použití vyšší trestní sazby jsou „získání pro sebe nebo pro jiného prospěch velkého rozsahu“, „způsobení jinému škody velkého rozsahu“ a „spáchání činu ve velkém rozsahu“ (viz § 270 odst. 3 TrZ).

Z hlediska nově zavedené bipartice je trestný čin porušování autorských práv podle ustanovení § 270 TrZ přečinem. Dispozice skutkové podstaty tohoto trestného činu je blanketní povahy, tzn., že odkazuje na normu nebo více norem určitého druhu. Tato legislativní technika je v českém právu častá právě u trestných činů hospodářských. V tomto případě je obsah dispozice stanoven normami autorského práva, které

<sup>4</sup> Viz rozhodnutí NS ČR ze dne 19. října 2010, sp. zn. 5 Tdo 1146/2010.

<sup>5</sup> Srov. přestupky a jiné správní delikty podle § 105a až 105c autorského zákona. Tato ustanovení byla do autorského zákona včleněna zákonem č. 216/2006 Sb. s účinností od 22. května 2006. Došlo tak k přesunutí a rozšíření správně právní ochrany autorského práva. Dosavadní úprava v ustanovení § 32 odst. 1 písm. a) přestupkového zákona byla zrušena. Nová právní úprava kromě rozšíření své působnosti též zpřísnila sankce. Dochází tak k částečné dekriminalizaci a rozšiřuje se možnost uplatnění zásady subsidiarity trestní represe.

je upraveno v zákoně č. 121/2000 Sb., autorský zákon, ve znění pozdějších předpisů (dále též „AutZ“). Výklad skutkové podstaty musí proto vycházet ze znalosti povahy autorského práva. Zejména je nezbytné mít na paměti, že *autorský zákon odpovídá dualistickému pojetí autorského práva, které se chápe jako celek práv osobnostních a práv majetkových*.<sup>6</sup> *Specifičnost osobnostních práv, jež jsou nepřevoditelná a autor se jich nemůže vzdát, má vliv např. na vymezení objektu trestného činu a na aplikaci institutu svolení poškozeného, které je možné pouze v případě zájmů, o nichž tato osoba může bez omezení oprávněně rozhodovat* (viz § 30 odst. 1 TrZ). Autorské právo sice vychází ze zásady nepřevoditelnosti autorských práv, včetně práv majetkových, avšak tato nepřevoditelnost má u osobnostních práv jinou kvalitu. *U autorských práv, která mají majetkovou povahu, je totiž možné udělení oprávnění k výkonu těchto práv* (např. na základě licenční smlouvy). Blanketní dispozice pro soud v praxi znamená povinnost ve výroku o vině uvést, *jaké konkrétní ustanovení určitého právního předpisu* (v tomto případě autorského zákona) *obviněný porušil způsobem zakládajícím jeho trestní odpovědnost*,<sup>7</sup> neboť ve výroku o vině je vždy nutné uvést všechny znaky skutkové podstaty.<sup>8</sup> Jakýkoli jiný přístup by byl zpochybněním správného a odůvodněného posouzení skutku z hlediska hmotného práva. Pro pachatele trestného činu, v souladu s principem *ignorantia iuris non excusat*, neznamená blanketní dispozice právní normy žádnou výhodu. Již prvorepubliková judikatura přímo ve vztahu k trestnému činu chránícímu autorská práva zastávala, že neznalost ustanovení zákona, zakládajících a vymežujících právo autorovo, pachatele neomlouvá.<sup>9</sup> Stejně stanovisko zastává i současná soudní praxe.<sup>10</sup> Platí tedy, že neznalost autorského zákona pachatele nevyvíňuje a posuzuje se stejně jako neznalost normy trestní (srov. ustanovení § 19 TrZ o právním omylu).

Důsledkem blanketní dispozice v trestním zákoníku je, že s každou změnou relevantních ustanovení autorského zákona se mění i obsah skutkové podstaty trestného činu.

S každou změnou právního předpisu je spojena otázka jeho časové působnosti. Trestnost činu ve smyslu 2 odst. 1 TrZ je třeba posoudit zásadně podle celého souhrnu zákonných norem trestních i mimotrestních (na něž trestní zákon odkazuje ve skutkových podstatách s blanketní dispozicí), které jsou všechny účinné ke stejnému momentu rozhodnému z hlediska časové působnosti zákona podle citovaného ustanovení.<sup>11</sup> Takovým momentem je okamžik spáchání trestného činu. Komentáře k trestnímu zákoníku<sup>12</sup>

<sup>6</sup> Tento dualismus byl do českého práva zaveden až v roce 2000. Srov. ŠEBELOVÁ, M. *Autorské právo: zákon, vzory, komentáře a judikatura*. Brno: Computer Press, 2006, s. 45–46.

<sup>7</sup> Viz např. usnesení NS ČR ze dne 24. 5. 2006, sp. zn. 5 Tdo 542/2006, publikované též pod č. 916/2006 Sb. rozh. tr. nebo usnesení NS ČR ze dne 16. května 2007, sp. zn. 5 Tdo 449/2007.

<sup>8</sup> Rozhodnutí citované v předešlé poznámce evidentně vychází z pojetí, které řadí protiprávnost mezi znaky skutkové podstaty. I kdybychom protiprávnost do rámce skutkové podstaty nezařadily, nic by to na uvedeném stanovisku nezměnilo, neboť nepochybně jde o obligatorní znak trestného činu, v tomto případě v ustanovení zvláštní částí výslovně vyjádřený.

<sup>9</sup> Viz např. rozhodnutí NS ČR ze dne 3. dubna 1925, sp. zn. Zm I 614/24, publikovaný ve sbírce Vážného pod č. 1945, sv. VII., roč. 1925, s. 184–188.

<sup>10</sup> Viz např. rozhodnutí NS ČR 2 ze dne 17. července 1996, sp. zn. 2 Tzn 46/96, publikovaný pod č. 9/1997 Sb. rozh. tr.

<sup>11</sup> Rozhodnutí NS ČR ze dne 19. března 2003, sp. zn. 5 Tdo 200/2003, publikované pod č. 3/2004 Sb. rozh. tr.

<sup>12</sup> Např. FENYK, J., HÁJEK, R., STRÍŽ, I., POLÁK, P. *Trestní zákoník a trestní řád. Průvodce trestněprávními předpisy a judikaturou*. 1. díl. Praha: Linde, 2010, s. 1006; PROUZA, D. *Trestní zákoník*. 1. vydání. Praha: C. H. Beck, 2010, s. 973; ŠÁMAL et al. *Trestní zákoník. Komentář*. 1. díl (§ 1–139). Praha: C. H. Beck, s. 2517 a 2518.

a komentář k autorskému zákonu<sup>13</sup> uvádějí jako stále aktuální soudní rozhodnutí NS ČR ze dne 12. října 2005, sp. zn. 5 Tdo 1254/2005, publikované též pod č. 53/2006 Sb. rozh. tr., a rozhodnutí NS ČR ze dne 24. 5. 2006, sp. zn. 5 Tdo 542/2006, publikované též pod č. 916/2006 Sb. rozh. tr., podle kterého za dobu, kdy byl čin spáchán, se zásadně považuje okamžik dokonání trestného činu, kterým se u trestného činu porušení autorského práva rozumí okamžik, kdy došlo k následku. Toto rozhodnutí vychází z předešlého trestního zákona, který výslovně neupravoval otázku doby spáchání trestného činu. Praxe tedy dříve preferovala teorii kritizované stanovisko,<sup>14</sup> že dobou spáchání trestného činu je okamžik dokonání trestného činu, tedy moment vzniku následku. Nový trestní zákoník se přiklonil k pojetí, podle něžž čin je spáchán v době, kdy pachatel nebo účastník konal nebo byl povinen konat, přičemž není rozhodující, kdy následek nastane nebo kdy měl nastat (§ 2 odst. 4 trestního zákoníku). Současné pojetí považujeme za správné, neboť trestem se má hrozit právě určitému protiprávnímu jednání. Doba, kdy následek nastane, může být dílem náhody a v době jednání pachatele často nelze dobu následku předvídat. Důsledkem pojetí, které za okamžik spáchání trestného činu považuje následek, resp. dokonání trestného činu, může být nedovolená retroaktivita.<sup>15</sup> Problémové mohou být případy, kdy se jednání uskuteční za účinnosti starého a následek nastane až za účinnosti zákona nového.

### 2.1.1 ZNAKY TRESTNÉHO ČINU PORUŠENÍ AUTORSKÉHO PRÁVA

#### 2.1.1.1 SUBJEKT TRESTNÉHO ČINU PORUŠENÍ AUTORSKÉHO PRÁVA

Pachatelem trestného činu porušení autorského práva může být kdokoli, hovoříme tedy o subjektu obecném. Rovněž v případě italské, slovenské, španělské a švýcarské právní úpravy se mluví o subjektu obecném.

Trestně odpovědné jsou za tento trestný čin nejen osoby fyzické, ale od 1. ledna 2012 za podmínek stanovených zákonem č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim (dále též „zTOPO“), i osoby právnické (srov. § 7 zákona o trestní odpovědnosti právnických osob).<sup>16</sup> Z hlediska postihu fyzické a právnické osoby za stejný trestný čin zakotvuje v ustanovení § 9 odst. 3 zTOPO zásadu nezávislé souběžné trestní odpovědnosti fyzických a právnických osob.<sup>17</sup> Na Slovensku se dlouhou dobu uvažovalo o zavedení právě trestní odpovědnosti právnických osob. Nakonec však byla zákonem s účinností od 1. září 2010<sup>18</sup> přijata úprava, která umožňuje v řízení proti fyzické osobě uložit fakultativně právnické osobě tato ochranná opatření: zabránění

<sup>13</sup> TELEČ, I., TŮMA, P. *Autorský zákon. Komentář*. 1. vydání. Praha: C. H. Beck, 2007, s. 888.

<sup>14</sup> Srov. např. JELÍNEK, J. et al. *Trestní právo hmotné. Obecná část. Zvláštní část*. 3. vydání. Praha: Linde, 2008, s. 53–54 nebo NOVOTNÝ, O., VANDUCHOVÁ, M. et al. *Trestní právo hmotné. Obecná část*. 5. vydání. Praha: ASPI, 2007, s. 94; opačně např. ŠÁMAL, P., PŮRY, F., RIZMAN, S. *Trestní zákon. Komentář*. 1. díl. 6. vydání. Praha: C. H. Beck, 2004, s. 148.

<sup>15</sup> Tato otázka je podrobně rozebrána v italské doktríně. Viz např. ANTOLISEI, F. *Manuale di diritto penale. Parte generale*. 4. edizione. Milano: Giuffrè, 1956, p. 75.

<sup>16</sup> K tomuto BOHUSLAV, L.: K rozsahu kriminalizace trestní odpovědnosti právnických osob. *Kriminalistika*, č. 3, 2011, s. 161–169.

<sup>17</sup> Srov. JELÍNEK, J., HERCZEG, J. *Zákon o trestní odpovědnosti právnických osob a řízení proti nim. Komentář s judikaturou*. Praha: Leges, 2012, s. 80.

<sup>18</sup> Zákon č. 224/2010 Z. z., kterým sa mení a dopĺňa zákon č. 300/2005 Z. z., trestný zákon v znení neskorších predpisov a o zmene a doplnení niektorých zákonov.

peněžité částky a zabrání majetku. Tyto sankce mají *de facto* povahu trestně či administrativně právní. Právníkům osobě však za trestný čin porušování autorského práva podle § 283 slovenského trestního zákoníku lze uložit jen sankci spočívající v zabrání peněžité částky (§ 58 odst. 2 a 3 *a contrario*). Jejich uložení není vázáno na odsouzení fyzické osoby, podmínkou je existence trestného činu či činu jinak trestného, který se dostal alespoň do stádia pokusu, nebo jestliže došlo k účasti na tomto činu (srov. § 83a, 83b a 438c slovenského trestního zákoníku). Můžeme tedy hovořit o nepravé trestní odpovědnosti právnických osob. Za pachatele trestného činu může být na Slovensku prohlášena pouze fyzická osoba. Španělský trestní zákoník, ačkoliv od roku 2010 zná pravou trestní odpovědnost právnických osob,<sup>19</sup> nečiní právnické osoby za trestné činy související s duševním vlastnictvím trestně odpovědné.<sup>20</sup> Do švýcarského trestního zákoníku byla trestní odpovědnost právnických osob zavedena s účinností od 1. října 2003. Zde mohou být za trestné činy stanovené v autorském zákoně právnické osoby odpovědné tehdy, když z důvodu nedostatečné vnitřní organizace v rámci právnické osoby nelze určité jednání přiřítat konkrétní fyzické osobě (srov. čl. 102 odst. 1 švýcarského trestního zákoníku). Bez ohledu na trestní odpovědnost fyzické osoby jsou právnické osoby trestně odpovědné pouze za taxativně vyjmenované trestné činy, např. praní peněz (viz čl. 102 odst. 2 švýcarského trestního zákoníku). Ve Švýcarsku je tak trestní odpovědnost právnických osob za trestné činy proti právu autorskému pouze subsidiární.<sup>21</sup>

#### 2.1.1.2 OBJEKTIVNÍ STRÁNKA TRESTNÉHO ČINU PORUŠENÍ AUTORSKÉHO PRÁVA

Objektivní stránku trestného činu charakterizuje zejména jednání, následek a příčinný vztah mezi nimi.

Jednání spočívá v *konání*<sup>22</sup> pachatele, který neoprávněně zasáhne více než nepatrně (nikoli nepatrně) do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi.

Z hlediska trestněprávního je významná ochrana, kterou autorský zákon poskytuje:

- 1) autorským právům, čili právům autora k jeho autorskému dílu (hlava I, § 2 až 66 AutZ),
- 2) některým právům souvisejícím s právem autorským (hlava II, § 67 až 87 AutZ),<sup>23</sup> kterými jsou:
  - práva výkonného umělce k jeho uměleckému výkonu (§ 67 a násl. AutZ),
  - právo výrobce zvukového záznamu k jeho záznamu (§ 75 a násl. AutZ),
  - právo výrobce zvukově obrazového záznamu k jeho prvotnímu záznamu (§ 79 a násl. AutZ),

<sup>19</sup> Nová úprava trestní odpovědnosti právnických osob byla do španělského trestního zákoníku zakotvena s účinností od 23. prosince 2010 ústavním zákonem č. 5/2010 ze dne 22. června 2010.

<sup>20</sup> Srov. čl. 31 bis a čl. 270–272 španělského trestního zákoníku.

<sup>21</sup> Švýcarský trestní zákoník ze dne 21. prosince 1937 je v aktuálním znění dostupný na <http://www.admin.ch/>.

<sup>22</sup> Jde o tzv. komisivní delikt. Srov. KÜCHTA, J. et al. *Kurs trestního práva. Trestní právo hmotné. Zvláštní část*. 1. vydání. Praha: C. H. Beck, 2009, s. 337.

<sup>23</sup> Trestněprávní ochrana se z tzv. práv souvisejících s právem autorským nedostává právu prvního zveřejnitelce k dosud nezveřejněnému dílu, k němuž uplynula doba trvání majetkových práv a právu nakladatele na odměnu v souvislosti se zhotovením rozmnoženiny jím vydaného díla pro osobní potřebu.

- právo rozhlasového a televizního vysílatele k jeho původnímu vysílání (§ 83 a násl. AutZ),
- 3) zvláštnímu právu pořizovatele k jím pořízené databázi (hlava III, § 88 až 94 AutZ).

U autorských práv je klíčovým pojmem autorské dílo. Při jeho vymezení je třeba vycházet z ustanovení § 2 odst. 1 AutZ, podle kterého autorským dílem je dílo literární, umělecké a vědecké. Pojmovými znaky autorského díla jsou:

- výsledek tvůrčí činnosti autora,
- vlastnost díla být vnímán jako výsledek tvůrčí kategorie umění nebo vědy,
- vyjádření díla v jakékoli smysly objektivně vnímatelné podobě,
- jedinečnost výsledku tvůrčí činnosti,
- nevyloučení z rozsahu ochrany.

Otázka pojmových znaků autorského díla je otázkou právní,<sup>24</sup> neboť se vychází z abstraktních znaků stanovených v autorském zákoně. Tvůrčí (duševní) činnosti je schopen pouze člověk. Autorem (původcem) autorského díla může tedy z povahy věci být pouze fyzická osoba. Vytvoření díla není právním jednáním, ale tzv. jinou právní skutečností.<sup>25</sup> Z povahy autorských práv vyplývá, že mají nejen majetkovou, ale i osobnostní povahu. Pokud jde o práva příbuzná právům autorským, tak osobnostní povahu mají pouze práva výkonného umělce k jeho uměleckému výkonu.

Vlastnost díla být vnímán jako výsledek tvůrčí kategorie umění nebo vědy znamená, že dílo lze objektivně označit za tvůrčí zpracování myšlenky. Tato činnost může mít povahu uměleckou (zejména literární, ale např. i výtvarné, architektonické, divadelní, choreografické, pantomimické, filmové, fotografické) nebo vědeckou (činností vědeckou můžeme označit takovou činnost, která přináší nové poznatky do současného stavu vědy).<sup>26</sup> Z práv souvisejících s právem autorským pouze práva výkonného umělce mají tvůrčí charakter, jsou tedy stejně jako autorská práva jak povahy majetkové, tak povahy osobnostní. Tvůrčí charakter mohou mít i díla méně hodná našeho obdivu, např. díla pornografická. Určení, zda tyto výtvořiny mají alespoň minimální tvůrčí charakter, aby je bylo možno považovat za díla autorská, je nutné provést v každém jednotlivém případě. I autoři filmů s pornografickou tematikou mohou požívat ochrany autorských práv.<sup>27</sup> Nejčastějším místem, kde přes který dochází k rozšiřování pornografických děl, je právě kyberprostor. Není vyloučena ani tvorba těchto děl přímo prostřednictvím internetu. Pokud jde o práva související s právem autorským, tak pouze práva výkonných umělců představují tzv. tvůrčí práva.

Dílo také musí být vyjádřeno v jakékoli smysly objektivně vnímatelné podobě, tedy musí být seznatelné osobami odlišnými od autora. Tento znak vyplývá z evropské kontinentální koncepce založené na bezformálnosti autorského práva. Rozvoj internetu

<sup>24</sup> TELEČ, I., TŮMA, P. *Přehled práva duševního vlastnictví 2. Česká právní ochrana*. Brno: Doplněk, 2006, s. 25. Srov. opačně rozhodnutí Nejvyššího soudu ČR ze dne 7. 10. 1927, publikované ve sbírce Vážného, sv. IX., roč. 1926, s. 696–702.

<sup>25</sup> Srov. přiměřeně TELEČ, I., TŮMA, P. *Přehled práva duševního vlastnictví 2. Česká právní ochrana*. Brno: Doplněk, 2006, s. 25, kde se hovoří o právním úkonu. Tento termín však nový občanský zákoník opouští.

<sup>26</sup> Vědu možno označit jako soubor vědeckých poznatků. Vědeckým poznatkem pak rozumíme poznatek přinášející něco nového. Srov. např. KNAPP, V. *Vědecká propedeutika pro právníky*. Praha: Eurolex Bohemia, 2003, s. 21–22.

<sup>27</sup> Usnesení Nejvyššího soudu ČR ze dne 18. 6. 2003, sp. zn. 5 Tdo 631/2003, publikované pod č. 2/2004 Sb. rozh. tr.

ve spojení s novými technologiemi vytváří prostředí, ve kterém je možné páchat trestnou činnost zasahující do autorských a příbuzných práv v daleko větším měřítku a větší rychlostí, než je tomu mimo toto prostředí. Kyberprostor je zároveň místem, kde v současné době nejčastěji dochází k vyjádření autorských děl. Z hlediska kvantitativního není rozhodující počet vyjádření díla, např. jeho hmotné zachycení nebo takové opatření, které umožní opakovaně vyjádřit dílo v objektivně vnímatelné podobě (např. uložení na pevném disku počítače, uchování obsahu na internetu).

Výsledek tvůrčí činnosti musí být jedinečný.<sup>28</sup> Podle autorského práva je tedy vyloučeno, aby právní ochrany požívala dvě totožná, či téměř totožná díla. Jedinečnost charakterizují vlastnosti, jakými jsou původnost, novost či osobitost. U taxativně vyjmenovaných děl zákon klade na dílo zmenšené nároky z hlediska jejich jedinečnosti, proto se někdy hovoří o tzv. fiktivních dílech.<sup>29</sup> Z praktických důvodů tak činí u počítačových programů, fotografických děl a databází (viz § 2 odst. 2 AutZ). U těchto děl tedy mohou autorskoprávní ochrany požívat teoreticky i dvě téměř shodná díla. V souvislosti s pácháním trestného činu porušení autorských práv prostřednictvím počítačového programu je nutné poukázat na to, že bude zpravidla nutné udělat posudek znalce, jak obtížná je práce s takovým systémem, pokud je pro dokazování důležitá. Důvodem je, že tato oblast vyžaduje specifickou odbornost.<sup>30</sup>

Posledním pojmovým znakem, nebo přesněji řečeno negativní podmínkou, je skutečnost, že zákon nevylučuje dílo z autorskoprávní ochrany. Jde o to, že z důvodu veřejného zájmu nejsou určité výtvořiny považovány za autorská díla, ačkoli jinak splňují všechny shora vyjmenované podmínky. Těmito výjimkami z autorskoprávní ochrany jsou úřední díla, výtvořiny tradiční lidové kultury (viz § 3 AutZ). Někdy se za pojmové znaky autorského díla považuje i skutečnost, že dílo není výtvořinou nezpůsobilým autorskoprávní ochrany,<sup>31</sup> jak toto vyplývá z ustanovení § 2 odst. 6 autorského zákona. Z hlediska systematického zařazení tohoto ustanovení, jeho konstrukce (demonstrativní výčet) a výčtu výtvořin, který obsahuje, se spíše zdá, že nezpůsobilost být autorským dílem vyplývá z pojmových znaků autorského díla a nemůže tedy být sama o sobě jeho pojmovým znakem. Například skutečnost, že autorským dílem není námět díla sám o sobě nebo myšlenka vyplývá již z toho, že pojmovým znakem autorského díla je jeho vyjádření v jakékoli smysly vnímatelné podobě. Dle výslovného ustanovení zákona je autorským dílem tvůrčí zpracování již existujícího díla, včetně jeho překladu (viz § 2 odst. 4 AutZ).

Jak jsme uvedli výše, pro existenci autorského díla není rozhodující, zda je vyjádřeno trvale nebo dočasně. Stejně tak nezáleží na rozsahu, účelu a významu díla. Z historie jsou známy případy, kdy bylo zasaženo do autorských práv nevýznamných autorů a výsledkem bylo vytvoření díla, které dosáhlo velkého úspěchu.<sup>32</sup>

<sup>28</sup> Někdy se hovoří o tzv. statistické jedinečnosti. Srov. ŠEBELOVÁ, M. *Autorské právo: zákon, vzory, komentáře a judikatura*. Brno: Computer Press, 2006, s. 26.

<sup>29</sup> ŠÁMAL, P. et al. *Trestní zákoník: komentář*. 1. díl (§ 1–139). Praha: C. H. Beck, s. 2500.

<sup>30</sup> Viz též usnesení NS ČR ze dne 27. 1. 2010, sp. zn. 5 Tdo 31/2010.

<sup>31</sup> Srov. např. TELEČ, I., TUMA, P. *Přehled práva duševního vlastnictví 2. Česká právní ochrana*. Brno: Doplněk, 2006, s. 27.

<sup>32</sup> George Harrison byl soudem odsouzen k zaplacení půl milionu dolarů Ronaldu Mackovi za to, že jeho melodii písně He's So Fine použil ve své známé písni My Sweet Lord. Obhajoba Harrisona, že se „krádeže“ melodie dopustil nevědomky, by mohla obstat z hlediska trestněprávního, nikoli však občanskoprávního.



Konečně, autorským právem není chráněno pouze hotové a kompletní autorské dílo, ale i jeho jednotlivé vývojové fáze a části,<sup>33</sup> za předpokladu, že splňují podmínky podle ustanovení § 2 odst. 1 nebo odst. 2 autorského zákona (viz. ustanovení § 2 odst. 3 AutZ).

Právo výkoného umělce patří již mezi tzv. práva související s právem autorským. Jediná z této skupiny práv mají tvůrčí povahu a jsou tedy jak povahy majetkové, tak povahy osobnostní. Ostatní práva související s právem autorským, které požívají trestněprávní ochrany, vyjadřují ochranu investice do zhotovení a zpřístupnění daného nehmotného statku.<sup>34</sup> Pro vznik těchto práv není nutné, aby obsahem záznamu nebo vysílání bylo autorské dílo. Jelikož jde o typický majetek (ač nehmotné povahy), uplatňuje se zde zásada převoditelnosti, kdy lze nejen udělit licenci k výkonu těchto práv, ale je možné je převést.

Následkem se obecně rozumí ohrožení (neboli nebezpečí vzniku poruchy) nebo porušení hodnot, které tvoří objekt<sup>35</sup> trestného činu.<sup>36</sup> Podle druhu následku dělíme trestné činy na ohrožovací a poruchové. Ačkoli z názvu trestného činu („porušení“)<sup>37</sup> a z formulace skutkové podstaty („zasáhne“) se může zdát, že trestný čin porušování autorského práva je typickým trestným činem poruchovým, není tomu tak. Porušování autorského práva může mít i podobu ohrožovacího deliktu či tzv. předčasně dokonaného deliktu, neboť k jeho spáchání postačí např. pouhé neoprávněné zhotovení rozmnoženin určitého díla z jiného důvodu než pro vlastní potřebu. Takové jednání je však z hlediska své formy přípravným jednáním kupř. pro následný prodej. Tento názor podporuje i občanskoprávní doktrína, podle které „[...] autorský zákon odmítá i jednání, kterým je právo k příslušnému nehmotnému statku ohroženo, nikoli pouze porušeno“.<sup>38</sup>

### 2.1.1.3 OBJEKT TRESTNÉHO ČINU PORUŠENÍ AUTORSKÉHO PRÁVA

Objekt trestného činu je abstraktní teoretickou kategorií vyjadřující jaké právní vztahy, společenské hodnoty a zájmy jsou danou skutkovou podstatou chráněny. Určení objektu má klíčový význam pro systematické zařazení trestného činu v rámci zvláštní části trestního zákoníku. Individuální objekt je však především znakem skutkové podstaty, tzn., že čin, který by nesměřoval proti žádnému individuálnímu objektu, nemůže být trestným činem. Z hlediska důležitosti pak u konkrétního trestného činu můžeme rozlišovat objekt primární (hlavní) a sekundární (vedlejší). Česká doktrína objektu trestného činu porušení autorských práv příliš pozornosti nevěnuje. Český i slovenský trestní kodex řadí tyto trestné činy mezi trestné činy hospodářské. To by napovídalo, že objektem tohoto trestného činu je zájem na řádném fungování hospodářství. Individuální objekt tohoto trestného činu je však o něco složitější. *Zahraníční literatura správně akcentuje zejména osobnostní a majetkovou povahu autorských práv,*

<sup>33</sup> K ochraně části díla srov. rozhodnutí NS ČR ze dne 3. dubna 1925, sp. zn. Zm I 614/24, publikované ve sbírce Vážného pod č. 1945/1925, sv. VII., roč. 1925, s. 184–188.

<sup>34</sup> TELEČ, I., TŮMA, P. *Přehled práva duševního vlastnictví 2. Česká právní ochrana*. Brno: Doplněk, 2006, s. 48.

<sup>35</sup> Blíže srov. kapitolu 3.1.3.

<sup>36</sup> Viz např. JELÍNEK, J. et al. *Trestní právo hmotné*. 1. vydání. Praha: Leges, 2009, s. 167.

<sup>37</sup> Ačkoli nadpisy mohou mít interpretační význam, tak platí, že *rubrica non est lex*.

<sup>38</sup> TELEČ, I., TŮMA, P. *Přehled práva duševního vlastnictví 2. Česká právní ochrana*. Brno: Doplněk, 2006, s. 77.

tedy zájem na ochraně osobnosti a majetku poškozeného.<sup>39</sup> Tyto dva zájmy lze označit za primární objekt trestného činu porušení autorských práv. Až druhotně může být v konkrétním případě zasazen např. vnitrostátní a mezinárodní obchod, rovnováha na trhu nebo práva spotřebitelů.<sup>40</sup>

*De lege ferenda* by tedy bylo správnější, aby trestný čin porušení autorských práv byl zařazen do hlavy V. zvláštní části trestního zákoníku mezi trestné činy majetkové. Španělský trestní kodex tyto trestné činy uvádí výstižně v samostatné sekci mezi trestnými činy proti majetku a sociálně-ekonomickému pořádku.

#### 2.1.1.4 SUBJEKTIVNÍ STRÁNKA TRESTNÉHO ČINU PORUŠENÍ AUTORSKÉHO PRÁVA

Subjektivní stránka trestného činu vyjadřuje psychický (vnitřní) vztah pachatele k protiprávnímu jednání. Obligatorním znakem subjektivní stránky je zavinění, které se musí vztahovat v zásadě na všechny skutečnosti, které jsou znakem skutkové podstaty trestného činu.<sup>41</sup> Trestný čin porušení autorského práva je typickým úmyslným trestným činem, kdy nestačí pouhé zavinění z nedbalosti (srov. § 13 odst. 2 a § 270 TrZ), nutný je alespoň úmysl eventuální (*dolus eventualis*). Při nedostatku úmyslu může u fyzické osoby dojít k uplatnění správní odpovědnosti za přestupek (srov. § 105a AutZ), právnické osoby mohou být podle správního práva odpovědné (odpovědnost za jiný správní delikt) dokonce i bez ohledu na zavinění (srov. § 105b AutZ), avšak s možností liberace (srov. § 105c odst. 1 AutZ).

Slovenská a švýcarská právní úprava neobsahuje z hlediska subjektivní stránky tohoto trestného činu žádné zvláštní požadavky, jakými mohou být např. pohnutka, cíl či záměr. Naproti tomu v italské právní úpravě u některých skutkových podstat týkajících se porušování autorských práv postačí pouze eventuální úmysl, u dalších skutkových podstat však vyžaduje, aby jednání bylo vedeno s určitým cílem, kterým je podle současné úpravy zisk (prospěch).<sup>42</sup> U protiprávních jednání, která jsou postihována přísněji, je nutné, aby pachatel jednal úmyslně s cílem získat prospěch. Italská literatura v takovém případě hovoří o úmyslu specifickém (jako opak úmyslu obecného).<sup>43</sup> Španělská úprava v některých případech dokonce žádá, aby jednání bylo vedeno s úmyslem získat prospěch a zároveň způsobit újmu jiné osobě. Rozlišení jaké existuje v Itálii a ve Španělsku sice podle našeho názoru vede k jemnější trestní diferenciaci, avšak může v praxi působit problémy při dokazování.

Pro posouzení trestnosti jednání není obvykle důležité zjištění autorství autorského (např. napodobeného) díla, podstatná je především skutečnost, že pachatel úmyslně zasáhl autorská práva poškozeného.<sup>44</sup> Posuzování úmyslu je obvykle velmi obtížné. Nejvyšší soud k tomu uvádí, že *při posuzování, zda se pachatel dopustil trestného činu podle § 270 TrZ úmyslně, je třeba vycházet zejména z jeho výpovědi, z rozboru*

<sup>39</sup> Viz např. SACCO, R. et al. *Digesto delle Discipline Penalistice*. IV. Torino: UTET, 2002, s. 13–14.

<sup>40</sup> Srov. KUPKA, P. Autorské právo z pohledu práva trestního. *Trestněprávní revue*, č. 3/2003, s. 73.

<sup>41</sup> JELÍNEK, J. et al. *Trestní právo hmotné*. 1. vydání. Praha: Leges, 2009, s. 155.

<sup>42</sup> Např. pro napodobování a nedovolené rozmnožování autorského díla postačí úmysl obecný, kdežto pro naplnění skutkové podstaty neoprávněného rozmnožování počítačových programů je nutné, aby tak dotyčný činil „za účelem dosažení zisku“.

<sup>43</sup> Srov. např. SACCO, R. et al. *Digesto delle Discipline Penalistice*. IV. Torino: UTET, 2002, s. 19.

<sup>44</sup> Srov. usnesení NS ČR ze dne 15. září 2010, sp. zn. 5 Tdo 937/2010 nebo usnesení NS ČR ze dne 26. ledna 2011, sp. zn. 5 Tdo 1553/2010–36.

*jeho konkrétního jednání s přihlédnutím k motivu (pohnutce) tohoto jednání, jakož i ke všem dalším skutečnostem a okolnostem vyplývajícím z opatřených a provedených důkazů. Zavinění přitom musí zahrnovat skutkové okolnosti odůvodňující protiprávnost, a proto se musí vztahovat i na neoprávněnost zásahu do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu anebo rozhlasovému nebo televiznímu vysílání.<sup>45</sup> Možné škody vzniklé zasahováním do práv duševního vlastnictví donutily některé subjekty, zejména pak velké společnosti, jejichž zájmy jsou takovými jednáními dotčena, aby se zajímaly o ochranu svých práv samy a nenechávaly vše jen na iniciativě státní moci. Na posuzování úmyslu pachatele tedy bude mít určité vliv zjištění, jakým způsobem reagoval na oznámení poškozeného, že porušuje jeho práva, popř. jeho výzvu, aby učinil kroky k nápravě.*

### 2.1.2 TRESTY ZA TRESTNÝ ČIN PORUŠENÍ AUTORSKÉHO PRÁVA

Za spáchání trestného činu porušení autorského práva podle odstavce 1 bude pachatel potrestán trestem odnětí svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty. Naplní-li pachatel některou ze zvlášť přitěžujících okolností odstavce 2 (spáchání činu při obchodní činnosti, ve značném rozsahu nebo získání značného prospěchu či způsobení značné škody), bude pachatel potrestán odnětím svobody na šest měsíců až pět let, peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty. Trestný čin porušení autorského práva podle prvních dvou odstavců je přečinem. Kdo naplní zvlášť přitěžující okolnosti podle odstavce 3 (získání prospěchu velkého rozsahu či způsobení škody velkého rozsahu), bude potrestán odnětím svobody na tři léta až osm let. V tomto případě je trestný čin porušení autorských práv zločinem.

Za podmínek stanovených § 53 TrZ je možné uložit i další druhy trestů. Mezi těmi, které nejsou uvedeny výše, připadají v úvahu např. trest obecně prospěšných prací nebo trest domácího vězení.

Nejčastěji ukládaným druhem trestu za trestný čin porušení autorského práva trest je tzv. podmíněně odsouzení. Pokud je tento trestný čin přečinem (tzn. podle § 270 odst. 1 a 2 TrZ), mělo by být uloženo nepodmíněného trestu odnětí svobody naprosto výjimečně (srov. § 55 odst. 2 TrZ).<sup>46</sup> Soudní praxe tento požadavek plně respektuje. V roce 2011 nedošlo k uložení nepodmíněného trestu odnětí svobody a byl uložen pouze jeden trest domácího vězení za trestný čin porušení autorského práva dle § 270 trestního zákoníku. Vedle podmíněného odsouzení došlo v minulém roce k uložení trestu zákazu činnosti u více než poloviny odsouzených. V několika případech došlo k uložení peněžitého trestu a trestu obecně prospěšných prací.

Slovenská právní úprava je v trestněprávním postihu porušování autorského práva přibližně stejně přísná, jako úprava česká, a to i přesto, že obecně jsou trestní sazby za trestné činy ve slovenském právu přísnější (srov. § 283 slovenského trestního kodexu).

<sup>45</sup> Viz usnesení NS ČR ze dne 19. října 2010, sp. zn. 5 Tdo 1146/2010.

<sup>46</sup> Od 1. 12. 2011, účinnosti zákona č. 357/2011 Sb., platí pravidlo, že za trestné činy s horní hranicí trestní sazby odnětí svobody nepřevyšující pět let (dříve tři léta) se zásadně neukládá nepodmíněný trest odnětí svobody.

Španělská úprava je ve srovnání s úpravou českou a slovenskou z pohledu trestání méně přísná. Naplnění základní skutkové podstaty se trestá odnětím svobody v rozmezí šesti měsíců až dvou let (srov. § 270 španělského trestního zákoníku). Pokud je spáchán tento trestný čin při výkonu povolání, bude pachateli uložen trest odnětí svobody v rozmezí od jednoho do čtyř let; sazba od dvou do pěti let je stanovena u případů, kdy navíc ke spáchání trestného činu při výkonu povolání je naplněna některá z dalších zvlášť přitěžujících okolností, např. spáchání trestného činu za použití osoby mladší 18 let nebo v rámci organizované zločinecké skupiny (viz čl. 271 španělského trestního zákoníku). Ještě méně přísná je pak úprava švýcarská. Horní sazba u základních skutkových podstat týkajících se porušení autorského práva je jeden rok (srov. např. čl. 67 odst. 1 a čl. 69 odst. 1 švýcarského zákona o právu autorském a právech příbuzných). Trestní stíhání těchto protiprávních jednání je navíc podmíněno tzv. trestní žalobou na návrh poškozeného. Již z úřední povinnosti jsou stíhána stejná protiprávní jednání, která jsou učiněna při výkonu povolání; horní hranice trestní sazby odnětí svobody zde činí pět let (srov. čl. 67 odst. 2 a čl. 69 odst. 2 švýcarského zákona o právu autorském a právech příbuzných). Italská právní úprava je poměrně složitá a i její pouhý zjednodušený popis je vzhledem k rozsahu tohoto textu velmi obtížný. Horní hranice trestní sazby odnětí svobody činí u nejzávažnějších jednání zasahujících do autorských a příbuzných práv tři léta. Za nezbytné však považujeme uvést, že základním pravidlem pro trestání zásahu do autorských práv, ze kterého vychází italská úprava (srov. čl. 171 italského zákona o ochraně autorských práv a práv souvisejících s právem autorským), je fakt, že *jednání, která zasahují do majetkových práv, se postihují pouze peněžitým trestem, kdežto jednání, která zasahují do práv osobnostních, se alternativně postihují trestem odnětí svobody a peněžitým trestem*. Tento přístup považujeme za principiálně správný. Složitost italské úpravy vyplývá i ze skutečnosti, že zákonem č. 689/1981 došlo k dekriminalizaci těch činů (není jich mnoho), za které zákon o ochraně autorských práv a práv souvisejících s právem autorským stanoví pouze peněžitý trest či pokutu. Tato protiprávní jednání, ačkoli je upravují ustanovení v zákoně obsažené pod nadpisem s názvem „trestní ochrana a sankce“, se od té doby postihují pouze v rámci správního trestání.

### 3. ZÁVĚR

Předměty ochrany autorského práva lze považovat za velmi specifické a svižně se rozvíjející. Za snad ještě více bazální, vzhledem k charakteru oboru autorského práva, než v případě jiných právních odvětví lze považovat prameny mezinárodního práva a práva Evropské unie. Právní úprava však není schopna na pružně se vyvíjející obor a změny v něm dostatečně rychle reagovat a podchytit tyto změny tak, aby se formální úprava přizpůsobovala materiálním podmínkám. Pokud však hovoříme o vztahu trestního a autorského práva, tak trestní právo by jako prostředek „ultima ratio“ mělo trestat pouze závažnější jednání porušování autorského práva v případech společensky škodlivých, a nikoliv každé porušení norem práva autorského. Za pozitivní lze v tomto směru považovat novou úpravu v zákoně o trestní odpovědnosti právnických osob, který činí za toto porušování odpovědnou i právnickou osobu, za předpokladu, že

ji lze trestný čin přičítat (ustanovení § 8 odst. 2 zTOPO). Dle koncepce přičitatelnosti tak je na právnickou osobu kladen zcela nový požadavek obezřetného chování v politice autorských práv, a to včetně chování jejich zaměstnanců. Další vývoj trestněprávních aspektů a prosazování ochrany autorských práv naznačí, alespoň dle autorů tohoto článku, přijetí či nepřijetí Obchodní dohody proti padělatelství.

## THE CRIME OF COPYRIGHT INFRINGEMENT

### Summary

The paper deals with still hot topic of infringement of copyright law and its consequences in criminal law. International and European Union sources of copyright law and the current criminal legislation with a focus on the crime of copyright infringement are stated in the article which also follows up the penalties that can be imposed because of criminal infringement of copyright. It also includes relation to the criminal corporate liability.

*Key words:* copyright law, infringement, criminal law, criminal corporate liability

*Klíčová slova:* autorské právo, porušení, trestní právo, trestní odpovědnost právnických osob



## ZÍSKÁVÁNÍ TELEKOMUNIKAČNÍCH DAT JAKO NÁSTROJ V BOJI S INTERNETOVOU KRIMINALITOU

LENKA POŠÍKOVÁ

Internet, celosvětově propojený systém počítačových sítí, se stal součástí našeho života. Revoluce v informačních technologiích zásadním způsobem změnila svět. Důsledkem rychlého rozvoje telekomunikačních prostředků v poslední době došlo nejenom ke vzniku nových forem trestné činnosti, ale i tradiční trestné činy jsou páčány pomocí nových technologií. Internetová kriminalita už dávno není spojena jen s počítačem či notebookem. Na trh přicházejí nové technické prostředky,<sup>1</sup> které obsahují výkonné mikroprocesory a operační paměť,<sup>2</sup> takže umožňují obdobné operace. Kriminální jednání se stává dalekosáhlejším, neboť není omezeno zeměpisnými hranicemi, což navíc i komplikuje vyšetřování.

### 1. K VÝVOJI PRÁVNÍ ÚPRAVY V OBLASTI UCHOVÁVÁNÍ ÚDAJŮ O USKUTEČNĚNÉM TELEKOMUNIKAČNÍM PROVOZU

Hrozba zneužití elektronických informačních systémů k páčání trestné činnosti si vyžádala rychlou odezvu i v oblasti trestního práva procesního. Již v roce 1995 bylo Výborem ministrů přijato Doporučení č. R (95) 13, které radí členským státům přijmout odpovídající právní prostředky pro boj s internetovou kriminalitou. Jako jeden z nástrojů bylo doporučeno vložit do rukou vyšetřujících orgánů pravomoc nařídít provozovatelům telekomunikačních služeb poskytnutí potřebných dat a informací. Providerům,<sup>3</sup> kteří nabízejí telekomunikační služby pro veřejnost, ať už veřejných nebo soukromých sítí, měla být podle tohoto Doporučení uložena zvláštní povinnost poskytnout informace vedoucí k identifikaci uživatele.<sup>4</sup>

Ustanovení § 88a zákona č. 141/1961 Sb., o trestním řízení soudním (dále jen TR), zakotvující postup při získávání údajů o uskutečněném telekomunikačním provozu bylo do trestního řádu doplněno novelou č. 265/2001 Sb., s účinností od 1. 1. 2002, a to

<sup>1</sup> Novými technickými prostředky v této oblasti jsou například mobilní telefony tzv. nové generace s přístupem na internet apod.

<sup>2</sup> VOLEVECKÝ, P. K pojmu počítačová kriminalita. *Bezpečnostní teorie a praxe*, č. 4, 2008, s. 68.

<sup>3</sup> Pojmem provider se rozumí poskytovatel internetového připojení.

<sup>4</sup> Recommendation No. R (95) 13 of the Committee of Ministers to Member States, bod 12.

na základě pozměňovacího návrhu Výboru pro obranu a bezpečnost. Důvodem k novelizaci bylo několik nálezů Ústavního soudu<sup>5</sup> týkajících se práva na ochranu zpráv podávaných telefonem. Stěžovatelé se obraceli na Ústavní soud, neboť se domnívali, že způsob, kterým policejní orgán získal údaje o telekomunikačním provozu, byl nezákonný. Telekomunikační společnost tento výpis poskytla orgánům policie na základě blíže nespecifikované žádosti a bez souhlasu stěžovatele, čímž došlo k zásahu do jejich zaručených základních lidských práv a svobod.<sup>6</sup> Jádrem věci bylo posoudit, zda se čl. 13 Listiny základních práv a svobod vztahuje nejen na samotný obsah zpráv podávaných telefonem, ale i na údaje o volaných číslech, datum a čas hovoru, dobu jeho trvání atd. Ústavní soud se ve svých rozhodnutích ztotožnil s názorem Evropského soudu pro lidská práva vyjádřeným ve věci *Malone v. Spojené království*,<sup>7</sup> že „je třeba takové údaje považovat za nedílnou součást komunikace. Článek 13 Listiny nezakládá pouze ochranu tajemství vlastního obsahu zpráv, ale i tzv. vedlejších složek“. Pojem „záznam“ telekomunikačního provozu se tak vztahuje i na údaje získané jeho evidencí.

Orgány činné v trestním řízení byly napříště povinny při získávání údajů o telekomunikačním provozu postupovat přiměřeně dle § 88 TR, tedy obdobně jako při získávání odposlechu a záznamu telekomunikačního provozu.<sup>8</sup> A to do doby, než byla přijata specifická úprava opatřování těchto údajů. Ve vztahu k § 88 TR byly podmínky pro poskytnutí údajů o uskutečněném telekomunikačním provozu stanoveny o poznání benevolentněji. Za dostatečný důvod byla považována již potřeba *objasnění skutečností důležitých pro trestní řízení*.

Uchovávání provozních a lokalizačních údajů a jejich poskytování oprávněným orgánům je upraveno zákonem č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (ZEK) a do dubna roku 2011 i prováděcí vyhláškou Ministerstva informatiky č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání. Ta byla zrušena nálezem Ústavního soudu sp. zn. Pl. ÚS 24/10 vydaným 22. března 2011.

Dne 15. března 2006 byla za účelem harmonizace předpisů členských států přijata Směrnice Evropského parlamentu a Rady 2006/24/ES o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES (dále jen „směrnice o data retention“ či „směrnice o uchovávání údajů“). Pro větší flexibilitu ve vztahu ke specifikům jednotlivých právních řádů členských států byla zvolena právě forma směrnice.<sup>9</sup> Cílem harmonizace právních předpisů jednotlivých

<sup>5</sup> Např. nálezy Ústavního soudu pod sp. zn. II. ÚS 502/2000 ze dne 22. 1. 2001; sp. zn. IV. ÚS 536/2000 ze dne 13. 2. 2001 a sp. zn. IV. ÚS 78/2001 ze dne 27. 8. 2001.

<sup>6</sup> K tomu blíže: nálezy Ústavního soudu sp. zn. II. ÚS 502/2000 ze dne 22. 1. 2001.

<sup>7</sup> *Malone v. Spojenému království*, rozsudek ESLP (plenary session) ze dne 2. 8. 1984, stížnost č. 8691/79 (srov. *Klass a další proti Německu*, rozsudek ESLP (plenary session) ze dne 6. září 1978, stížnost č. 5029/71; *Kruslin proti Francii*, rozsudek ESLP (Chamber) ze dne 24. dubna 1990, stížnost č. 11801/85; *Kopp proti Švýcarsku*, rozsudek ESLP (Chamber) ze dne 25. března 1998, stížnost č. 23224/94; *Amann proti Švýcarsku*, rozsudek ESLP (Grand Chamber) ze dne 16. února 2000, stížnost č. 27798/95).

<sup>8</sup> Nálezy Ústavního soudu sp. zn. IV. ÚS 536/2000 ze dne 13. 2. 2001; stejně nálezy Ústavního soudu sp. zn. IV. ÚS 78/2001 ze dne 27. 8. 2001.

<sup>9</sup> REDING, V. The European data protection framework for the twenty-first century. *International Data Privacy Law*, 2012, roč. 2, č. 3, s. 120–121.



členských států bylo zajistit dostupnost provozních a lokalizačních údajů pro účely odhalování, vyšetřování a stíhání závažných trestných činů. Implementace směrnice do právních řádů měla být provedena do 15. září 2007, s výjimkou pro uchovávání údajů o internetové komunikaci. V tomto případě byl umožněn odklad do 15. března 2009. Česká republika svou povinnost splnila 1. září 2008, kdy zákon č. 247/2008 Sb. nabyl účinnosti. Některé státy,<sup>10</sup> a šlo především o ty, kde byla směrnice přezkoumávána tamními Ústavními soudy, však směrnici nestihly transponovat ani v prodloužené lhůtě. Její následné promítnutí do vnitrostátní úpravy pak bylo spíše projevem obavy z vysokých pokut ze strany EU.

Povinnost uchovávat technická data a na požádání je poskytnout oprávněným orgánům, však český zákonodárce poskytovatelům veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí ukládal již dříve. Bylo ale třeba implementovat některé články směrnice o data retention, k jejichž promítnutí do vnitrostátní úpravy dosud nedošlo. Jednalo se především o nově uloženou povinnost uchovávat provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány a uchovávány nebo zaznamenávány při neúspěšném pokusu o volání, což zvýšilo finanční a administrativní zátěž povinných subjektů.

Ke zpřesnění právní úpravy došlo v tom, že vyžádané údaje musí být oprávněným orgánům poskytnuty bezodkladně.<sup>11</sup> Dále byla uložena povinnost zajistit ochranu uchovávaných údajů, jejich likvidaci po uplynutí stanovené doby a evidenci případů, kdy byly údaje oprávněnými orgány vyžádány.

V původním znění odstavce 3 § 97 zákona č. 127/2005 Sb. před provedenou novelizací doba uchovávání dat nesměla být delší než 12 měsíců, v tomto směru došlo ke zpřesnění právní úpravy tak, že doba uchovávání technických dat nesmí být kratší než 6 měsíců a delší než 12 měsíců. Směrnice přitom umožňuje, aby členské státy na základě svého uvážení lhůtu k uchovávání provozních a lokalizačních údajů stanovily až na 24 měsíců, nejméně však vždy po dobu 6 měsíců. V průběhu tvorby směrnice některé státy dokonce navrhovaly lhůtu mnohem delší, v řádu několika let. Česká republika naopak zastávala stanovisko opačné, neboť byly vneseny pochybnosti o přínosnosti starších dat. Delší lhůta navíc zvyšuje administrativní zátěž operátorů a tím i náklady, které nese stát.<sup>12</sup> V pozměňovacích návrzích zákona č. 247/2008 Sb., kterým se novelizuje zákon č. 127/2005 o elektronických komunikacích, bylo původně navrhováno, aby lhůta pro uchovávání provozních a lokalizačních údajů činila nejvýše 6 měsíců.<sup>13</sup> Nakonec bylo zvoleno, jak víme, kompromisní řešení zahrnující časové

<sup>10</sup> Mezi státy, které nestihly diskutovanou směrnici transponovat v určené lhůtě, patří např. Rumunsko či Švédsko.

<sup>11</sup> Důvodová zpráva k zákonu č. 247/2008 Sb., sněmovní tisk 398/0, Novela zákona o elektronických komunikacích – EU – RJ; Poslanecká sněmovna, 2008, 5. volební období 2006–2010. Dostupná z: <http://www.psp.cz/sqw/text/tiskt.sqw?o=5&ct=398&ct1=0#prilohy>.

<sup>12</sup> Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), a některé další zákony, 2012, s. 14. Dostupná z: [http://eklep.vlada.cz/eklep/getAttachment?id=zd\\_rack8rveqpl.doc](http://eklep.vlada.cz/eklep/getAttachment?id=zd_rack8rveqpl.doc). Souladně: MARAS, M.-H. The economic costs and consequences of mass communications data retention: Is the data retention directive a proportionate measure? *European Journal of Law and Economics*, 2012, roč. 33, č. 2, s. 447–472.

<sup>13</sup> Sněmovní tisk 398/4, Pozměňovací a jiné návrhy k tisku 398/0. Poslanecká sněmovna, 2008, 5. volební období 2006–2010. Dostupný z: <http://www.psp.cz/sqw/text/tiskt.sqw?o=5&ct=398&ct1=4>.

rozmezí 6 až 12 měsíců. Vedle České republiky jsou to další tři členské státy Evropské unie, které stanovily dobu uchovávání telekomunikačních dat na nejnižší hranici, a těmi jsou Kypr, Lucembursko a Litva. Naopak nejdéle uchovávají tyto citlivé údaje v Polsku (2 roky). Jiné státy rozlišují, zda se jedná o telekomunikační údaje z mobilní/pevné sítě nebo z internetu a shodně pak pro prvně jmenovanou kategorii stanovují obecně lhůtu delší.

Po uplynutí dané lhůty musí dojít k likvidaci shromážděných dat, pokud nebyly poskytnuty oprávněným orgánům dle zvláštního předpisu nebo nejsou používány poskytovatelem telekomunikačních služeb pro vlastní potřebu. Způsob likvidace však neupravuje ani prováděcí předpis. Zákodárce providerům ukládá povinnost zničit údaje, pokud ovšem nejsou poskytnuty oprávněným orgánům. Avšak jaká je nejvyšší přípustná doba, po kterou mohou být uchovávány, v případě, že poskytnuty oprávněným orgánům jsou? Na tuto otázku odpověď dána není. Řešením by mohlo být stanovení konkrétní lhůty od vyžádání, případně údaje smazat poté, co budou poskytnuta orgánu, který si je vyžádal, nejdříve však po uplynutí šestiměsíční lhůty.

## 2. VYŠETŘOVACÍ NÁSTROJ V RUKOU OPRÁVNĚNÝCH ORGÁNŮ

Vylákání finanční hotovosti za účelem poskytnutí půjčky a její následné nevrácení, zjištění místa posledního pobytu zavražděného, určení pohybu mobilního telefonu podezřelé osoby, odhalení pachatelů loupežného přepadení i sériových krádeží vloupáním do motorových vozidel,<sup>14</sup> šíření dětské pornografie, rozpletení případu organizovaného obchodu s drogami a další trestná činnost<sup>15</sup> – to je ilustrativní výčet situací, ve kterých bylo využito informací získaných podle § 88a TŘ, jež významným způsobem přispěly k objasnění trestné činnosti. Provozní a lokalizační údaje bývají často prvotní informací, kterou policisté při vyšetřování trestného činu mají a která je rozhodující pro určení dalšího postupu policejního orgánu. Policejní orgány jsou tak při vyšetřování odkázány především na spolupráci se soukromými subjekty, tzv. providery.

Získání provozních údajů může být klíčem k odhalení pachatele trestného činu nebo alespoň místa posledního připojení k síti. Díky komunikaci pachatele s okolím je možno vystopovat IP adresu jeho PC a následně lokalizovat místo připojení k síti internet. To bude mít význam především tehdy, pokud půjde o nepfenosné zařízení. Avšak vypátrání místa připojení neznamená zároveň i najít pachatele. Identifikace pachatele jako klíčový úkol v boji proti kyberkriminalitě je velice obtížná. Důležitým pomocníkem pro vyšetřovací orgány je tzv. IP adresa.<sup>16</sup> Každé zařízení připojené k síti obdrží od poskytovatele internetu IP adresu. Bez ní se k internetu připojit nelze. Práci policejnímu orgánu ulehčí

<sup>14</sup> Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), a některé další zákony, 22. 2. 2012, s. 4, 5. Dostupná z: [eklep.vlada.cz/eklep/getAttachment?id=zd\\_rack8rveqpl.doc](http://eklep.vlada.cz/eklep/getAttachment?id=zd_rack8rveqpl.doc).

<sup>15</sup> Provozní a lokalizační údaje jsou využívány nejen při vyšetřování majetkové trestné činnosti či kriminality počítačové, ale i násilné trestné činnosti (vražda, loupež, znásilnění...) či obchodování s lidmi, šíření pornografie, kuplířství, obchodování s drogami atd.

<sup>16</sup> Značka IP je zkratkou pro Internet Protocol.

tzv. statická IP adresa, neboť v takovém případě pod touto unikátní adresou vystupuje pouze jediný počítač, což umožní stálou identifikaci majitele zařízení. Proto je pachateli dáвана přednost tzv. dynamické IP adrese. Při každém dalším připojení počítače k internetu dojde ke změně IP adresy. IP adresa či její část se může měnit v závislosti na tom, v jakém pořadí se uživatel do sítě přihlásí. Nicméně policejní orgán alespoň obdrží informaci o tom, odkud se pachatel k síti připojil. Existují však i způsoby, jak svou IP adresu skrýt.<sup>17</sup>

V souvislosti s vyšetřováním kyberkriminality vyvstává několik problémů, se kterými se musí orgány činné v trestním řízení potýkat. Jde nejen o obtíže s identifikací pachatele, ale i nestálost elektronických dat či posouzení rozsahu a dopadu trestné činnosti. Orgány činné v trestním řízení se musí vyrovnávat s nehmotnou povahou důkazních prostředků. Navíc je třeba pracovat rychle, neboť je nutné zachytit důkazy dříve, než jsou smazány, změněny či přepsány jinými informacemi. Některé provozní údaje nejsou trvale uchovávány a v paměti počítačového systému zůstanou jen po krátkou dobu.<sup>18</sup> Zničení důkazů tak může být otázka i několika vteřin – ať již jde o úmyslné odstranění dat, jejich ztrátu neopatrnou manipulací či rutinní smazání údajů, které již nemusí být uchovávány. Často se stává, že na přenosu sdělení se podílí více providerů, to ale také znamená, že klíčové provozní či lokalizační údaje týkající se dané činnosti jsou rozptýleny mezi více poskytovatelů služeb, kdy „každý má jen část skládačky“.<sup>19</sup> Tyto dílky je nutné složit, aby bylo možné vysledovat zdroj nebo naopak místa určení. V kyberprostoru jsou denně zaznamenávány, shromažďovány a případně i dále zpřístupňovány miliony dat zasahující do soukromí jednotlivce.

### 3. EFEKTIVNÍ VYŠETŘOVACÍ NÁSTROJ VERSUS PRÁVO NA SOUKROMÍ

V posledních dvou letech byly vydány dva klíčové nálezy Ústavního soudu, a to nález Pl. ÚS 24/10 ze dne 22. března 2011, publikovaný ve Sbírce zákonů pod č. 94/2011 Sb. a dále nález Pl. ÚS 24/11<sup>20</sup> (č. 43/2012 Sb.), který navazuje na právní závěry obsažené v nálezu předešlém. V prvním ze dvou výše zmiňovaných nálezů se předmětem přezkumu z hlediska souladu s ústavním pořádkem stal § 97 odst. 3 a 4 zákona č. 127/2005 Sb. o elektronických komunikacích a prováděcí vyhláška k tomuto zákonu č. 485/2005 Sb.<sup>21</sup> Bylo třeba vypořádat se s otázkou, zda plošné shromažďování a využívání provozních a lokalizačních údajů o telekomunikačním provozu v rozsahu vymezeném napadenými právními předpisy je vzhledem k užítku z těchto informací

<sup>17</sup> Pro další informace týkající se změny či skrytí IP adresy odkazují např. na: <http://czblog.cz/co-je-to-ip-adresa-jak-zmenit-ip-adresu/>.

<sup>18</sup> Council of Europe. *Convention on cybercrime*. Budapest, 23. 11. 2001. Explanatory report. Dostupné z: <http://conventions.coe.int/treaty/en/reports/html/185.htm>.

<sup>19</sup> Council of Europe. *Convention on cybercrime*. Budapest, 23. 11. 2001. Explanatory report, bod 167. Dostupné z: <http://conventions.coe.int/treaty/en/reports/html/185.htm>.

<sup>20</sup> Autorka si dovoluje upozornit, že se v některých případech můžeme setkat s nesprávným číselným označením nálezu Ústavního soudu, kdy je na místo sp. zn. Pl. ÚS 24/11 označován sp. zn. Pl. ÚS 42/2011.

<sup>21</sup> Vyhláška č. 485/2005 Sb. o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání.

plynoucímú proporcionálným zásahem do základných práv a svobod zaručených v Listine základných práv a svobod a Úmluvě o ochraně lidských práv a svobod.

Jde jen o důslednou ochranu našich základných práv a svobod, nebo si orgány činné v trestním řízení oprávněně stěžují, že jim Ústavní soud bere jeden z nejučinnějších prostředků v boji s kriminalitou? Na to nelze dát jednoznačnou odpověď.

Podle napadeného ustanovení § 97 odst. 3 a 4 zákona č. 127/2005 Sb. měly fyzické a právnické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinnost uchovávat provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejich veřejných komunikačních sítí a při poskytování jejich veřejně dostupných služeb elektronických komunikací. Zjednodušeně řečeno se tato povinnost týkala především mobilních operátorů a poskytovatelů internetového připojení, kterým zákon takto ukládal povinnost po dobu šesti až dvanácti měsíců uchovávat telekomunikační data, např. telefonní číslo volajícího a volaného, datum a čas zahájení komunikace i její délku, geografické souřadnice veřejných telefonních automatů a další údaje o telefonní, faxové či SMS komunikaci. V případě internetového spojení jde o datum a čas zahájení a ukončení připojení, IP adresu či adresu elektronické pošty odesílatele stejně jako příjemců, množství přenesených dat, informace o navštívených webových stránkách apod. Ústředním problémem jsou citlivé informace, které nám tyto digitální stopy o jednotlivých osobách prozrazují – jejich zájmy, politickou příslušnost, aktuální zdravotní stav či dokonce sexuální orientaci. Lokalizační údaje Vašeho mobilního telefonu nám zase poskytnou informace o tom kdy, kde a s kým jste se setkali. Dostaneme tak „komunikační a pohybový profil jednotlivce, z kterého lze získat nejen údaje o jeho minulých aktivitách, ale s vysokou mírou pravděpodobnosti i správně předvídat jeho aktivity v budoucnosti“.<sup>22</sup> To vše představuje významný zásah do ústavně zaručeného práva na ochranu soukromí.

Sama směrnice o data retention již od svého počátku čelí kritice i ze strany jiných členských států. K přezkumu transpozičních právních předpisů z hlediska jejich ústavnosti došlo i v Rumunsku, Německu a na Kypru. Kontrola transponujících právních předpisů stále probíhá v Polsku. Tamní ústavní soudy shledaly právní předpisy zakotvující *preventivní uchovávání dat protiústavními pro zásah do práva na soukromí. Shodně bylo právní úpravě vytykáno porušení zásady proporcionality, nedostatečné vymezení účelu uchovávání dat, vágní regulace práv a povinností, nedostatečné záruky proti zneužití či absence soudní kontroly apod.*<sup>23</sup> Právní problémy spojené s transpozicí směrnice řešilo i Bulharsko, Rakousko, Irsko<sup>24</sup> či Švédsko. The High Court of Ireland se v červenci roku 2012 obrátil na Evropský soudní dvůr a požádal jej o zodpovězení předběžné otázky, zda je směrnice 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně do-

<sup>22</sup> Nález pléna Ústavního soudu sp. zn. Pl. ÚS 24/10 ze dne 22. 3. 2011, bod 7. Publikovaný ve Sbírce zákonů jako předpis č. 94/2011 Sb. In: *Sbírka zákonů*, 2011, částka 35, s. 931–951. Dostupný z: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5908>.

<sup>23</sup> K tomu blíže: MARKOU, Ch. The Cyprus and other EU court rulings on data retention: The Directive as a privacy bomb. *Computer Law and Security Review*, 2012, roč. 28, č. 4, s. 468–475.

<sup>24</sup> K vývoji irské právní úpravy ukládání telekomunikačních dat a problémů s tím spojených odkazují na: MCINTYRE, T. J. Data retention in Ireland: Privacy, policy and proportionality. *Computer Law and Security Review*, 2008, roč. 24, č. 4, s. 326–334.

stupných služeb elektronických komunikací služeb nebo veřejných komunikačních sítí v souladu s právem Evropských společenství.<sup>25</sup>

I přes vyjmenované nedostatky trvá Evropská komise na transpozici dotčené směrnice k zajištění plného souladu s pravidly EU. Ve většině zemí nakonec k provedení směrnice došlo. Například rumunskému parlamentu byl předložen nový návrh zákona transponující směrnici o data retention. Tento návrh byl v prosinci roku 2011 nejdříve projednán senátem,<sup>26</sup> který jednomyslně rozhodl o jeho zamítnutí. Dolní komorou rumunského parlamentu byl však zákon přijat. Za přijetím zákona se pravděpodobně skrývá obava z vysokých sankcí ze strany EU v případě neprovedení směrnice.<sup>27</sup> Vedle Rumunska došlo k přijetí transponujícího právního předpisu také ve Švédsku. Poté, co Evropská komise proti Švédsku vznesla stížnost u ESD a hrozilo uložení vysoké pokuty, transponující předpis byl tamním parlamentem v březnu 2012 přijat.<sup>28</sup> Evropská komise uvažuje, že podá u Evropského soudního dvora žalobu za nesplnění povinnosti v podobě promítnutí směrnice do národního právního řádu i proti Německu.<sup>29</sup> Německo sice původně zákon transponující směrnici o data retention v listopadu 2007 zavedlo, nicméně měsíc poté byla proti tomuto právnímu předpisu vznesena ústavní stížnost, které německý Ústavní soud 2. března 2010 vyhověl a předpis zrušil. Německý ústavní soud byl doslova zaplaven vlnou individuálních stížností proti implementaci směrnice 2006/24/EC do vnitrostátní úpravy. Uvádí se, že ústavní stížnost podalo 34 000 jednotlivců.<sup>30</sup>

Po vydání nálezu Pl. ÚS 24/10 byl Ústavnímu soudu dne 27. května 2011 doručen návrh Obvodního soudu pro Prahu 6 na zrušení § 88a TŘ. Ústavní soud rozhodl o zrušení předmětného ustanovení trestního řádu k 30. září 2012. Ministerstvo vnitra ve spolupráci s Ministerstvem spravedlnosti a Ministerstvem průmyslu a obchodu začalo připravovat novelu trestního řádu ještě před derogací § 88a TŘ nálezem ÚS vydaného pod č. 43/2012 Sb. Zákonomárcé měli upravit tento právní nástroj tak, aby splnil test proporcionality<sup>31</sup> a požadavek předvídatelnosti, jak to vyžaduje Ústavní soud pro zachování ústavní konformity. Zejména jedná-li se o automatické zpracování údajů patřících pod ochranu článků 10 odst. 3 a 13 Listiny i článku 8 Evropské úmluvy o ochraně lidských práv a svobod. „Právo na soukromí taktéž garantuje právo jednotliv-

<sup>25</sup> Do data uzavření rukopisu nebyla předběžná otázka Evropským soudním dvorem zodpovězena.

<sup>26</sup> Návrh zákona je v Rumunsku vždy nejdříve projednán horní komorou Parlamentu a až následně je předložen dolní komoře.

<sup>27</sup> Romanian Parliament Adopts The Data Retention Law. Again. *Digital Civil Right*. Květen 2012. Dostupné z: <http://www.edri.org/edriagram/number10.10/romanian-parliament-adopts-data-retention-law-again>.

<sup>28</sup> Swedish parliament passes controversial data storage bill. *EUbusiness*. Březen 2012. Dostupné z: <http://www.eubusiness.com/news-eu/sweden-telecom.ft>.

<sup>29</sup> Commission still seeking proof of the necessity of mandatory data retention. *Statewatch organization*. Leden 2012. Dostupné z: <http://www.statewatch.org/news/2012/jan/09eu-pnr.htm>.

<sup>30</sup> HORNUNG, G., SCHNABEL, Ch. Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention. *Computer Law and Security Review*, 2009, roč. 25, č. 2, s. 115–122.

<sup>31</sup> Nález pléna Ústavního soudu sp. zn. Pl. ÚS 24/10 ze dne 22. 3. 2011, bod 37. Publikovaný ve Sběrce zákonů jako předpis č. 94/2011. In: *Sbírka zákonů*. 2011, částka 35, s. 931–951. Dostupný z: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5908>. Test proporcionality zahrnuje tři kritéria. Zda je daný prostředek schopen dosáhnout zamýšleného cíle, zda se jedná o prostředek k základnímu právu nejšetřejší a v neposlední řadě je třeba zkoumat přiměřenost v užším smyslu. Tedy zda pozitiva, která z toho zásahu plynou, převáží negativní důsledky spojené se zásahem do základních lidských práv.

*ce sám rozhodnout, zda a v jakém rozsahu, jak a za jakých okolností mají být informace z jeho soukromí zpřístupněny jiným subjektům.*<sup>32</sup>

Zároveň byly začátkem ledna 2012 zahájeny práce na přípravě nového prováděcího předpisu na místo zrušené vyhlášky č. 485/2005 Sb. Prováděcí předpis blíže upravuje nejen rozsah a formu uchovávaných provozních a lokalizačních údajů, způsob jejich předávání oprávněným orgánům, ale i způsob likvidace těchto citlivých dat,<sup>33</sup> což v minulé prováděcí vyhlášce chybělo.

#### 4. CO PŘINESLA NOVELIZOVANÁ ÚPRAVA

Obecně se zpřísňují podmínky pro získání příkazu k zjištění provozních a lokalizačních údajů. Zákonodárce tak reaguje na výtky Ústavního soudu, který shledal § 88a TŘ ústavně nekonformním z důvodu neomezeného okruhu trestných činů, k jejichž objasnění lze tento vyšetřovací nástroj použít, neexistence principu subsidiarity a selhání tohoto institutu v testu proporcionality ve vztahu k zásahu do práva na informační sebeurčení, obsaženém v čl. 10 odst. 3 a čl. 13 Listiny. Pro futuro bylo nezbytné jednoznačně vymezit okruh oprávněných orgánů, zamyslet se nad délkou uchovávání provozních a lokalizačních údajů, zpřísnit pravidla pro jejich uchovávání i následnou likvidaci, zakotvit povinnost zpětně informovat uživatele o nařízeném zjišťování údajů o telekomunikačním provozu a současně možnost obrátit se na příslušný soud s žádostí o přezkum, zda nedošlo v daném případě ke zneužití tohoto institutu.

Směrnice o data retention pracuje s pojmem „závažné trestné činy“, aniž by jej definovala. Toto vymezení se neshoduje s žádnou kategorií trestných činů v § 14 odst. 3 trestního zákoníku. Zůstalo tak na zákonodárci, aby sám vymezil, co pokládá za tzv. závažný trestný čin. Ústavní soud zákonodárci vytkl, že tak v původním znění ustanovení § 88a TŘ činil příliš vágně. Ústavní soud se navíc vyslovil, že je nezbytné, aby možnost použití uchovávaných údajů byla omezena jen pro účely trestních řízení vedených pro zvlášť závažné trestné činy.<sup>34</sup> Opřel se zde o úpravu v § 88 TŘ a Směrnici o data retention. Avšak jak vyplývá z výše uvedeného, Směrnice o uchovávání údajů v tomhle směru tak striktní není a členským státům neukládá, aby použitelnost tohoto institutu omezily jen na vedení trestního stíhání pro zvlášť závažné zločiny.

V novém znění § 88a TŘ již získání příkazu k zjištění údajů o telekomunikačním provozu nestačí odůvodnit potřebností objasnit „skutečnosti důležité pro trestní řízení“. Toto vágní vymezení bylo na místo toho nahrazeno třemi skupinami trestných

<sup>32</sup> Nález pléna Ústavního soudu sp. zn. Pl. ÚS 24/10 ze dne 22. 3. 2011. Publikovaný ve Sbírce zákonů jako předpis č. 94/2011. In: *Sbírka zákonů*. 2011, částka 35, s. 931–951. Dostupný z: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5908>.

<sup>33</sup> Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), a některé další zákony, 22. 2. 2012, s. 27, 33. Dostupná z: [eklep.vlada.cz/eklep/getAttachment?id=zd\\_rack8rveqpl.doc](http://eklep.vlada.cz/eklep/getAttachment?id=zd_rack8rveqpl.doc).

<sup>34</sup> Nález pléna Ústavního soudu sp. zn. Pl. ÚS 24/10 ze dne 22. 3. 2011, bod 47, 48. Publikovaný ve Sbírce zákonů jako předpis č. 94/2011. In: *Sbírka zákonů*. 2011, částka 35, s. 931–951. Dostupný z: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5908>.

činů, k jejichž objasnění budou moci orgány činné v trestním řízení provozní a lokalizační údaje získat.

První skupinu tvoří úmyslné trestné činy, na které zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně tři roky. Jak již bylo řečeno výše, dotčená směrnice sama pojem „závažné trestné činy“ nevynechává a zůstalo tak na členských státech, aby tento pojem samy vymezily ve vztahu k svým trestněprávním předpisům. Důvodová zpráva uvádí, že horní hranice trestní sazby byla odvozena analogicky od institutu vazby jako nejintenzivnějšího prostředku trestního práva vedoucího k zbavení osobní svobody obviněného.<sup>35</sup> Ve srovnání s ostatními členskými státy tak tato hranice byla stanovena zhruba uprostřed. Stejně učinilo i Estonsko. V Irsku naopak je vedle taxativně vymezených trestných činů možné tyto údaje získat až pro trestné činy, na něž trestní zákon stanovuje trest odnětí svobody nejméně 5 let. V jiných členských státech je hranice horní hranice trestní sazby stanovena naopak níže (Maďarsko 2 roky; Lucembursko 1 rok) nebo dokonce takové omezení neexistuje a provozní a lokalizační údaje je možné žádat ve vztahu ke všem trestným činům, jakož i k prevenci trestné činnosti a obecně národní a veřejné bezpečnosti, bezpečnosti státu (Belgie, Dánsko, Francie, Itálie, Lotyšsko, Polsko, Slovensko, Slovinsko).<sup>36</sup>

Druhá skupina je stanovena taxativním výčtem jednotlivých trestných činů, jejichž objasnění by bez provozních a lokalizačních údajů bylo značně ztíženo. Pro ně výše uvedená omezení neplatí. V těchto případech pachatel často využívá ke spáchání trestné činnosti prostředků elektronické komunikace.<sup>37</sup> Jde o například o trestný čin podvodu dle § 209 TZ, porušení tajemství dopravovaných zpráv (§ 182 TZ), nebezpečné vyhrožování (§ 353 TZ), nebezpečné pronásledování (§ 354 TZ) a další trestné činy postihující počítačovou kriminalitu; trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací (§ 230 TZ), pro trestný čin opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 TZ).

Úmyslné trestné činy, k jejichž stíhání zavazuje vyhlášená mezinárodní smlouva, kterou je Česká republika vázána, jsou třetí a poslední skupinou trestných činů, u které lze vyžádat údaje o telekomunikačním provozu, jež jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat.

Příkaz k zjištění údajů o telekomunikačním provozu může být vydán jen tehdy, pokud není možné trestný čin objasnit prostřednictvím jiných důkazních prostředků. Sledovaného účelu tedy nelze dosáhnout jinak nebo by jeho dosažení bylo podstatně ztíženo. Nová úprava po vzoru § 88 TŘ zavádí princip subsidiarity.<sup>38</sup> Byť Ústavní soud netvrdí, že by znění § 88a TŘ mělo být totožné s úpravou odposlechů, v mnohém se jí

<sup>35</sup> Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), a některé další zákony, 22. únor 2012, s. 27. Dostupná z: [http://eklep.vlada.cz/eklep/getAttachment?id=zd\\_rack8rveqpl.doc](http://eklep.vlada.cz/eklep/getAttachment?id=zd_rack8rveqpl.doc).

<sup>36</sup> Evropská komise. Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES) z 18. dubna 2011, Brusel. Dostupná z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:CS:PDF>.

<sup>37</sup> Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), a některé další zákony, 22. únor 2012, s. 20. Dostupná z: [eklep.vlada.cz/eklep/getAttachment?id=zd\\_rack8rveqpl.doc](http://eklep.vlada.cz/eklep/getAttachment?id=zd_rack8rveqpl.doc).

<sup>38</sup> Srov. § 88 trestního řádu, zákon č. 141/1961 Sb., o trestním řízení soudním.

blíží. Vedle zásady subsidiarity a proporcionality byla zakotvena povinnost předsedy senátu v řízení před soudem, případně státního zástupce či policejního orgánu, byla-li věc pravomocně skončena jejich rozhodnutím, zpětně informovat uživatele o nařízeném zjišťování údajů o telekomunikačním provozu.<sup>39</sup> Z tohoto důvodu bylo třeba upravit i související ustanovení trestního řádu upravující řízení o přezkumu. Nepředpokládá se však, že by tento nový přezkumný prostředek představoval výrazné zatížení pro příslušný soud, neboť počet žádostí o přezkum u odposlechů stěžá překročí 10 případů ročně.<sup>40</sup>

Vydat příkaz ke zjištění údajů o uskutečněném telekomunikačním provozu byl před novelizací oprávněn předseda senátu a v přípravném řízení soudce. Zpravidla se tak dělo na návrh státního zástupce, byť tento postup § 88a TŘ výslovně neuváděl. Postupovalo se analogicky dle ustanovení § 88 odst. 2 TŘ. Nebylo však vyloučeno, aby v případech, které nesnesly odkladu, podal návrh na vydání příkazu i policejní orgán.<sup>41</sup> Novým zněním ustanovení § 88a TŘ došlo k zakotvení povinnosti v přípravném řízení předkládat žádost o vydání příkazu ke zjištění údajů o uskutečněném telekomunikačním provozu pouze prostřednictvím státního zástupce. Zákodárce si od toho slibuje větší uvážení při podávání návrhu na vydání příkazu. I ostatní členské státy Evropské unie podmiňují získání příkazu k zjištění provozních a lokalizačních údajů zpravidla souhlasem soudce. Ovšem není tomu tak ve všech případech. Některé z členských států stanovují podmínky přísnější, např. souhlas předsedy senátu krajského soudu,<sup>42</sup> jiné naopak svěřují tuto pravomoc i do rukou jiného orgánu než soudu.<sup>43</sup>

Z příkazu musí vyplývat, jaký druh údajů, za jaké období a za jakým účelem se vyžaduje, kterému orgánu v trestním řízení a v jaké podobě (listinné či elektronické) se poskytují. Dále se uvádí známé údaje o účastníkovi telekomunikace, ohledně něhož se dané skutečnosti sdělují.<sup>44</sup> Nově právní úprava kromě písemného odůvodnění také vyžaduje, aby bylo odkazováno na konkrétní mezinárodní smlouvu, která zavazuje ke stíhání daného trestného činu a dále se ukládá povinnost uvést totožnost uživatele, je-li známa.<sup>45</sup> V tomto směru opět napodobuje ustanovení § 88 TŘ.

<sup>39</sup> Podle důvodové zprávy bude uživateli sděleno, který soud příkaz vydal, jaká data byla poskytnuta a doba, za kterou byly provozní a lokalizační údaje vyžádány. Zároveň musí být uživatel poučen o možnosti podat návrh na přezkoumání zákonnosti příkazu, které provede Nejvyšší soud. Viz Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), a některé další zákony, 22. únor 2012, s. 21. Dostupná z: [eklep.vlada.cz/eklep/getAttachment?id=zd\\_rack8rveqpl.doc](http://eklep.vlada.cz/eklep/getAttachment?id=zd_rack8rveqpl.doc).

<sup>40</sup> Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), a některé další zákony, 22. únor 2012, s. 32. Dostupná z: [eklep.vlada.cz/eklep/getAttachment?id=zd\\_rack8rveqpl.doc](http://eklep.vlada.cz/eklep/getAttachment?id=zd_rack8rveqpl.doc).

<sup>41</sup> ŠAMAL, P. et al. *Trestní řád. Komentář*. 1. díl. 6. vydání. C. H. Beck, Praha, 2008, s. 747

<sup>42</sup> Souhlas předsedy senátu krajského soudu je vyžadován v Bulharsku. Viz Evropská komise. Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES) z 18. dubna 2011, Brusel. Tabulka č. 2, s. 10. Dostupná z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:CS:PDF>.

<sup>43</sup> V Belgii, Itálii či Nizozemsku může vydání příkazu k zjištění provozních a lokalizačních údajů povolit i státní zástupce. Viz Evropská komise. Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES) z 18. dubna 2011, Brusel. Tabulka č. 2, s. 10. Dostupná z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:CS:PDF>.

<sup>44</sup> ŠAMAL, P. et al. *Trestní řád. Komentář*. 1. díl. 6. vydání. C. H. Beck, Praha, 2008, s. 748.

<sup>45</sup> Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), a některé další zákony, 22. únor 2012, s. 28. Dostupná z: [http://eklep.vlada.cz/eklep/getAttachment?id=zd\\_rack8rveqpl.doc](http://eklep.vlada.cz/eklep/getAttachment?id=zd_rack8rveqpl.doc).



## 5. K NADUŽÍVÁNÍ § 88a TRESTNÍHO ŘÁDU

V odůvodnění nálezu Ústavního soudu Pl. ÚS 24/10 bylo negativně hodnoceno nadužívání tohoto nástroje orgány činnými v trestním řízení i k vyšetřování bagatelní trestné činnosti. Uvádí, že dle Zprávy o bezpečnostní situaci v ČR za rok 2008 bylo na území České republiky zjištěno celkem 343 799 trestných činů, z toho bylo objasněno 127 906 trestných činů. Počet žádostí o poskytnutí provozních a lokalizačních údajů činil ve stejném roce dle statistických údajů 131 560.<sup>46</sup> Statistika říká, že v Evropské unii je každoročně vzneseno více než 2 miliony takových žádostí. Počet vznesených žádostí tak ve vztahu k objasněným trestným činům je obrovský a vede k domněnce o nadužívání tohoto institutu i pro vyšetřování méně závažné trestné činnosti. Policejní statistiky se však od těch Českého telekomunikačního úřadu značně liší.<sup>47</sup> A to proto, že v České republice je třeba žádost o poskytnutí údajů o telefonní komunikaci v mobilní síti předložit všem významným mobilním operátorům, tedy minimálně třem.<sup>48</sup> Stejná žádost je pak ve statistice poskytovatelů telekomunikačních služeb evidována hned třikrát, zatímco ve statistikách policie se objeví jen jednou. Z tohoto důvodu jsou uváděná čísla zkrleslena.

Ze statistických dat<sup>49</sup> vyplývá, že orgány činné v trestním řízení nejčastěji vyžadují data, která nejsou starší víc než 3 měsíce. Jedná se o více jak 80 % z celkového počtu žádostí. Stejně závěry vykazují i jiné státy.<sup>50</sup> Data starší více jak 9 měsíců jsou vyžadována pouze sporadicky a údaje, od jejichž záznamu uběhlo víc než 12 měsíců, nejsou vyžadovány vůbec. To je však dáno tím, že legislativa umožňovala a zároveň nařizovala provozní a lokalizační údaje uchovávat nejméně po dobu 6 měsíců, nejvýše však po dobu 12 měsíců. Následně musí být tyto údaje zničeny. Nejvíce orgány činné v trestním řízení zajímají technické údaje o telekomunikaci v mobilní síti,<sup>51</sup> počet těchto žádostí několikanásobně převyšuje oblast pevné sítě i internetového prostoru. Jak již bylo zmíněno výše, je třeba vzít v úvahu, že počet případů, ke kterým byly dané údaje vyžádány,

<sup>46</sup> Nález pléna Ústavního soudu sp. zn. Pl. ÚS 24/10 ze dne 22. 3. 2011, bod 49. Publikovaný ve Sbírce zákonů jako předpis č. 94/2011. In: Sbírka zákonů. 2011, částka 35, s. 931–951. Dostupný z: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5908>. Souladně: Evropská komise. Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES) z 18. dubna 2011, Brusel, s. 35–43. Dostupná z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:CS:PDF>.

<sup>47</sup> Z důvodové zprávy k návrhu zákona, kterým se mění zákon č. 127/2005 Sb. a zákon č. 141/1961 Sb.: „Podle údajů Policie České republiky byl v roce 2010, tedy před zrušením příslušných ustanovení Ústavním soudem, celkový počet úkonů podle § 88a trestního řádu 82 639. Celkový počet spisů, k nimž byly úkony podle § 88a trestního řádu provedeny, je pak 10972.“

<sup>48</sup> Evropská komise. Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES) z 18. dubna 2011, Brusel. Dostupná z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:CS:HTML>. Souladně: Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), a některé další zákony, 22. února 2012, s. 30. Dostupná z: [eklep.vlada.cz/eklep/getAttachment?id=zdrack8rveqjpl.doc](http://eklep.vlada.cz/eklep/getAttachment?id=zdrack8rveqjpl.doc).

<sup>49</sup> Evropská komise. Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES) z 18. dubna 2011, Brusel, tabulky č. 7 a 8 na s. 34, 35. Dostupná z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:CS:HTML>.

<sup>50</sup> *Liberty and security: Striking the balance*. UK Presidency Paper, 2005, s. 1–5. Dostupné z: <http://www.edri.org/docs/UKpresidencypaper.pdf>.

<sup>51</sup> Za rok 2008 se jednalo v České republice o 125 040 žádostí o poskytnutí technických dat v mobilní síti, v pevné síti byl tento počet 4983 žádostí a na zjištění lokalizačních a provozních údajů v rámci internetové komunikace bylo vydáno žádostí 1537.

je ve skutečnosti menší, neboť žádost o poskytnutí technických dat k jednomu případu může být současně podána hned k několika mobilním operátorům.<sup>52</sup>

Komise v závěrečné části své Hodnotící zprávy o směrnici o uchovávání údajů doporučuje harmonizovat dobu povinného uchovávání dat a její případné zkrácení. Je tak možné, že ke starším technickým údajům se vyšetřovatelé trestné činnosti nedostanou již vůbec. Přitom právě u organizované kriminality, složitějších finančních deliktů, kde samotné odhalení trestného činu trvá delší dobu, či u závažnější trestné činnosti obecně hraje dostupnost starších provozních a lokalizačních údajů velmi významnou roli. Mohou totiž zachycovat přípravnou fázi trestné činnosti, její plánování, rozdělení rolí mezi jednotlivé pachatele a jejich vzájemné vztahy. Kolik pachatelů se podaří na základě provozních a lokalizačních údajů odsoudit, však zjistit nelze.

Přesto se dá říci, že hodnota uchovávaných technických údajů je pro policejní orgány nesmírná. Kromě toho, že představují indicie cenné pro vyšetřování trestných činů, vykreslují vazby mezi podezřelými a jejich role. Zároveň jsou i usvědčujícími důkazy a jindy pomohou kontaktovat svědka činu či zbavit podezření ze spáchání trestného činu nevinného, aniž by bylo třeba použít jiné operativně pátrací prostředky. V některých případech jsou dokonce jedinou stopou. Například při objasňování vyhrůzek zasílaných prostřednictvím internetových diskuzních skupin jsou provozní údaje zásadním vodítkem.

Přímo se tedy nabízí otázka, zda omezení povinnosti poskytovat provozní a lokalizační údaje nepovede ke zhoršení postavení policejních orgánů v boji s kriminalitou?

Důvodová zpráva uvádí, že úkonů podle § 88a trestního řádu bylo nejčastěji využito při šetření trestné činnosti násilné (vražda, loupež, usmrcení z nedbalosti), mravnostní (znásilnění, šíření pornografie, kuplířství), hospodářské, majetkové (krádež, vloupání do bytů, krádež motorového vozidla) a u další trestné činnosti (obchodování s lidmi, počítačová kriminalita, toxikomanie).<sup>53</sup> Avšak u většiny z těchto úmyslných trestných činů můžeme o vydání provozních a lokalizačních údajů žádat i nadále, za podmínky, že sledovaného účelu nelze dosáhnout jinak nebo bylo-li by jeho dosažení podstatně ztíženo. Trestný čin vraždy (§ 140 TZ), znásilnění (§ 185 TZ), loupeže (§ 173 TZ), kuplířství (§ 189 TZ), obchodování s lidmi (§ 168 TZ), výroba a jiné nakládání s dětskou pornografií (§ 192 TZ) stejně jako drogové delikty (§ 283, 286, 287 TZ) jsou úmyslnými

<sup>52</sup> Směrnice náhradu nákladů vznikajících v důsledku uložení povinnosti neupravuje, tuto otázku přenechává vnitrostátní úpravě. Postup a rozsah náhrady efektivně vynaložených nákladů upravuje vyhláška Českého telekomunikačního úřadu č. 486/2005 Sb. Poskytovatelé telekomunikačních služeb se mohou se svým nárokom obrátit na subjekt, který si úkon vyžádal nebo jej nařídil, zpravidla tedy Policii ČR, respektive Ministerstvo vnitra. Česká republika nahrazovala do zrušení § 97 odst. 3 a 4 nálezem Ústavního soudu jak provozní, tak kapitálové výdaje. Pro představu uvádím, že v roce 2009 Česká republika zaplatila za náhradu nákladů částku 6,8 mil. Eur. V roce 2010 Policie ČR vyčísila úhradu operátorům na více než 50 mil. Kč a v prvním čtvrtletí roku 2011 stihly náklady dosáhnout 17,4 mil. Kč. Novelizující právní úprava oproti předchozímu stavu nic nového nepřináší. Lze předpokládat, že vzhledem k omezení § 88a TR pouze na závažnější trestnou činnost budou výdaje za poskytování údajů o telekomunikačním provozu v příštích letech nižší.

Bliže k přímým a nepřímým nákladům spojeným s uchováváním údajů odkazují na publikaci: MARAS, M.-H. The economic costs and consequences of mass communications data retention: is the data retention directive a proportionate measure? *European Journal of Law and Econom*, 2012, roč. 33, č. 3; s. 447–472.

<sup>53</sup> Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), a některé další zákony, 22. únor 2012, s. 13. Dostupná z: [eklep.vlada.cz/eklep/getAttachment?id=zd\\_rack8rveqpl.doc](http://eklep.vlada.cz/eklep/getAttachment?id=zd_rack8rveqpl.doc).

trestnými činy, na které trestní zákoník stanoví trest odnětí svobody s horní hranicí nejméně tři roky a patří tedy do tzv. 1. skupiny trestných činů, u kterých je pro účely trestního řízení možné telekomunikační data podle § 88a TŘ žádat. U počítačových trestných činů pod § 230 a 231 TZ je sice horní hranice trestní sazby nižší než požadované tři roky, avšak ty patří do taxativního výčtu trestných činů v § 88a TŘ. Drogové delikty přechovávání omamné a psychotropní látky a jedu (§ 284 TZ), nedovolené pěstování rostlin obsahujících omamnou nebo psychotropní látku (§ 285 TZ) či výroba a jiné nakládání s látkami s hormonálním účinkem (§ 288 TZ) nelze zařadit ani do první či druhé vymezené skupiny, avšak v tomto případě zavazují Českou republiku ke stíhání mezinárodní smlouvy,<sup>54</sup> a proto i zde je možné telekomunikační data získat. Z výše uvedeného výčtu úmyslných trestných činů, k nimž byly podle důvodové zprávy provozní a lokalizační údaje žádány nejčastěji, tak nově není možné získat záznam o proběhnuvší telefonické či internetové komunikaci zásadně pouze u trestného činu krádeže.

Byly proto porovnány policejní statistické údaje týkající se nápadu počtu trestných činů krádeže a krádeže vloupáním za účelem zjištění, zda a jaký vliv měla novela § 88a TŘ na objasněnost tohoto druhu kriminality. Právě u drobné majetkové kriminality byl z důvodu novelizace predikován výrazný pokles objasněnosti. Srovnání nápadu a objasněnosti těchto trestných činů bylo provedeno za období 1. 1. 2012 – 1. 8. 2012<sup>55</sup> a ve stejném období v roce 2010.<sup>56</sup> Ze srovnání statistických dat překvapivě vyplynulo procentuální zvýšení objasněnosti, a to jak u krádeže vloupáním, tak i krádeže prosté, ač bych sama očekávala opačný výsledek.<sup>57</sup>

Můžeme proto dojít k závěru, že novela zpříšňující podmínky pro získání telekomunikačních dat se výraznějším způsobem nedotkne objasněnosti kriminality, neboť u většiny trestných činů je možné získat příkaz podle § 88a TŘ i nadále a ani u drobné majetkové kriminality negativní vliv *prozatím* prokázán nebyl.

## 6. K OPRÁVNĚNÝM ORGÁNŮM

Avšak které orgány jsou těmi orgány oprávněnými získat provozní a lokalizační údaje? Zrušené ustanovení § 97 odst. 3 zákona o elektronických komunikacích ukládalo povinnost operátorům poskytovat dané údaje orgánům oprávněným k jejich vyžádání dle zvláštního předpisu. Takováto formulace však v aplikační praxi vzbuzovala pochybnost, zda mezi tyto orgány patří i zpravodajské služby, konkrétně Bezpečnostní informační služba (dále jen BIS) a Vojenské zpravodajství, a to přestože zvláštní předpisy<sup>58</sup> toto oprávnění ustanovovaly. Paragraf 8 odst. 1 písm. b) zákona

<sup>54</sup> Např. Úmluva OSN proti nedovolenému obchodu s omamnými a psychotropními látkami ze dne 20. 12. 1988; Mezinárodní antidopingová Úmluva č. 57/2005 Sb. m. s.

<sup>55</sup> Aktuálnější statistická data nebyla v době uzavření rukopisu k dispozici.

<sup>56</sup> Porovnání proběhlo na základě kriminalistických statistik PČR zveřejňovaných na webových stránkách Policie České republiky. Policie České republiky. *Statistické přehledy kriminality za rok 2010, 2012*. Dostupné z: <http://www.policie.cz/statistiky-kriminalita.aspx>.

<sup>57</sup> V roce 2010 objasněnost trestného činu krádeže vloupáním činila 22,6 %, v roce 2012 pak 23,8 %. U tzv. krádeže prosté se míra objasněnosti zvýšila z 18,4 % (2010) na 22 % (2012). Není však vyloučeno, že výsledek byl ovlivněn zkreslením statistických dat.

<sup>58</sup> Zákon č. 154/1994 Sb., o Bezpečnostní informační službě, ve znění pozdějších předpisů, a zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění zákona č. 274/2008 Sb.

o Bezpečnostní a informační službě opravňuje BIS nejen k odposlouchávání a zaznamenávání telekomunikačního, radiokomunikačního a jiného podobného provozu, ale i k jeho zjišťování. V praxi tak docházelo k paradoxní situaci, kdy příslušníci BIS mohli na základě předchozího písemného povolení předsedy senátu Vrchního soudu<sup>59</sup> přímo odposlouchávat telekomunikační provoz nebo jej sami zaznamenávat, avšak získat údaje o skutečném provozu od operátorů bylo zřehla nemožné, neboť ti odmítali zpravodajským službám vyhovět s ohledem na nedostatečně vymezené oprávnění.<sup>60</sup> Předkládaný návrh zákona učinil taxativním výčtem oprávněných orgánů takovým pochybám přítrž. Právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává, je na požádání povinna je bezodkladně poskytnout orgánům činným v trestním řízení,<sup>61</sup> Policii České republiky,<sup>62</sup> Bezpečnostní informační službě a Vojenskému zpravodajství i České národní bance pro účely dohledu nad kapitálovým trhem.

Naopak Úřad pro zahraniční styky a informace jako jediná zpravodajská služba obdobné oprávnění nemá a změnu nepřinesl ani novelizující zákon č. 273/2012 Sb. A to přestože v připomínkovém řízení k návrhu zákona Úřad pro zahraniční styky a informace požadoval vložit do § 97 odst. 3 ZEK nové písmeno a současně zapracovat do zákona č. 153/1994 Sb., o zpravodajských službách nové ustanovení, které by zakotvovalo oprávnění „pro ochranu činností, které koná na území České republiky, a jestliže je to nezbytné pro plnění úkolů v jeho působnosti zjišťovat údaje o telekomunikačním, radiokomunikačním a jiném obdobném provozu“.<sup>63</sup> Tento požadavek byl odůvodňován získáním poznatků důležitých pro ochranu zájmů a bezpečnosti České republiky, zejména v oblasti boje proti terorismu.<sup>64</sup> Některé členské státy navíc svěřují toto oprávnění daňové a celní správě nebo pohraničním orgánům.<sup>65</sup>

Přitom v původním návrhu zákona č. 247/2008 Sb., kterým se novelizoval zákon č. 127/2005 Sb., byl navrhován taxativní výčet oprávněných orgánů jejich pojmenováním – v prvním návrhu stálo pouze Policie České republiky, pozměňovací návrhy vkládaly vedle PČR i státního zástupce a soud. Přijatý zákon však se od tohoto výčtu oprostil a vložil na místo toho širší pojem „oprávněným orgánům“.<sup>66</sup>

<sup>59</sup> Srov. § 9 zákona č. 154/1994 Sb., o Bezpečnostní informační službě.

<sup>60</sup> Stejně je tato situace upravena v zákoně č. 289/2005 Sb., o Vojenském zpravodajství.

<sup>61</sup> Jsou-li splněny podmínky stanovené zákonem č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů. Podmínky vymezuje § 88a TR. Co se rozumí pojmem policejní orgán, vymezuje § 12 odst. 2 TR.

<sup>62</sup> Pro účely zahájeného pátrání po konkrétní hledané nebo pohřešované osobě, zjištění totožnosti osoby neznámé nebo totožnosti nalezené mrtvoly, předcházení nebo odhalování konkrétních hrozeb v oblasti terorismu nebo prověřování chráněné osoby a při splnění podmínek stanovených zákonem č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

<sup>63</sup> Vypořádání připomínek k materiálu s názvem: návrh zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, a některé další zákony.

<sup>64</sup> Průběh vypořádání připomínek k návrhu zákona říká, že zásadní připomínka Úřadu pro zahraniční styky a informace byla akceptována, avšak v návrhu zákona se neobjevila.

<sup>65</sup> Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), a některé další zákony, 22. únor 2012, s. 20. Dostupná z: [http://eklep.vlada.cz/eklep/getAttachment?id=zd\\_rack8rveqlpl.doc](http://eklep.vlada.cz/eklep/getAttachment?id=zd_rack8rveqlpl.doc).

<sup>66</sup> Pozměňovací návrhy ke Sněmovnímu tisku 398; Sněmovní tisk 398/4. Poslanecká sněmovna, 2008, 5. volební období, 2006–2010. Dostupné z: <http://www.psp.cz/sqw/text/tiskt.sqw?o=5&ct=398&ct1=4>.

Pro účely výkonu dohledu nad kapitálovým trhem je tento nástroj svěřen i České národní bance.<sup>67</sup> Byť se někteří domnívají, že Česká národní banka by měla být z okruhu oprávněných orgánů vyškrtána.<sup>68</sup> Svěřit tento nástroj správním orgánům je velice neobvyklé i v porovnání s ostatními členskými státy.<sup>69</sup> Je možné pochybovat i o souladu s účelem uchovávání telekomunikačních dat dle Směrnice o data retention.<sup>70</sup> Tento nástroj má sloužit především k prevenci, odhalování a objasňování závažné trestné činnosti. Přesto do taxativního výčtu orgánů oprávněných získat provozní a lokalizační údaje ČNB v rámci novely § 97 odst. 3 zákona č. 127/2005 Sb. zařazena byla.

Policejní orgán má oprávnění získávat provozní a lokalizační údaje nejen pro účely trestního řízení, ale i v jiných případech. Zmocnění k vyžádání těchto dat obsahuje vedle § 88a TR i § 68 odst. 2 a § 71 písm. a) zákona o Policii ČR, a to k zahájení pátrání po konkrétní hledané či pohřešované osobě, za účelem identifikace osoby neznámé totožnosti, popř. nalezené mrtvoly a pro boj s terorismem. Další zmocnění policejního orgánu je obsaženo v zákoně č. 137/2001 Sb., o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením a o změně zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů. Za takových okolností je policejní orgán oprávněn žádat provozní a lokalizační údaje bez jakéhokoli soudního či jiného povolení. Úřad pro ochranu osobních údajů v souvislosti s novelizací institutu zjišťování telekomunikačních údajů navrhoval vrátit se ke starší úpravě a podmínit poskytnutí těchto dat souhlasem soudce krajského soudu, aby došlo ke sjednocení praxe při vydávání povolení a bylo ochráněno soukromí učiněno za dost.<sup>71</sup> Jeho připomínka však akceptována nebyla.

Přestože povinnost uchovávání provozních a lokalizačních dat byla nálezem Ústavního soudu Pl. ÚS 24/10 zrušena, operátoři těmito údaji disponovali i po tomto datu. Ovšem jen v rozsahu nezbytném pro potřeby účtování, řízení provozu, zákaznické dotazy, odhalování podvodů apod. V souvislosti s tím jim i v době po vydání nálezů Pl. ÚS 24/10 a Pl. ÚS 24/11 zůstala povinnost na žádost oprávněných orgánů provozní a lokalizační údaje poskytovat. Pokud tedy poskytovatelé telekomunikačního provozu takové údaje měli, byli povinni je na základě soudního příkazu poskytnout. Až vydáním

<sup>67</sup> Své oprávnění s největší pravděpodobností čerpá z čl. 12 odst. 2 písm. d) Směrnice Evropského parlamentu a Rady 2003/6/ES o zneužívání trhu, které stanoví, že orgán dohledu má mít pravomoc požadovat existující záznamy telefonní i o datovém provozu. Viz Vypořádání připomínek k materiálu s názvem: Návrh zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, a některé další zákony. Praha, leden 2012, s. 61.

<sup>68</sup> Legislativní rada vlády. Zmocněnkyně pro lidská práva. Vypořádání připomínek k materiálu s názvem: Návrh zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, a některé další zákony. Praha, leden 2012, s. 62, 44.

<sup>69</sup> Srovnaj s Hodnoticí zprávou Evropské komise o Směrnici o data retention. Evropská komise. Hodnoticí zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES) z 18. dubna 2011, Brusel. Dostupná z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:CS:PDF>.

<sup>70</sup> Srov. čl. 1 odst. 1 Směrnice Evropského parlamentu a Rady 2006/24/ES.

<sup>71</sup> Vypořádání připomínek k materiálu s názvem: Návrh zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, a některé další zákony. Praha, leden 2012, s. 34, 35.

onoho druhého zmiňovaného nálezu Ústavního soudu, který dnem 30. září roku 2012 zrušil ustanovení § 88a TŘ, přestaly soudu příkazy v bagatelních věcech vydávat.<sup>72</sup>

Za zamyšlení stojí otázka, jak soud naloží s údaji, které byly získány ještě před tím, než došlo k derogaci § 97 odst. 3 a 4 ZEK. Mohou být před soudem použity jako důkaz? Ústavní soud správně nechává řešení tohoto problému na obecných soudech, aby v jednotlivých případech zvážily, zda došlo k porušení základních práv dotčeného uživatele elektronických komunikací. Vydaný nálezn automaticky nevylučuje využití získaných důkazů v již probíhajícím soudním řízení. Podle mého názoru by tak soud měl v každém jednotlivém případě posoudit, zda vyžádání telekomunikačních dat vyhovuje testu proporcionality tak, jak jej definoval Ústavní soud ve svém rozhodnutí pod sp. zn. Pl. ÚS 24/10 ze dne 22. března 2011. Především by měl vzít v úvahu, zda nebylo možné sledovaného účelu dosáhnout jiným způsobem a zda zjištění, která ze získaných údajů vyplynula, dokázala převážit negativní důsledky spojené se zásahem do základních lidských práv a svobod.

## 7. ZÁVĚR

Hovoříme-li o uchovávání telekomunikačních údajů, hledáme rovnováhu mezi dvěma hodnotami – důslednou ochranou základních lidských práv a svobod na jedné straně a neméně důležitou činností orgánů spočívající v ochraně společnosti před trestnými činy na straně druhé. Právo na informační sebeurčení má jedinci garantovat kontrolu nad údaji o sobě samém a ponechat na jeho rozhodnutí, jaké informace prozradí svému sociálnímu okolí.

Soukromé subjekty poskytující telekomunikační služby tato data uchovávají v první řadě pro vlastní potřeby týkající se účtování, vyřizování zákaznických dotazů, odhalování podvodů apod. Směrnice o data retention providerům stanovuje povinnost činit tak i nadále, neboť v souvislosti s vývojovými trendy (nárůst paušálních tarifů, předplacené služby e-komunikace) přestávala být tato data ukládána a stala se tím nedostupná i pro účely odhalování, vyšetřování a stíhání trestné činnosti.<sup>73</sup> Otázka, kterou bychom si měli položit, proto nezní, zda provozní a lokalizační údaje uchovávat, nýbrž po jakou dobu a v jakých případech je oprávněným orgánům pro účely trestního řízení poskytnout.

Ačkoli je směrnice o data retention v některých ohledech nedokonalá – zmiňme kupříkladu chybějící definici pojmu „závažný trestný čin“, poměrně velký rozptyl lhůty pro uchovávání telekomunikačních dat či rozlišně vymezený okruh oprávněných orgánů v jednotlivých právních úpravách – představuje důležitý prostředek, na jehož základě má dojít ke sjednocení národních právních úprav za účelem usnadnění odhalování, vyšetřování a stíhání závažných trestných činů.

<sup>72</sup> Nález pléna Ústavního soudu sp. zn. Pl. ÚS 24/11 byl vydán dne 20. prosince 2011.

<sup>73</sup> Evropská komise. Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES) z 18. dubna 2011, Brusel, s. 5. Dostupná z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:CS:PDF>.

Evropská Unie prostřednictvím dotčené směrnice stanovila určitý cíl a členské státy se měly postarat o to, aby byl naplněn ústavně konformním způsobem. Nevyhovující znění ustanovení § 88a TR však existovalo ještě před vznikem samotné směrnice, a tímto se pouze dostalo do středu pozornosti Ústavního soudu, který jej shledal neproporcionálním ve vztahu k zásahu do práva na informační sebeurčení. Díky rozumně stanovené horní hranici trestní sazby, která vymezuje okruh trestných činů, u kterých je možné údaje o telekomunikačním provozu získat, doplněné o taxativní výčet trestných činů a závazek ke stíhání trestné činnosti vyplývající z mezinárodních smluv, je i po novele možné telekomunikační údaje získat u většiny z trestných činů, u nichž byl tento prostředek využíván nejčastěji. Data o proběhnuvší telekomunikaci tak již není možné využít zpravidla jen pro bagatelní trestnou činnost, jakou je např. trestný čin krádeže. A i přesto statistické údaje prozatím neukazují na pokles objasněnosti tohoto druhu kriminality. Můžeme proto říci, že se zákonodárci podařilo najít schůdné řešení a rovnováhu mezi oběma hodnotami – zachovat tento vyšetřovací nástroj pro potřeby orgánů činných v trestním řízení a omezit zásah do práv na ochranu osobnosti na případy, kdy veřejný zájem oprávněně převažuje nad zájmy jednotlivce. Snad bych jen novelizované úpravě vytknula příliš široký výčet orgánů oprávněných nakládat s telekomunikačními daty a na druhou stranu krátkou lhůtu k jejich uchovávání, jež je stanovena na nejnižší možné hranici.

Jaký je skutečný význam přístupu k provozním a lokalizačním údajům pro vyšetřování trestných činů, je těžké hodnotit. Například shrnující zpráva týkající se směrnice o data retention ve Velké Británii uvádí, že až 85 % žádostí se týká dat nikoli starších než 6 měsíců.<sup>74</sup> Dále se v literatuře můžeme setkat s odkazem na výzkum, podle kterého pouze ve 2–4 % vyšetřovaných případů již nebyla požadovaná data dostupná.<sup>75</sup> Na druhou stranu však stejná zpráva zmiňuje, že údaje starší jsou využívány právě k objasnění závažné trestné činnosti. Více než polovina žádostí o poskytnutí telekomunikačních dat za účelem vyšetřování teroristických hrozeb se týká dat starších 6 měsíců.<sup>76</sup>

Pro futuro si tedy dovoluji navrhnout znovu zvážit délku uchovávání telekomunikačních dat pro účely trestního řízení za stávajícího omezení na závažnou trestnou činnost. Doporučila bych prodloužení lhůty na 1 rok. Naopak delší retenční období než 1 rok již podle některých zdrojů orgánům činným v trestním řízení neposkytuje žádnou nebo jen malou přidanou hodnotu,<sup>77</sup> a je proto shledáno jako nepřiměřené ve vztahu k osobnostním právům, mezi něž patří i právo na informační sebeurčení. Jak již bylo výše zmíněno, Česká republika patří mezi několik málo členských států Evropské Unie, které délku uchovávání provozních a lokalizačních údajů stanovily na nejnižší možné hranici 6 měsíců. Prodloužením lhůty by se oprávněné orgány dostaly ke starším datům, jež

<sup>74</sup> *Liberty and security: Striking the balance*. UK Presidency Paper. 2005, s. 1–5. Dostupné z: <http://www.edri.org/docs/UKpresidencypaper.pdf>.

<sup>75</sup> Max-Planck Institut für ausländisches und internationalisches Strafrecht. Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach § 100g, 100h StPO. Forschungsbericht im Auftrag des Bundesministeriums der Justiz. Freiburg. 2008.

<sup>76</sup> *Liberty and security: Striking the balance*. UK Presidency Paper. 2005, s. 1–5. Dostupné z: <http://www.edri.org/docs/UKpresidencypaper.pdf>.

<sup>77</sup> MARAŠ, M.-H. The economic costs and consequences of mass communications data retention: is the data retention directive a proportionate measure? *European Journal of Law and Economics*, 2012, roč. 33, č. 2; s. 458.

by mohly významným způsobem pomoci při odhalování a vyšetřování organizované trestné činnosti. Soukromé subjekty tato data pro své účely uchovávají i ve lhůtách několikrát delších, tak proč je současně neposkytnout i oprávněným orgánům pro boj s kriminalitou?

#### OBTAINING TELECOMMUNICATION DATA AS AN INSTRUMENT FOR INVESTIGATION OF INTERNET CRIME

##### Summary

The paper deals with the legislation of obtaining telecommunication data as an important instrument for investigation of crime and changes that have occurred as a result of finding the existing legislation unconstitutional. The main point is the necessity of transposition of the data retention directive 2006/24/ES which has produced many contradictory reactions and has been the subject of review constitutional courts of several EU Member States. The main conflict is between two values – protection of intimate personal data, on the one hand and the investigation of criminal activity on the other. The paper deals with development of legislation, highlights the amendments and also offers a comparison of issues in the legislation of other EU Member States. The author also tries to infer whether and what influence did amendment § 88a TR have on solving of criminality.

*Key words:* data retention, telecommunications, cyber crime, criminal procedure

*Klíčová slova:* uchovávání dat, telekomunikace, kybernetická kriminalita, trestní řízení



## PHISHING A PROBLÉMY S JEHO TRESTNĚPRÁVNÍ KVALIFIKACÍ V TEORII A PRAXI

JIŘÍ KRUPIČKA

### 1. ÚVOD

Internet v mnoha ohledech usnadňuje každodenní život velké většiny obyvatelstva a lze bez nadsázky říci, že si již život bez něj dokážeme představit jen stěží. Krok za krokem se na něm naše společnost stala závislá. Internet nepřinesl však jen samé výhody, stejně jako dobře slouží naší společnosti, tak podobně dokáže posloužit i zločinu. Jednou z konkrétních podob tohoto nebezpečí je phishing, jímž se podrobněji zabývá tento příspěvek.

Phishing je jako druh kybernetické kriminality v mnoha ohledech specifický. Na jedné straně se v podstatě jedná jen o podvodné jednání, na druhou stranu jeho zvláštní charakter profitující z výhod, které nabízí internetové prostředí, jej od jiných druhů podvodů známých s reálného světa zcela zásadně odlišuje. Phishing tak stojí na pomezí mezi tzv. přímou internetovou kriminalitou, u které kriminální aktivity nemají obvykle výrazně podobný ekvivalent mimo kybernetický svět, a internetovou kriminalitu nepřímou, u níž naopak nelegální aktivity zcela existují i ve světě fyzickém.

Toto ambivalentní postavení phishingu pak může někdy činit potíže i při jeho trestněprávní kvalifikaci. Je to dáno zejména nesprávným pochopením tohoto druhu kriminality, popř. konkrétního způsobu spáchání trestného činu. Cílem tohoto příspěvku je proto jednak v krátkosti tento jev popsat, srovnáním jeho historických předchůdců vysvětlit způsob jeho fungování a následně na konkrétním příkladu poukázat na nesprávné právní vyhodnocení tohoto jevu orgány činnými v trestním řízení. Jelikož předkládaný případ se stal ještě za účinnosti starého trestního zákona, bude v poslední části tohoto příspěvku věnována pozornost stávající trestně právní kvalifikaci phishingu podle nového trestního zákoníku, neboť ten na poli kybernetické kriminality přinesl některé významné změny.

## 2. PHISHING JAKO FENOMÉN

### 2.1 DEFINICE PHISHINGU

Phishing může být definován jako kriminální jednání, jehož cílem je prostředky elektronické komunikace podvodně získat či vylákat citlivé informace, jako jsou přihlašovací jména, hesla a údaje o kreditních a debetních kartách, tak, že se pachatel maskuje za důvěryhodnou osobu či organizaci.<sup>1, 2</sup>

Etymologicky tento pojem vychází z anglické parafráze na slovo „fishing“, tedy „rybaření“.<sup>3</sup> Důvod je zřejmý. Pachatel phishingu vhadzuje své oběti návnadu, na kterou se jí snaží „chytit“. Zároveň rybaření odpovídá phishingu i v tom, že stejně jako případný pachatel i rybář ví, že se na jeho návnadu všechny ryby v rybníce nechytí. Oběma však bohatě postačí, když alespoň nějaká oběť jejich lovu na jejich návnadu zabere. V literatuře se někdy lze setkat s českým překladem slova phishing v podobě „rhybaření“,<sup>4</sup> ten se však u široké veřejnosti neujal a obvykle se tento jev i v českých podmínkách označuje původním názvem z angličtiny.

Podstatou phishingu je využívání tzv. sociálního inženýrství. To zahrnuje umění získat pomocí určitých psychologických technik citlivé údaje či další informace od oběti samotné.<sup>5</sup> Pachatel se tak často snaží získat důvěru oběti, která pak potřebné informace či údaje vlastně sdělí dobrovolně.<sup>6</sup> Tuto důvěru může získat buď bezprostředním kontaktem, což však od pachatele vyžaduje velkou míru odvahy a sebejistoty, nebo pomocí prostředků elektronické komunikace.<sup>7</sup> Tato varianta na pachatele neklade zdaleka tak vysoké nároky na komunikační a rétorické schopnosti, navíc skýtá velkou míru anonymity. Potenciální pachatel navíc může těžit z masovosti sítí elektronických komunikací, která mu umožňuje napadnout naráz obrovské množství potenciálních obětí. Děje se tak např. elektronickou poštou, na různých internetových diskusních fórech, sociálních sítích či na vlastních webových stránkách.

### 2.2 PŘEDCHŮDCI PHISHINGU

O phishingu jako takovém se začíná hovořit až s rostoucím rozvojem internetu v druhé polovině 90. let minulého století a zejména s rozmachem elektronického bankovníctví, na které bývá phishing často zaměřen. Je však zřejmé, že phishing měl své předchůdce ještě v dobách, kdy internet v dnešní podobě vůbec neexistoval. Sociální inženýrství se totiž neomezuje, jak už bylo řečeno, pouze na elektronický svět. Jedním z prvních předchůdců dnešního phishingu bylo jednání známé pod ná-

<sup>1</sup> CHOO, K.-K. R. Cyber threat landscape faced by financial and insurance industry. *Trends & issues in crime and criminal justice series*, 2011, č. 408, s. 3.

<sup>2</sup> Podobně též VOLOVECKÝ, P. Kybernetické hrozby a jejich trestně právní kvalifikace. *Trestní právo*, 2011, roč. 15, č. 1, s. 15.

<sup>3</sup> DUMAS, B. M. *Information Technology and Society*. Routledge, 2012, s. 169.

<sup>4</sup> Srov. např. BAUDIŠ, P. Staronové nebezpečí Rhybaření. *CHIP.CZ*, 2006, č. 4, s. 14 n.

<sup>5</sup> ČEPIČKA, D., ARNOLD, A., BEHRENS, D. Odhalte triky hackerů. *PC WORLD*, 2007, č. 12, s. 68 n.

<sup>6</sup> WORKMAN, M. Gaining Access with Social Engineering: An Empirical Study of the Threat. *Information Systems Security*, 2007, č. 16, s. 316.

<sup>7</sup> Idem., s. 321.

zvem španělský vězeň. Toto podvodné jednání sahá až do druhé poloviny 19. století<sup>8</sup> a bylo dokonce podrobně literárně zpracováno v povídce Arthura Traina z roku 1910.<sup>9</sup> Jeho podstatou je přesvědčení oběti, že jistý velmi bohatý vězeň bude ochoten se o své bohatství podělit, pokud prostřednictvím svého důvěrníka obdrží určitý obnos na podplacení strážní, které jej vězní. Poté, co oběť požadovanou částku důvěrníkovi zaplatí, se objeví neočekávané komplikace, pro které bude třeba uhradit další a další prostředky. Jediného, čeho se pak oběť tohoto podvodu dočká, je přivedení sebe sama na mizinu.

V dnešní době by se na takovou báchorku nechal nachytat asi málokdo. Stačí však příběh jen trochu pozměnit, aby zapadl do dnešního světa, a je na světě velice rafinované podvodné jednání, které v malých obměnách dokázalo způsobit obrovské škody. Právě španělským vězněm se totiž beze zbytku inspirovali tvůrci tzv. nigerijských listů, také známých pod označením „419 scam“<sup>10,11</sup>. V tomto případě pachatelé využívají obecně nízkou povědomost osob o politickoekonomické situaci v západoafrických zemích. Záminka pro samotné vylákání peněz je různá. Někdy to bývá převedení mnohamilionových částek z „mrtvých kont“ po obětech nebo svržených diktátorech po proběhlé občanské válce v Nigerii či jiné africké zemi. Podobnou zástěrkou je příběh místních bohatých podnikatelů a farmářů, kteří jsou po převratu ohroženi na životě a majetku, a tak se rozhodli emigrovat, přičemž nechtějí za sebou zanechat veškerý poctivě a namáhavě vydělaný majetek. Stejně jako u španělského vězně se však záhy objeví problémy – např. nutnost založit konto v místní bance, na které budou nejprve peněžní prostředky přeposlány, potřeba zaplatit poplatek finančnímu úřadu, poplatek za převod samotný, atp. Tyto taktiky vždy spoléhají na zákonitosti fungování lidské psychiky, kdy oběť v okamžiku, kdy se rozhodne prvotní částku zaplatit, není ochotna se své investice vzdát a neustále následuje vidinu snadného zbohatnutí. Jak se zvyšuje částka, kterou oběť pachatelům poskytla, je stále obtížnější ztrátu přijmout a naopak roste (částečně ze zoufalství) očekávání, že právě poslední splátka byla ta opravdu poslední a nyní bude již jen následovat sladká odměna.

Samotné nigerijské listy by měly, pokud by byly využívány pouze klasické prostředky komunikace (např. dopisy), pouze omezený rozsah. Co však z nich učinilo celosvětovou hrozbu, je elektronická pošta. Ta totiž umožňuje rozesílat podvodné dopisy (pod jakoukoliv záminkou k vylákání peněz) neomezenému počtu adresátů. Tím tento způsob podvodů vydláždil cestu phishingu.

Jak již bylo uvedeno výše, pozadí, za kterým se skrývá podvodné jednání, může nabývat nejrůznějších podob. Autor tohoto příspěvku sám čelil poměrně rafinovanému podvodnému útoku, a to při nákupu ojetého mopedu na německých serverech sdružujících inzeráty potenciálních prodávajících. Poté, co autor (německy) odpověděl na inzerát k prodeji skútru za cca 850 €, což byla cena sice výhodná, avšak nikoliv nereálná, přišla od „majitele“ motocyklu tato e-mailová odpověď:

<sup>8</sup> AN OLD SWINDLE REVIVED. The “Spanish Prisoner” and Buried Treasure Bait Again Being Offered to Unwary Americans. *The New York Times*, 20 March 1898, s. 12.

<sup>9</sup> TRAIN, A. The Spanish Prisoner. *The Cosmopolitan Magazine New York*, March 1910, č. 43, s. 465 n.

<sup>10</sup> Výraz odkazuje na číslo ustanovení nigerijského trestního zákoníku upravujícího podvodné jednání.

<sup>11</sup> TIVE, Ch. *419 Scam: Exploits of the Nigerian Con Man*. iUniverse, 2006, s. VII.

„Sir,

Re: 2010 Yamaha Aerox 50 r with 5400 km

Because of my financial problems that i have got i am willing to give it for € 700,- – shipping included .

It is in perfect condition with no damage on it. Technical inspection and emissions testing is passed and stamped as well. It has title of ownership, cleared of any obligations or fees and comes with all the documents you need to register it. You will not have to pay additional taxes for this (VAT reclaimable). (the bike is register in Germany and have german documents) It's my personal bike. I have worked in Germany for one year and I've purchased the motorcycle there. My company wanted me back home, so currently I'm in England (United Kingdom).The motorcycle it's now located in ENGLAND – United Kingdom.

it's a pity to keep such a motorcycle and not to use it.

UK registration tax is too high and have some financial problems to deal with and selling this motorcycle at this low price is the only option that I have right now. I am aware that I'm selling it way too cheap but I have no other solution.

I list my motorcycle under Europe Handler websites so I can sell it faster and for more publicity. The price is correct and the motorcycle can be transported to any location. My motorcycle is already at one Transport company from UK. I paid them to take care for my motorcycle sale protection. I can deliver the motorcycle to any location in Europe on my cost.

Please write me back to discuss only if you are interested!“

Z textu vyplývá, že požadovaná motorka je stále na prodej, nyní dokonce o 150 € levněji, avšak v současné době není k dispozici v Německu, ač tam byla zakoupena, ale v docích v Anglii, kam byl pisatel povolán zaměstnavatelem. Jelikož je registrace ve Spojeném Království příliš vysoká, nevyplatí se majiteli moped na ostrovech provozovat, a tak se ho rozhodl prodat. Moped majitel inzeroval přes německého prodejce, aby zvýšil publicitu inzerátu a prodej urychlil. Motorka je v současné době uschována u jednoho britského dopravce, na náklady majitele je možné ji dopravit na kterékoliv místo v Evropě. Ke zprávě bylo rovněž přiloženo 7 podrobných fotografií prodávané motorky.

Z odpovědi sice nikterak nevyplývá, že by zájemce musel uhradit jakékoliv prostředky navíc, je však možné, že by v další komunikaci byl ze strany majitele vznesen požadavek na (zálohovou) platbu předem, nejlépe prostřednictvím služeb Western Union, která zaručuje prakticky absolutní anonymitu příjemce. Rovněž lze očekávat požadavek na platbu pojištění přepravy apod.

Autor tohoto příspěvku byl s obdobnými praktikami na automobilových serverech obeznámen, avšak i pro něj bylo překvapivé, že podvodníkům stojí za snahu pokoušet své štěstí i na serverech inzerujících mopedy, jejichž cena je na rozdíl od automobilů řádově nižší. Navíc se u motocyklů nemůže uplatnit zástěrka nepoužitelnosti automobilů s levostranným řízením v Anglii. Přesto však již sama zpráva vzbuzuje určité pochybnosti. Jednak je neobvyklé, že majitel posílá svou zprávu v angličtině, ačkoliv zájemce odpovídal na inzerát ve spisovné němčině, navíc když majitel měl dle svých slov rok pracovat v Německu. I kdyby se za tu dobu německy nenaučil, prozrazuje podvodníka

samotný jazyk. Ačkoliv o sobě tvrdí, že je v Anglii doma, z textu je patrné (kromě jiných chyb), že angličtinu příliš neovládá, neboť přestože v názvech států důsledně dodržuje psaní velkých písmen („Germany“, „England“, „United Kingdom“), v případě přídavného jména „německý“, tj. „German“, píše toto slovo s malým počátečním písmenem, což je typické pro kontinentální země.

Uvedená zpráva vyvolala ihned u svého příjemce podezření z podvodného jednání. Přesto je třeba poznamenat, že pro osobu, která se rozhodla např. právě ke koupi motocyklu a už se viděla, jak se stane jeho hrdým majitelem, je tato nabídka opravdu lákavá. Přeci jen, co kdyby to nebyl podvod... I pro autora tohoto příspěvku, který metody sociálního inženýrství a nigerijských listů velmi dobře zná, bylo pokušení opravdu velké. Jak potom musí působit na neinformované osoby?

Autor, nyní však již z čirého zájmu, napsal (v angličtině) majiteli, že zájem o motorku stále má, je sice ochoten ji převzít na majitelem původně udávaném místě v Dortmundu, v žádném případě však nebude hradit jakékoliv poplatky ani zálohy za uvedenou motorku. Ze zprávy však bylo jasně patrné, že její autor je obeznámen s podvodnými praktikami. Odpověď od „majitele“ přišla nečekaně z e-mailové adresy s doménou registrovanou ve východní Evropě. Tato zpráva by však již pro svou vulgaritu nemohla být v tomto příspěvku publikována.

### 2.3 KONKRÉTNÍ PODOBA PHISHINGU

Phishingové praktiky se tedy inspirovaly v podvodných jednáních typu nigerijských listů ve dvojím směru. Jednak v metodách sociálního inženýrství, jednak v masivním využívání prostředků elektronických komunikací (zejména služby elektronické pošty, diskusních internetových fór, sociálních sítí apod.). Ty dokáží vzhledem k obrovskému počtu potenciálních obětí snižovat pravděpodobnost neúspěchu a zároveň díky své relativní anonymitě snižují i riziko odhalení.

Jedna z nejčastějších podob phishingu spočívá ve snaze pachatele vylákat z oběti údaje a hesla k internetovému bankovníctví, popř. číslo kreditní (platební)<sup>12</sup> karty, její dobu platnosti a tzv. Card Validation Code (CVC), tedy číslo k ověření platnosti karty nacházející se na její zadní straně. Pomocí těchto údajů pak může útočník z bankovního (karetního) účtu oběti odčerpat někdy i všechny finanční prostředky. Samotný útok obvykle probíhá v několika fázích. První z nich (přípravná fáze) zahrnuje opatřování potřebného (obrovského) počtu e-mailových adres potenciálních obětí. Toho lze dosáhnout hned několika způsoby. Jedním z nich je odkoupení (či jiné obstarání) databáze cizích e-mailových adres, která byla získána buď např. od internetových obchodníků přímo (v rozporu se zásadami ochrany osobních údajů), nebo bývá sama terčem např. hackerských útoků na systémy, kde jsou tyto databáze uloženy. V dnešní době se objevují dokonce i webové servery a internetová fóra s omezeným přístupem (tzv. carding

<sup>12</sup> Ve společnosti se obvykle oba výrazy zaměňují, resp. převažuje využívání výrazu „kreditní karty“ i pro karty platební. Z hlediska bankovního je však mezi oběma značný rozdíl, neboť prvně uvedený výraz slouží k čerpání prostředků z již bankou poskytnutého úvěru, jedná se tak v podstatě o úvěrovou kartu, v druhém případě se jedná o kartu sloužící k čerpání peněz (platbě) z běžného či spořicího účtu.

forums), kde probíhá čilý černý trh s kradenými osobními a finančními údaji.<sup>13</sup> Další způsob spočívá ve využití počítačového generátoru adres. Jedná se vlastně o počítačový program, který za pomoci slovníkových hesel, telefonních seznamů a seznamu registrovaných domén uměle vytváří jednotlivé e-mailové adresy s tím, že lze očekávat, že existující adresy budou obsahovat kombinaci takovýchto slov. Při tomto způsobu sice vzniká obrovské množství neexistujících adres, to však útočníkům nevadí, pokud zároveň získají dostatečný počet adres existujících.

V této souvislosti je třeba si uvědomit, že phishingu značně napomáhá neostražitost uživatelů internetu, kteří neváhají svou soukromou e-mailovou adresu vyplnit při registraci i na stránkách, jejichž solidnost je minimálně pochybná. Koncový uživatel totiž prakticky nemá žádnou kontrolu, co se s jeho údaji vyplněnými při registraci děje a zda není třeba právě jeho e-mailová adresa poskytnuta třetím osobám. Pokud by si uživatelé internetu zřizovali více e-mailových schránek, přičemž jednu by např. používali k oficiální komunikaci a jednu jako tzv. „spamovou“ schránku, která by byla využívána při nejručnějších registracích na webových serverech, jistě by tím do značné míry omezili možnost být adresátem pokusů o phishing.

Součástí přípravné fáze pak rovněž bývá i vytvoření webových stránek pod takovou doménou, která odpovídá očekávání oběti o webové stránce, kam bude údaje (dobrovolně) vyplňovat. Pokud tedy útok míří kupříkladu na klienty určité banky, bude se útočník snažit napodobovat webové stránky internetového bankovníctví tohoto bankovního ústavu, a to pod doménou (adresou), která tomuto účelu bude odpovídat. Oběť pak snadněji uvěří, že jí vyplněné údaje míří do správných rukou. Zároveň pachatel s webovými stránkami vytvoří i e-mailovou adresu, ze které bude uskutečněn samotný útok a která bude rovněž názvem odpovídat oběti očekávanému odesílateli.

Po těchto přípravách následuje vlastní phishingový útok. Ten spočívá v rozeslání e-mailové zprávy na získané adresy schránek, která má za úkol přimět oběť k vyrazení požadovaných údajů. Právě v této chvíli se uplatní metody sociálního inženýrství. I ta nejdůvěřivější osoba totiž nevyzradí tak důvěrné informace zcela bez důvodu. Zástěrka bývá v tomto ohledu různorodá, nejčastěji se lze setkat s tím, že pachatel vydávající se za bankovní ústav bude jejího klienta informovat o přechodu na nové (lepší) webové rozhraní internetového bankovníctví, protože je zapotřebí, aby se klient na nich přeregistroval pomocí původních přihlašovacích údajů. Rafinovanější varianta využívá obezřetnosti veřejnosti s existencí phishingu, a proto v tomto případě útočník kontaktuje oběť s tím, že její banka aktivně reaguje na zvyšující se phishingové nebezpečí. Proto banka zavádí bezpečnější systém, kam se má klient přihlásit pomocí stávajících údajů a autentifikovat jejich pravost. Vždy je však v e-mailové zprávě uveden odkaz, který klienta přesměruje přímo na „zabezpečené“ stránky. V tuto chvíli nastává rozhodující chvíle, zda se phishingový útok vydaří či nikoliv. Pokud bude oběť zprávě důvěřovat, útočníkovi s největší pravděpodobností v sítích uvízne. Odradit by ji totiž mohlo už jen podezřelý či nekvalitní zpracování webového rozhraní stránek, na které ji odkaz poslal. V případě, že oběť „klikne“ na odkaz uvedený v e-mailové zprávě a na stránkách vy-

---

<sup>13</sup> K tomu blíže v: PERETTI, K. K. Data Breaches: What the Underground World of “Carding” Reveals. *Santa Clara Computer and High Technology Journal*, 2008, č. 2, s. 375 n.

tvořených útočníky údaje do podstrčeného formuláře vyplní, získají pachatelé okamžitě přístupové údaje k internetovému bankovníctví.

Poslední fáze phishingového útoku konečně zahrnuje neoprávněné odčerpání prostředků z bankovního účtu oběti pomocí vylákaných přihlašovacích údajů, popř. zakoupení hodnotného zboží prostřednictvím vyzískaných údajů o kreditní kartě oběti. Jelikož elektronické peněžní přesuny bývají poměrně dobře vysledovatelné, využívají často pachatelé-organizátoři nastrčených osob (bílých koní). V případě bezhotovostního odčerpání peněžních prostředků oběti tito za určitou odměnu zakládají bankovní účty, na které následně phishingem podvodně získané finanční prostředky přicházejí. Ať již pomocí platebních karet v bankomatech či přímo na pobočce jsou neoprávněně nabyté prostředky vybírány a v hotovosti či právě pomocí platebních příkazů Western Union předávány hlavním pachatelům. V případě nákupu zboží na základě vylákaných (či odkoupených) údajů z platebních a kreditních karet spolupracují tito bílí koně nezřídka nevědomky. Pouze příjmu nikterak obtížnou „administrativní“ práci v podobě kontroly obsahu a přeposílání zásilek, které jim po uzavření „pracovní smlouvy“ začnou být ve velkém počtu doručovány, na předem dané adresy. Tímto způsobem je pak možné zastříť původ zboží z phishingových aktivit.

### 3. TRESTNĚPRÁVNÍ KVALIFIKACE PHISHINGU PODLE TR. ZÁKONA

#### 3.1 PŘÍPAD NEPOCHOPENÉHO PHISHINGU

Předkládaný případ názorně ukazuje, jak je někdy pro orgány činné v trestním řízení obtížné konkrétní podobu internetové kriminality uchopit. V dané věci napadla obžaloba pro dva skutky spočívající v tom, že:<sup>14</sup>

- 1) „Obžalovaný R. F. po vzájemné dohodě s již odsouzeným K. Z. a další dosud neustavenou osobou, či dalšími osobami, prostřednictvím e-mailu, zasláného na e-mailovou adresu poškozené A. L. R., nechal podvrhnout falešný internetový formulář, vložený prostřednictvím <http://citationline.czechrepublic-online.com/index2html>, na originální stránky Citibank, a. s., předstírající, že je originální internetový formulář <https://czechrepublic.2.online.citibank.cz/HomeBankingSecure/Pers/StartSession.asp?>, kdy pod záminkou potvrzení údajů, týkající se transakce ke dni 24. 3. 2006, nechal vylákat od A. L. R. citlivé údaje k jejímu účtu vedenému u Citibank, a. s., č. účtu X a poté, co A. L. R., dle příslušných odkazů uvedených na podvrženém internetovém formuláři, se dostala na nezabezpečené falešné stránky, předstírající, že patří bankovnímu ústavu Citibank, a. s., a dispoziční údaje k předmětnému účtu zadala spolu s HPINem, tedy heslem k uvedenému účtu, nechal provést prostřednictvím služby internetového bankovníctví podvodnou transakci vyplněním příslušných údajů do předepsaného formuláře poskytnutého bankou, aby z účtu plátce, tedy účtu č. X byly převedeny finanční prostředky ve výši 999,79 EU na účet č. Y, na základě

<sup>14</sup> Text je ohledně prvního skutku v autentickém znění, pouze anonymizován, u druhého skutku je parafrázován.

takto vyplněného a posléze odeslaného formuláře do Citibank, a. s., skutečně došlo k odúčtování uvedené finanční částky z předmětného účtu majitelky A. L. R., vedeného u pobočky Citibank, a. s., v Praze 6, Evropská 178, bez jejího vědomí došlo, přičemž dne 27. 3. 2006 byla částka 999,79 EU v ekvivalentu 28 664 Kč převedena na účet Y u eBanky v Praze 1, Václavské nám. 43, který si zatím účelem a s příslibem provize v částce 3000 Kč na pokyn obv. R. F. založil dne 20. 3. 2006 K. Z., jenž dne 29. 3. 2006, když se pokoušel z účtu peníze vyzvednout, byl zadržen.“

- 2) R. F. po vzájemné dohodě s S. K. padělali podpis třetí osoby na formulářích příkazů k úhradě, které pak S. K. vhodil do sběrných boxů, případně odevzdal na přepážce banky, přičemž převod prostředků na účet zřízený S. K. a následný výběr hotovosti byl proveden ohledně částky 95 000 Kč pouze jedenkrát, za což obžalovaný S. K. obdržel odměnu ve výši 5000 Kč. V dalších pěti případech k převodu částky ve výši 95 000 Kč, resp. 97 000 Kč (v jednom případě) nedošlo, neboť při provádění kontroly podpisových vzorů k těmto příkazům k úhradě vzniklo podezření, že podpisy na nich jsou zfalšované. Obžalovaní tak měli způsobit poškozené bance H. B. C. R. škodu ve výši 95 000 Kč a pokusit se o způsobení škody v celkové výši 479 500 Kč.

Skutek pod bodem 1. obžaloby byl státním zástupcem kvalifikován jako „trestný čin padělání a pozměňování peněz podle § 140 odst. 2 zákona č. 140/1961 Sb., trestní zákon (dále jen „tr. zákon“), za užití ustanovení § 143 tr. zákona formou spolupachatelství podle § 9 odst. 2 tr. zákona v jednočinném souběhu s trestným činem podvodu podle § 250 odst. 1, odst. 2 tr. zákona ve stádiu pokusu podle § 8 odst. 1 tr. zákona formou spolupachatelství podle § 9 odst. 2 tr. zákona a v jednočinném souběhu s trestným činem poškození a zneužití záznamu na nosiči informací dle § 257a odst. 1 písm. a) tr. zákona, formou spolupachatelství podle § 9 odst. 2 tr. zákona“. Skutek pod bodem 2. obžaloby pak byl kvalifikován jako „trestný čin padělání a pozměňování peněz dle § 140 odst. 2, 3, písm. b) tr. zákona za užití ustanovení § 143 tr. zákona spáchaný formou spolupachatelství podle § 9 odst. 2 tr. zákona v jednočinném souběhu s trestným činem podvodu podle § 250 odst. 1, odst. 3 písm. b) tr. zákona dílem dokonaný dílem ve stádiu pokusu podle § 8 odst. 1 tr. zákona spáchaný formou spolupachatelství podle § 9 odst. 2 tr. zákona“.

Po provedeném dokazování Městský soud v Praze jako soud prvního stupně oproti obžalobě považoval jednání popsané pod bodem 1. obžaloby pouze jako další dílčí útok pokračování v podvodném jednání uvedeném pod bodem 2. obžaloby, a proto škodu z jednání pod bodem 1. přičetl do celkové částky škody, o kterou se obžalovaní měli pokusit, jinak však samotný popis jednotlivých útoků ponechal beze změn. Skutek, pro který byli obžalovaní uznáni vinnými, následně kvalifikoval ohledně obžalovaného R. F. jako „trestný čin padělání a pozměňování peněz podle § 140 odst. 2, al. 2 tr. zákona za užití ust. § 143 tr. zákona ve spolupachatelství podle § 9 odst. 2 tr. zákona v jednočinném souběhu s trestným činem podvodu podle § 250 odst. 1, odst. 3 tr. zákona dílem dokonaným, dílem ve stádiu pokusu podle § 8 odst. 1 tr. zákona ve spolupachatelství podle § 9 odst. 2 tr. zákona a v bodě 1. v jednočinném souběhu s trestným činem poškození a zneužití záznamu na nosiči informací dle § 257a odst. 1 písm. a) tr. zákona“. Ohledně obžalovaného S. K. byl skutek, kterým byl uznán vinným, kvalifikován jako „trestný čin padělání a pozměňování peněz podle § 140 odst. 2, al. 2 tr. zákona za užití



ustanovení § 143 tr. zákona ve spolupachatelství podle § 9 odst. 2 tr. zákona v jedním souběhu s tr. činem podvodu podle § 250 odst. 1, odst. 3 tr. zákona dílem dokonáným, dílem ve stádiu pokusu podle § 8 odst. 1 tr. zákona ve spolupachatelství podle § 9 odst. 2 tr. zákona“.

Vrchní soud v Praze jakožto soud odvolací se s kvalifikací jednání pod bodem 1. rozsudku jakožto dílčího útoku pokračování v podvodném jednání, jehož další útoky jsou uvedeny pod bodem 2. rozsudku, ztotožnil, přesto však zrušil výrok o vině i o trestu. Dle autora tohoto příspěvku vrchní soud zcela správně dospěl k závěru, že vzhledem k celkově způsobené škodě ve výši 95 000 Kč nemohl být trestný čin podvodu podle § 250 odst. 1, 3 písm. b) tr. zákona ani dílem dokonáný, neboť uvedená kvalifikace vyžadovala způsobení škody značné, tedy ve smyslu § 89 odst. 11 tr. zákona nejméně 500 000 Kč. Odvolací soud proto znovu uznal oba obžalované vinnými, avšak ohledně trestného činu podvodu podle § 250 odst., 3 písm. b) tr. zákona nikoliv dílem dokonáného a dílem nedokonáného, ale zcela ve stádiu pokusu podle § 8 odst. 1 tr. zákona. Jinak ponechal kvalifikaci soudu prvního stupně beze změn.

Za výše uvedené trestné činy vrchní soud odsoudil obžalovaného R. F. k úhrnnému trestu v trvání pěti let, pro který jej zařadil do věznice s dozorem. Zároveň jej oproti výroku o trestu soudu prvního stupně navíc odsoudil i k trestu vyhoštění na dobu pěti let. Obžalovaný S. K. byl odvolacím soudem odsouzen k trestu odnětí svobody v trvání tří let, jenž mu byl podmíněně odložen na zkušební dobu v trvání pěti let s dohledem. Konečně byla oba obžalovaným stanovena rozsudkem odvolacího soudu povinnost společně a nerozdílně nahradit poškozené bance H. B. C. R. částku 95 000 Kč na náhradu škody.

### 3.2 PROBLÉMY PRÁVNÍ KVALIFIKACE PŘÍPADU

Z uvedených rozhodnutí soudů obou stupňů vyplývá hned několik sporných otázek, které lze rozdělit do několika okruhů:

- 1) Lze podvodné jednání spočívající v odčerpání prostředků z účtů různých osob pomocí přístupových údajů k internetovému bankovníctví vylákaných od oběti cestou phishingu na jedné straně a na základě zfalšovaných papírových formulářů jednorázového příkazu k úhradě vhozeného do sběrného boxu v bance na straně druhé považovat celkově za pokračování v trestném činu ve smyslu § 89 odst. 3 tr. zákona, resp. § 116 tr. zákoníku?
- 2) Pokud na základě zfalšovaných příkazů k úhradě (ať už elektronických či listinných) dojde k transakci peněžních prostředků (v podobě tzv. žirálních peněz)<sup>15</sup> na jiný účet, v kterém okamžiku bude dokonán trestný čin podvodu?
- 3) Lze kvalifikovat elektronické zadání příkazu k úhradě na základě autentifikačních údajů vylákaných phishingem provedené před 1. 1. 2010 jako trestný čin padělání a pozměňování peněz podle § 140 odst. 2 alinea 2 tr. zákona?
- 4) Je možné samotné phishingové jednání v tomto případě kvalifikovat jako trestný čin poškození a zneužití záznamu na nosiči informací dle § 257a odst. 1 písm. a) tr. zákona? Řešením těchto otázek se bude v následujícím textu zabývat tento příspěvek.

<sup>15</sup> Tj. bezhotovostních peněz vedených na účtech.

### 3.2.1 PHISHING JAKO DÍLČÍ ÚTOK POKRAČOVÁNÍ V TRESTNÉM ČINU PODVODU

Jak již bylo zmíněno výše, soudy obou stupňů na rozdíl od obžaloby státního zástupce považovaly jednání uvedené pod bodem 1. obžaloby, tedy elektronické odčerpání prostředků z účtu oběti phishingu, pouze jako dílčí útok pokračování v trestném činu podvodu (resp. jeho pokusu). Přitom ostatní útoky tohoto pokračujícího trestného činu nebyly realizovány elektronicky, nýbrž písemnými formuláři příkazu k úhradě s falšovanými podpisy oprávněné osoby. Autor tohoto příspěvku se s tímto závěrem ztotožňuje. Ustanovení § 89 odst. 11 tr. zákona stejně jako ustanovení § 116 zákona č. 40/2009 Sb., trestní zákoník (dále jen „tr. zákoník“), považuje za pokračování v trestném činu jednání, jehož jednotlivé dílčí útoky vedené jednotným záměrem naplňují (v tr. zákoníku je již výslovně uvedeno „byť i v souhrnu“) skutkovou podstatu stejného trestného činu, jsou spojeny stejným nebo podobným způsobem provedení a blízkou souvislostí časovou a v předmětu útoku.

Je zřejmé, že jednání pod bodem 1. i 2. rozsudku byla vedena jednotným záměrem, a to podvodně pomocí falšovaných příkazů k úhradě vylákat finanční prostředky z účtů různých klientů bank. Zároveň všechna tato jednání naplnila, mimo jiné, skutkovou podstatu stejného trestného činu, a to podvodu podle § 250 tr. zákona, resp. jeho pokusu. V daném případě byla splněna i podmínka blízké souvislosti časové, byť útok spáchaný prostřednictvím elektronického bankovníctví a útoky v podobě padělaných listinných příkazů k úhradě od sebe dělila doba skoro 4 měsíců. Jednak tato doba není natolik dlouhá, aby zakládala automatické přetržení časové souvislosti, a jednak dle stávající judikatury Nejvyššího soudu ČR nelze blízkou časovou souvislost mezi dílčími útoky přesně ohraničit maximální lhůtou, ale je ji třeba posoudit s ohledem na konkrétní skutkové okolnosti každého případu.<sup>16</sup> V posuzovaném případě nasvědčuje pokračování zejména velice obdobný postup pachatele R. F., který si vždy před samotným pokusem o odčerpání finančních prostředků zajistil osobu, která pro něj založila „čistý“ bankovní účet, na který vylákané prostředky později zašle. Tyto osoby pak měly poté, co peníze na účet dorazí, tyto vybrat a předat pachateli R. F. Oba druhy jednání se tak od sebe lišily jen v tom, že v prvním případě podvod probíhal cestou elektronických příkazů k úhradě, který byl falešně autentifikován přístupovými údaji pocházející od oběti phishingu, v druhém případě pak formulářů k jednorázovému příkazu k úhradě, na kterém byl zfalšován podpis oprávněného disponenta. Lze proto shrnout, že všechny útoky podvodného jednání byly spojeny obdobným způsobem provedení. Konečně byl splněn i znak souvislosti v předmětu útoku, když všechny dílčí útoky mířily proti bezhotovostním penězům uloženým na účtech různých bankovních ústavů.

### 3.2.2 DOKONÁNÍ TRESTNÉHO ČINU PODVODU V PŘÍPADĚ, KDY TRANSAKCE NA ZÁKLADĚ PADĚLANÝCH PŘÍKAZŮ BYLA PROVEDENA.

Z předložených rozsudků, stejně jako obžaloby vyplývá, že orgány činné v trestním řízení považovaly za dokonání (alespoň v základní skutkové podstatě) pouze

<sup>16</sup> Viz např. usnesení Nejvyššího soudu ČR ze dne 2. 6. 2010, sp. zn. 7 Tdo 440/2010.

jediný dílčí útok pokračujícího trestného činu podvodu, a to ten, při kterém pachatelé dokázali neoprávněně převedené prostředky na základě zfalšovaného podpisu na formuláři příkazu k úhradě z účtu vybrat. Dle názoru autora tohoto příspěvku však takový závěr není správný. Trestný čin podvodu podle § 250 odst. 1 tr. zákona je dokonán v tom případě, když pachatel ke škodě cizího majetku sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou. V případě podvodných odčerpání finančních prostředků z bankovních účtů proto k dokonání trestného činu musí dojít v okamžiku, kdy banka uvedená v omyl ohledně osoby příkazce (jeho identity) platební transakci provede. V ten okamžik totiž oprávněný klient banky ztrácí nad těmito žirálními penězi kontrolu (dispozici), kterou naopak získává příjemce z provedené platební transakce. To platí zejména v těch případech, kdy peněžní prostředky jsou připsány na účet bankovního ústavu odlišného od banky domnělého plátce, kde kontrolu nad těmito prostředky banka plátce dokonce zcela ztrácí.

Peníze na účtech představují pohledávku za bankou. Z pohledu trestního práva se na ně vztahují i ustanovení o věcech (§ 89 odst. 13 věta druhá tr. zákona), jejichž hodnota se rovná jejich nominální výši. Pokud jsou tedy v rámci podvodné činnosti převedeny peněžní prostředky na jiný účet (oprávněnou osobu s ním disponující), vzniká tím původnímu majiteli této majetkové hodnoty škoda a naopak příjemci neoprávněný prospěch. Jejich zpětná výměna v nominální hodnotě je tak z hlediska okamžiku dokonání podvodu irelevantní, neboť již předtím došlo k převodu majetkové hodnoty (věci) ve stejné nominální výši.

Pokud tedy v případě prvního útoku, který využíval přístupových údajů k elektronickému bankovníctví získaných phishingem, došlo na základě elektronického příkazu k úhradě k bezhotovostnímu převodu finančních prostředků a tyto byly připsány na účet zřízený pachateli u jiné banky, byl okamžikem připsání těchto prostředků trestný čin podvodu dokonán, a to vzhledem k výše vzniklé škodě a neoprávněného prospěchu 28 664 Kč dle ustanovení § 250 odst. 2 tr. zákona. To samozřejmě nic nemění na tom, že vzhledem k dalším dílčím útokům bylo třeba jednání pachatelů v souhrnu kvalifikovat jako pokus pokračujícího trestného činu podvodu podle § 8 odst. 1, § 250 odst. 3 písm. b) tr. zákona, neboť aby tento trestný čin mohl být alespoň dílem dokonáný, musel by součet dílčími útoky způsobené škody dosahovat částky 500 000 Kč, což se v daném případě nestalo.

U zbylých útoků, které byly uskutečněny pomocí formulářů k jednorázovému příkazu k úhradě s padělaným podpisem, nedošlo k provedení bezhotovostního platebního převodu na účet ve formuláři uvedeného příjemce. Z toho důvodu nemohla být u těchto útoků naplněna skutková podstata trestného činu podvodu ani v prvním odstavci, a jednalo se tak pouze o ukončený pokus.

Lze tak uzavřít, že správně měla být skutková věta rozsudku Vrchního soudu v Praze doplněna tak, že obžalovaný R. F. způsobil jednáním pod bodem 1. poškozené Citibank, a. s., škodu ve výši 28 664 Kč, a zároveň o tuto částku měla být ponížena výše celkové škody, ke které dle odsuzujícího rozsudku mělo směřovat jednání obžalovaného R. F.

### 3.2.3 TRESTNĚPŘÁVNÍ KVALIFIKACE ELEKTRONICKÉHO ZADÁNÍ PŘÍKAZU K ÚHRADĚ NA ZÁKLADĚ AUTENTIFIKAČNÍCH ÚDAJŮ VYLÁKANÝCH PHISHINGEM

Dalším problematickým okruhem týkajícím se phishingu je trestněprávní kvalifikace samotného aktu, kdy pachatel neoprávněně získané autentifikační údaje použije k zadání jednorázového příkazu k úhradě pomocí služby elektronického bankovníctví. Je nesporné, že toto jednání je třeba (pokud na základě něho dojde k transakci prostředků) posoudit jako trestný čin podvodu, popř. jeho pokusu, v době vydání předkládaných rozhodnutí podle § 250 tr. zákona. Tím však není vyloučen v úvahu připadajících trestných činů vyčerpán. Orgány činné v trestním řízení v předkládané věci toto jednání posoudili jako jednočinný souběh trestného činu podvodu (ve stádiu pokusu) podle § 8 odst. 1, § 250 odst. 1, 3 písm. b) tr. zákona a trestného činu padělání a pozměňování peněz podle § 140 odst. 2 alinea 2 tr. zákona. Všechny ve věci rozhodující orgány přitom vycházely ze společných ustanovení § 143 tr. zákona, které přiznávají ochranu proti padělání též tuzemským a cizozemským platebním prostředkům.

Konkrétní úpravu příkazu k úhradě obsahovala od 28. 6. 2011 prováděcí vyhláška ČNB č. 62/2004 Sb., kterou se stanoví způsob provádění platebního styku mezi bankami, zúčtování na účtech u bank a technické postupy bank při oprávněném zúčtování (dále jen „vyhláška“). Podle § 2 této vyhlášky provádějí banky tuzemský platební styk formou úhrady nebo inkasní formou placení, přičemž úhradou se rozumí operace prováděná na základě příkazu, který dal příkazce své bance za účelem převedení peněžních prostředků ve prospěch příjemce.<sup>17</sup> Podle odst. 4 uvedeného ustanovení vyhlášky může být úhrada uskutečňována odepsáním peněžních prostředků z účtu plátce a jejich připsáním na účet příjemce (dále jen „bezhotovostní platební styk“). Podle § 3 odst. 1 vyhlášky pak banky používají v tuzemském bezhotovostním platebním styku ve vztahu s klienty příkazy k úhradě a příkazy k inkasu, které mohou být bance předávány na tiskopisech, formou elektronických dat nebo jiným sjednaným způsobem.

Z uvedených ustanovení tedy vyplývá, že zákon o platebním styku z roku 2002 i vyhláška ČNB z roku 2004 přiznávaly příkazům k úhradě postavení platebního prostředku, a to jak v jejich tiskopisných formách, tak i v elektronických, předávaných např. službou elektronického bankovníctví. Vzhledem k tomu, že přístupové údaje k elektronickému bankovníctví slouží v podstatě k autentifikaci osoby oprávněně disponovat prostředky na účtu stejně, jako je tomu v případě podpisu na tiskopisu příkazu k úhradě, bylo lze subsumovat jednání, kdy pachatel autentifikačními údaji jiné osoby potvrdil oprávněnost elektronického příkazu k úhradě z účtu oběti, pod skutkovou podstatu trestného činu padělání a pozměnění peněz podle § 140 odst. 2 alinea 2 tr. zákona ve spojení s § 143 tr. zákona. V tomto směru se proto lze se závěry obou soudů v předkládané věci zcela ztotožnit.

<sup>17</sup> Paragraf 3 odst. 1 zákona č. 124/2002 Sb., o platebním styku, v časově relevantním znění.

### 3.2.4 TRESTNĚPRÁVNÍ KVALIFIKACE SAMOTNÉHO PHISHINGOVÉHO JEDNÁNÍ PODLE § 257a ODSŤ. 1 PÍSM. a) TR. ZÁKONA

Soudy obou stupňů rovněž shodně s obžalobou kvalifikovaly výše popsané jednání pod bodem 1. jako trestný čin poškození a zneužití záznamu na nosiči informací dle § 257a odst. 1 písm. a) tr. zákona. Tato kvalifikace je však dle autora tohoto příspěvku nesprávná a vychází z určitého nepochopení modu operandi phishingu. O tom svědčí již skutková věta pod bodem 1. odsuzujícího rozsudku Vrchního soudu v Praze, kde je odsouzený R. F. uznán vinným tím, že jako spolupachatel „prostřednictvím e-mailu, zaslánoho na e-mailovou adresu poškozené A. L. R., nechal podvrhnout falešný internetový formulář, vložený na originální stránky Citibank, a. s., [...]“. Je totiž v praxi velice obtížné, aby pachatelé cokoliv „podvrhovali“, natož falešný internetový formulář k vyplnění přístupových údajů k elektronickému bankovníctví, na *originální* stránky jakéhokoliv bankovního ústavu. Ty bývají velmi důkladně zabezpečené, uloženy na obtížně přístupných serverech chráněných víceprvkovou ochranou, a proto by jejich narušení v takové míře bylo obtížné i pro velmi schopného hackera. Pachatelé phishingu tak na originální stránky banky nic nevkládají. Místo toho (jak bylo rozvedeno výše) vytvoří webové stránky vypadající shodně s rozhraním využívaným poškozenou bankou a následně zašlou oběti e-mailovou zprávu, která ji má přesvědčit, aby přístupové údaje na těchto stránkách, kam ji nasměruje odkaz v e-mailové zprávě, zadala. Oběť tedy pachatelům své přístupové údaje vlastně „dobrovolně“ předá v domnění, že je poskytuje svému bankovnímu ústavu.

Pachatelé phishingu proto nezískávají přístup k nosiči informací a takových informací neoprávněně neužívají v úmyslu získat sobě neoprávněný prospěch ve smyslu ustanovení § 257a tr. zákona. I když neoprávněně užívají určité informace (identifikační údaje k elektronickému bankovníctví), nemusí k nosiči s těmito informacemi ať už u banky či přímo u oběti získávat přístup, nýbrž je sami přímo obdrží od oběti na vlastní webový server. Naplnění skutkové podstaty uvedeného trestného činu tak připadá v úvahu pouze u poměrně malého množství phishingových případů. Bude tomu tak zejména v situacích, kdy budou k získání informací použity hackingové metody, např. pokud e-mailová zpráva určená oběti bude obsahovat určitý škodlivý kód, typicky tzv. keylogger, pomocí něhož bude možné „odposlechnout“ potřebné údaje. V případech, kdy ale pachatelé zvolili klasickou metodu phishingu, nebylo toto jednání možné pod skutkovou podstatu trestného činu poškození a zneužití záznamu na nosiči informací podřadit.

Stejně tak nelze dospět k závěru o naplnění trestného činu podle § 257a tr. zákona tím, že pachatel phishingem vyláká přístupové údaje k internetovému bankovníctví (tedy k nosiči informací obsluhujícího tuto službu banky) a informace (např. o stavu účtu) tam svým příkazem změní. Pachatelé phishingu sami takovéto informace nemění, nýbrž je to banka, resp. její systém internetového bankovníctví, která v důsledku transakce uskutečněné pachatelem phishingu provede změnu informací o zůstatku na bankovním účtu.

Lze proto uzavřít, že samotný phishing bylo podle právní úpravy do 31. 12. 2009 možné postihnout jen jako přípravné jednání k trestnému činu podvodu a padělání a pozměňování peněz, ne již však jako dokonaný trestný čin, pokud nedošlo k realizaci

peněžní transakce. Přitom je zřejmé, že nebezpečnost phishingu pro společnost je velmi vysoká a může vést k astronomickým škodám. V tomto směru lze tedy považovat předchozí právní úpravu postihu phishingu za nedostatečnou.

Na předloženém případě phishingu je poměrně pozoruhodné i to, že obžalovaný R. F. byl odsouzen za podvodné vylákání přístupových údajů oběti, aniž by byl proveden jakýkoliv důkaz, jak obžalovaný k těmto údajům přišel. Z dokazování totiž vyplynulo pouze to, že obžalovaný požádal svého známého, aby založil bankovní účet s tím, že jakmile na něj dorazí určité finanční prostředky, má tyto vybrat a odevzdat je obžalovanému R. F. Na nově otevřený účet následně peníze skutečně došly, a to na základě elektronického příkazu k úhradě, který zadala nezjištěná osoba, a to pomocí přihlašovacích údajů, které byly získány opět neznámou osobou či osobami z phishingu. V průběhu hlavního líčení však nikterak nebylo prokázáno, že se obžalovaný R. F. na samotném vylákávání údajů reálně podílel. Ten se přitom mohl k přihlašovacím údajům dostat tak, že by je prostě od někoho odkoupil, či mohl být jen osobou, která se dohodla se samotným původcem phishingu, že mu takto pomůže peníze z účtu oběti odčerpát. I v tomto směru tak lze považovat předkládané rozsudky za chybné.

#### 4. TRESTNĚPRÁVNÍ KVALIFIKACE PHISHINGOVÉHO JEDNÁNÍ PODLE NOVÉHO TRESTNÍHO ZÁKONÍKU

Nový trestní zákoník vstoupil v platnost zákonem č. 40/2009 Sb., trestní zákoník, s účinností od 1. 1. 2010. Tento zákoník měl odstranit některé nedostatky původní úpravy a harmonizovat vnitrostátní trestní právo s mezinárodními úmluvami a závazky plynoucími z komunitárního práva. V oblasti počítačové kriminality byla hlavním zdrojem této harmonizace Úmluva o počítačové (správněji však kyber) kriminalitě (Úmluva Rady Evropy č. 185, Budapešť, 2001), kterou Česká republika podepsala dne 9. 2. 2005,<sup>18</sup> avšak doposud ji neratifikovala. Ačkoliv Česká republika není touto úmluvou vázána, zákonodárce již v důvodové zprávě k novému trestnímu zákoníku vyjadřuje vůli zavést trestněprávní úpravu kyberkriminality, která by s předmětnou úmluvou byla v souladu, a splnit tak případně budoucí závazky napřed.<sup>19</sup>

##### 4.1 POSTIH PODLE § 230–232 TR. ZÁKONÍKU

Do nové trestněprávní úpravy majetkových trestných činů v ustanoveních § 230–232 byly začleněny tři trestné činy postihující kybernetickou kriminalitu. Prvním z nich je trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací, který v podstatě rozšiřuje původní trestný čin poškození a zneužití záznamu na nosiči informací dle § 257a odst. 1 písm. a) tr. zákona. Dle názoru autora tohoto příspěvku však phishingové jednání v jeho čisté formě, tzn. nezahrnující hackingové aktivity,

<sup>18</sup> Rada Evropy, <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=13/04/2011&CL=ENG> [cit. 2012-04-10].

<sup>19</sup> Důvodová zpráva k § 228–230 (dnes § 230–232) vládního návrhu trestního zákoníku, Poslanecká sněmovna Parlamentu České republiky, 5. volební období, 2006–2010, sněmovní tisk č. 410/0.

nemůže být podle tohoto trestného činu postiženo, a to v podstatě ze shodných důvodů, jako v úpravě předchozí.

Skutková podstata trestného činu podle § 230 odst. 1 tr. zákoníku vyžaduje překonání bezpečnostního opatření, a tím neoprávněného získání přístupu k počítačovému systému nebo k jeho části. To se však v případě phishingu neděje, neboť pachatel získá přístupové údaje k elektronickému bankovníctví přímo od oběti, a nemusí tak překonávat žádné bezpečnostní opatření.

Druhá základní skutková podstata obsažená v odst. 2 citovaného ustanovení pak postihuje (podobně jako úprava předchozí) „získání přístupu k počítačovému systému a nosiči informací“ a další aktivity s tam uloženými daty či naopak učinění zásahu do programového nebo technického vybavení počítače. Jak již však bylo zmíněno výše, pachatel potřebné informace (data) sám obdrží od oběti a nemusí získávat přístup ve smyslu uvedeného ustanovení.

Phishing však nebude možné trestat ani podle nově zavedeného trestného činu opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat podle § 231 tr. zákoníku. Ten sice postihuje již samotné opatření, přechovávání a další způsoby zpřístupnění přístupových dat, kódů, hesel apod., ovšem pouze v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv nebo právě trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací, což opět není případ klasického phishingu.

Třetí nově zavedený „počítačový“ trestný čin podle § 232 tr. zákoníku dopadá na případy nedbalostního poškození nebo zásahu do počítačového systému či vybavení počítače, a proto ani ten nebude na phishing dopadat.

#### 4.2 POSTIH PODLE § 234 TR. ZÁKONÍKU

Trestní zákoník rovněž nově rozlišuje ochranu proti padělání a pozměnění peněz na jedné straně a platebního prostředku na straně druhé. Zároveň byl s účinností k 1. 11. 2009 přijat nový zákon č. 284/2009 Sb., o platebním styku, který přináší definici platebního prostředku. Ten je v § 2 odst. 1 písm. d) vymezen jako „zařízení nebo soubor postupů dohodnutých mezi poskytovatelem a uživatelem, které jsou vztaženy k osobě uživatele a kterými uživatel dává platební příkaz“.

Jelikož skutková podstata trestného činu neoprávněného opatření, padělání a pozměnění platebního prostředku podle § 234 odst. 1 tr. zákoníku považuje mimo jiné za trestné i opatření a přechovávání platebního prostředku jiného, vyvstává tu otázka, zdali přístupové údaje k elektronickému bankovníctví naplňují výše uvedenou definici platebního prostředku. V takovém případě by bylo lze stíhat samotné podvodné vyláčení těchto údajů jako tento dokonaný trestný čin. Ke kladnému závěru dospívá např. Volovecký.<sup>20</sup>

Autor tohoto příspěvku zastává názor, že nikoliv, a to proto, že shora uvedená definice označuje za platební prostředek až (celý) soubor postupů, které jsou vztaženy k osobě uživatele a kterými uživatel dává platební příkaz, nikoliv samotné přístupové údaje. Ty

<sup>20</sup> VOLOVECKÝ, P. Kybernetické hrozby a jejich trestně právní kvalifikace. *Trestní právo*, 2011, roč. 15, č. 1, s. 15.

ostatně od platebního příkazu zřetelně rozlišuje, když v ustanovení § 2 odst. 3 písm. h) zákona č. 284/2009 Sb., o platebním styku, dále definuje jedinečný identifikátor jako kombinaci písmen, číslic nebo symbolů, kterými se podle určení poskytovatele identifikuje uživatel nebo jeho účet při provádění platebních transakcí, což není nic jiného než údaje, které pachatelé phishingem vylákávají.

Pachatelé phishingu proto dokonají trestný čin neoprávněného opatření, padělání a pozměnění platebního prostředku pouze v tom případě, že elektronický příkaz na základě podvodně získaných identifikačních údajů oběti zadají, čímž použijí padělaný platební prostředek jako pravý nebo platný podle § 234 odst. 3 alinea druhá tr. zákoníku, a to v jednočinném souběhu s trestným činem podvodu podle § 209 tr. zákoníku, popř. jeho pokusu. Dokud tak neučiní, bude jejich phishingové jednání možné posoudit pouze jako přípravu k těmto trestným činům.

## 5. ZÁVĚR

Tento příspěvek se snaží poukázat na teoretické i praktické problémy při posuzování trestnosti phishingu. Ty vycházejí zejména z určité rezignace orgánů činných v trestním řízení na pochopení jeho průběhu, a to zejména z důvodu nutnosti zabývat se jeho jednotlivými technickými aspekty, které se pro mnohé mohou zdát odtažitě a nepochopitelné. To ukazuje zejména předkládaný případ phishingu, který byl českými soudy posuzován. Aby totiž mohl být phishing správně trestně právně posouzen, musí být nejprve pochopen způsob a pozadí jeho provedení.

V první části tohoto příspěvku jsou v krátkosti představeni předchůdci phishingového jednání, jejichž metody jsou phishingem doposud využívány. Na předloženém případě jsou následně diskutovány jednotlivé problémové okruhy jeho trestněprávní kvalifikace, a to vzhledem k době jeho spáchání podle trestního zákona z roku 1961, v relevantním znění. Tato původní úprava je v této práci shledána jako nedostačující k postihu phishingu.

Určité změny do problematiky kyberkriminality, a to i phishingu, přinesl nový trestní zákoník. Poslední část tohoto příspěvku se proto zabývá otázkou, zdali lze phishing posoudit podle nově zavedených skutkových podstat trestných činů směřujících proti kyberkriminalitě. Z provedené analýzy ovšem vyplývá, že i současná úprava považuje za dokonaný trestný čin až moment, kdy pachatel phishingu provede elektronickou úhradu, resp. zadá elektronický příkaz k úhradě. Samotné opatření si přístupových údajů pomocí phishingu tak nadále lze stíhat pouze jako přípravu trestného činu podvodu a neoprávněného opatření, padělání a pozměnění platebního prostředku, a to při splnění podmínek trestnosti přípravy.



## PHISHING AND PROBLEMS WITH ITS LEGAL CLASSIFICATION IN THEORY AND PRACTICE

### Summary

This paper deals with the criminological and criminal law aspects of phishing, both in theory and practice of decision-making law enforcement agencies and judicial bodies. The contribution addresses the nature of this criminal phenomenon, its forerunners, and the usual *modus operandi* of the phishing. The second part of this paper consists of a study of concrete judicial case of phishing analyzing the problems with its legal classification, not only from the perspective of the former Czech criminal code, but also in the terms of the new Czech criminal code.

*Key words:* phishing, Penal code, criminal law

*Klíčová slova:* phishing, trestní zákoník, trestní právo



## VIRTUÁLNÍ DĚTSKÁ PORNOGRAFIE

MICHAELA POBOŘILOVÁ

Pornografie je v lidské společnosti chápána jako součást života, zejména sexuálního, sloužící k uspokojování sexuálních potřeb, avšak může být chápána i jako součást projevu života uměleckého. Pornografie je obecně členěna na jednotlivé subkategorie, mezi něž patří i pornografie dětská, která je snad v každé společnosti chápána negativně. Z hlediska trestního práva představuje jednu z nejzávažnějších forem trestné činnosti, neboť směřuje, resp. je zaměřena na členy společnosti, kteří vzhledem ke svému věku a rozumové vyspělosti nemají ještě dostatečné zkušenosti (psychické, životní) a možnosti správně se rozhodnout, a nebo dochází ke zneužívání proti jejich vůli. Všeobecně se dětská pornografie v jednotlivých státech odvíjí od společenských hodnot uznávaných konkrétní společností v určitém čase. Vztah společnosti, a potažmo i jedince, k pornografii je vztahem proměnným, tj. mění se v době a čase, a odráží aktuální postoj. Neblahý vliv na tento negativní fenomén mají informační technologie a technický rozvoj, který způsobuje nekontrolovatelnou produkci, distribuci a držení dětské pornografie, přičemž jedním z nejvýznamnějších zdrojů je Internet.<sup>1</sup> Jednání spočívající ve výrobě, šíření, případně jiném nakládání s dětskou pornografií prostřednictvím kyberprostoru tedy můžeme vymezit jako zločin, který využívá virtuální (digitální) prostředí.

### 1. PORNOGRAFIE A PORNOGRAFICKÉ DÍLO

*Pornografie* je slovo řeckého původu a skládá se ze spojení slov  *pornos* (prostitut, prostitutka) a *grafein* (psát). Encyklopedie a slovníky cizích slov vymezují podstatu tohoto slova zpravidla podobně. Jedná se o dílo zdůrazňující sexualitu a podněcující sexuální vzrušení, které překračuje obecně uznávané normy morálky a slušnosti.<sup>2</sup> V jednotlivých státech se pak můžeme setkat i s jinými pojmy, které pojem pornografie nahrazují nebo s ním úzce souvisí. Příkladem lze uvést pojem obscenita,

<sup>1</sup> Z hlediska České republiky viz např. tiskovou zprávu první internetové Internet Hotline z roku 2008 zachycující výsledky prvního roku provozu Internet Hotline, která byla založena 1. dubna 2007. Informace dostupná z: <http://www.nasedite.cz/webmagazine/articles.asp?idk=408&ida=481>.

<sup>2</sup> *Universum: Všeobecná encyklopedie*, 7. díl (Or–Q). Praha: Odeon, 2001, s. 414.

který se užívá zejména v americkém právním kontextu, a je vymezován jako neslušnost či nemravnost a nelze jej s pojmem pornografie zaměňovat.<sup>3</sup>

Pornografii z pohledu trestního práva můžeme chápat jen jako společenský jev negativní. Podle obsahu pornografického díla ji můžeme rozdělit na 3 kategorie:<sup>4</sup>

- a) *pornografie tvrdá*, do které spadají pornografická díla, v nichž se projevuje násilí či neúcta k člověku nebo která znázorňují pohlavní styk se zvířetem,
- b) *pornografie dětská*, do níž řadíme taková pornografická díla, která zobrazují, popř. jinak využívají dítě,
- c) *pornografie prostá*, kterou tvoří ostatní pornografická díla.

V současné době trestní zákoník,<sup>5</sup> ani žádný jiný právní předpis nedefinuje, co se pornografickým dílem rozumí. Vymezení a vyjádření této definice je ponecháno trestněprávní teorii a judikatuře. „Dílo“ je obecně definováno v ustanovení § 2 autorského zákona,<sup>6</sup> tj. je zde vymezeno dílo autorské jako předmět autorského práva. Předmětné ustanovení obsahuje demonstrativní výčet děl, která jsou pod autorskou ochranou, přičemž jsou rozdělena do jednotlivých kategorií (díla literární, jiná umělecká díla a díla vědecká). Dle autorského zákona mohou autorskoprávní ochrany požívat i díla pornografická za podmínky, že se jedná o dílo umělecké. V tomto směru je nutné, aby pornografie jako umělecké dílo mělo alespoň minimální tvůrčí charakter, přičemž pokud tento tvůrčí prvek chybí, není možno mluvit o díle ve smyslu autorském.<sup>7</sup> Naproti tomu, aby pornografické dílo bylo předmětem trestněprávního postihu, musí se jednat o dílo, které má veřejnoprávní charakter a vykazuje určitý stupeň společenské škodlivosti pro společnost. Reprobace takovýchto společensky nevhodných či nepřijatelných jevů je povahy veřejnoprávní, která nemá autorskoprávní (soukromoprávní) obsah, tzn. že se nejedná o žádný druh děl ve smyslu autorského práva.<sup>8</sup>

V teorii a praxi se za pornografické dílo považuje „dílo, které zvláště intenzivním a vtravým způsobem zasahuje a podněcuje sexuální pud, přičemž současně překračuje uznávané morální normy příslušné společnosti, čímž u většiny jejich členů vzbuzuje stud“.<sup>9</sup> Ústavní soud v této otázce judikoval, že pro účely trestního zákona je pornografickým dílem jakákoliv věc, pokud uráží, způsobem, který lze stěží akceptovat, cit pro sexuální slušnost. Pornografické dílo může u normální osoby vyvolávat sexuální vzrušení, vedle toho však může tuto osobu sexuálně znechucovat či odpuzovat.<sup>10</sup> Pornografické dílo je rovněž vyjádřeno jako „jakýkoli předmět, který, je-li pozorován ať přímo nebo prostřednictvím technického zařízení, zvláště intenzivním a vtravým způsobem zasahuje a podněcuje samotný sexuální pud. Současně takové dílo hrubě porušuje uznávané morální normy společnosti a vyvolává pocit studu.“<sup>11</sup>

<sup>3</sup> Srov. Miller v. California 413 U.S. 15 (1973), WESTLAW.

<sup>4</sup> ŠÁMAL, P. et al. *Trestní zákoník: komentář*. 2. díl (§ 140–421). 1. vydání. Praha: C. H. Beck, 2010, s. 1695.

<sup>5</sup> Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

<sup>6</sup> Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

<sup>7</sup> Srov. usnesení Nejvyššího soudu České republiky ze dne 18. 6. 2003, sp. zn. 5 Tdo 631/2003, ASPI.

<sup>8</sup> TELEČ, I., TUMA, P. *Autorský zákon. Komentář*. 1. vydání. Praha: C. H. Beck, 2007, s. 25.

<sup>9</sup> Usnesení Nejvyššího soudu České republiky ze dne 28. 12. 2004 sp. zn. 7 Tdo 1077/2004-I, ASPI.

<sup>10</sup> Usnesení Ústavního soudu České republiky ze dne 19. 4. 2004, sp. zn. IV. ÚS 606/03, ASPI.

<sup>11</sup> HERCZEG, J. Virtuální dětská pornografie: Zločin bez obětí? In: VANDUCHOVÁ, V., GRIVNA, T. (ed.). *Pocta Otovi Novotnému k 80. narozeninám*. Praha: ASPI, 2008, s. 38.

Podmínkou pornografického díla je, že takové dílo musí mít pornografický charakter a současně musí být zastoupen úmysl tvůrce k vytvoření díla s pornografickým charakterem, tj. musí být vytvořeno za účelem, aby sloužilo jako dílo pornografické. Musíme tedy mluvit o pornografické povaze díla, neboť ne každé takové dílo je předmětem trestního postihu. Příkladem mohou být historicky cenné předměty, předměty určené k vědeckým, vzdělávacím a osvětovým účelům, nebo umělecká díla, která i když zobrazují i ty nejintimnější chvíle člověka, nejsou považována za díla pornografická, a to i v případě, že mají pornografický charakter. Musí se naopak jednat o dílo, které bude hrubě porušovat morální hodnoty dané společností a na průměrného člověka bude dílo jako celek působit tak, že u něj vyvolá pocit studu, popř. takovou osobu bude znechucovat či odpuzovat, a celkově bude v rozporu s morálními hodnotami uznávanými v dané společnosti. Klíčový moment představuje určení, zda se jedná o dílo pornografické veřejnoprávního charakteru, neboť bez spojení těchto kritérií nemůže být nikdo trestně stíhán pro trestné činy uvedené v příslušných ustanoveních trestního zákoníku. Závěr o pornografickém charakteru díla musí být dovozován z celého obsahu díla, nikoli jen z určité části vytržené z kontextu. Tento závěr není možné vyvozovat například jen z určité pasáže, kapitoly, úryvku nebo z jednotlivé fotografie vyřazené z kolekce na sebe navazujících fotografií. Na druhé straně nelze závěr o pornografickém charakteru díla dovozovat bez dalšího jen z toho, že je prezentováno za účelem uspokojení osob trpících sexuální deviací, pro které jsou sexuálně atraktivní nedospělé osoby, například nelze paušálně hodnotit fotografické materiály jako pornografické jen z důvodu, že jsou na nich zachyceny děti a proto, že byly prezentovány na serveru určeném pedofilům.<sup>12</sup>

Posouzení charakteru díla musí být věnována pečlivá pozornost, neboť v konkrétním případě může dojít ke kolizi s právem na svobodu projevu stanovenou v čl. 17 Listiny základních práv a svobod (čl. 10 Evropské úmluvy o ochraně lidských práv a základních svobod), která tvoří jeden ze základů každé demokratické společnosti a znamená rovněž významný prostředek seberealizace jedince. V případě dětské pornografie je pak svoboda projevu úzce spjata s hodnotami, které příslušná společnost uznává a považuje za morální. Pokud tedy bude u díla shledán pornografický charakter ve smyslu veřejnoprávním, bude toto dílo stát mimo rámec ochrany svobody projevu. Test pornografické povahy díla spočívá na posouzení, zda jeho celkový dojem způsobuje morální pohoršení osobě s běžným citěním.<sup>13</sup> Morální pohoršení by však mělo být intenzivnějšího významu, neboť například některá umělecká díla mohou svým obsahem být díly pornografickými, avšak ne stíhatelnými podle trestního práva. Abychom mohli mluvit o pornografickém díle z pohledu trestního práva, musí jít o dílo, které nemá vážnou uměleckou, politickou nebo vědeckou hodnotu. Pokud dílo bude mít seriózní uměleckou hodnotu, pak nemůže být předmětem dětské pornografie.<sup>14</sup>

Důležitý předpoklad, ze kterého bude nutné vycházet, představují morální hodnoty společnosti, tzv. obecné standardy morálky. Morální hodnoty se mohou v jednotlivých společnostech odlišovat. Jiné chápání z pohledu dětské pornografie se projevuje v Ev-

<sup>12</sup> Usnesení Nejvyššího soudu České republiky ze dne 28. 12. 2004 sp. zn. 7 Tdo 1077/2004-I, ASPI.

<sup>13</sup> Usnesení Ústavního soudu České republiky ze dne 19. 4. 2004, sp. zn. IV. ÚS 606/03, ASPI.

<sup>14</sup> Srov. BARTON, M. Virtuální pornografie, limity svobody umělecké tvorby a svobody projevu a trestní zákon. *Právní rozhledy*, 2008, roč. 16, č. 17, s. 617–627.

ropě a jiné v asijských zemích.<sup>15</sup> Jednotné pojetí morálních standardů nenalezneme ani v případech menšího geografického určení, zaměřeného třeba jen na Evropu. Ústavní soud v této věci konstatoval, že svoboda projevu se vztahuje nejen na informace nebo ideje, které jsou vnímány příznivě či neutrálně, ale také na ty, které uráží, pohoršují, šokují či rozrušují stát nebo jakoukoliv část populace.<sup>16</sup> Tímto bylo deklarováno, že svoboda projevu je zaručena všem bez ohledu na hranice státu a současně Ústavní soud stanovil podmínku, že se musí jednat alespoň o část populace, která bude informace či ideje vnímat negativně. Otázkou pak zůstává, jak budou soudy posuzovat mínění části populace ohledně toho, co je v souladu s morálkou a co nikoliv. Jedním ze způsobů posuzování, zda informace či ideje má negativní dopad na společnost, a tudíž se vymyká obecným standardům morálky, může být vedle průzkumů a anket prováděnými různými institucemi i vyjádřením relevantního počtu občanů na internetových stránkách.<sup>17</sup>

Pornografické dílo může mít různou podobu. S podobou pornografického díla úzce souvisí a prolíná se i jeho forma. V dnešní době je nutné s ohledem na digitální a informační věk vzít v potaz skutečnost, že v mnoha případech pornografické dílo existuje pouze ve formě dat. Z tohoto důvodu je důležité zajistit, aby definice pornografického materiálu byla i co možná nejvíce technologicky neutrální. Za pornografické dílo by měl být považován materiál v jakékoliv formě nebo kombinaci forem, které jsou způsobilé založit nebo vytvořit komunikaci. Komunikací je myšlen jakýkoliv druh komunikace ve formě textu, slova, zvuku, vizuálních snímků, signálů, dat a dalších forem nebo jejich kombinací.<sup>18</sup>

Trestní zákoník uvádí demonstrativní výčet podob pornografického díla. Pornografické dílo může mít formu písemnou, fotografickou, filmovou, počítačovou, elektronickou nebo jinou.<sup>19</sup> Pokud se jedná o vyjádření rozdílu mezi dílem počítačovým a elektronickým, tak prvním dílem se rozumí dílo vytvořené pomocí počítače, elektronickým dílem to, které má podobu čitelnou jen strojově.<sup>20</sup> Podmínkou počítačového díla je, že musí být vytvořeno pomocí počítače, tzn. že půjde o dílo vytvořené ve virtuálním prostředí, které pak dále bude moci být rovněž dílem elektronickým a jeho obsah bude moci být produkován pomocí elektronické podoby zaznamenané na technické zařízení. Podoba demonstrativního výčtu byla zvolena zejména proto, aby reflektovala možný budoucí technický vývoj, čímž vložením slovního spojení „jiné pornografické dílo“ otevřela možnost extenzivního výkladu podob pornografického díla, resp. možnost subsumovat pod tento pojem jakákoliv nová technická zařízení a nové formy či podoby, které v budoucnu vzniknou a prostřednictvím nichž budou pornografická díla seznatelná.

<sup>15</sup> V evropských zemích je dětská pornografie posuzována přísněji, než je tomu v Japonsku. Srov. POREMSKÁ, M. Pornografie v USA. *Trestněprávní revue*, 2008, č. 8, s. 237.

<sup>16</sup> Usnesení Ústavního soudu České republiky ze dne 19. 4. 2004, sp. zn. IV. ÚS 606/03, ASPI.

<sup>17</sup> Srov. usnesení Nejvyššího soudu České republiky ze dne 12. 7. 2006, sp. zn. 8 Tdo 763/2006, ASPI. Ve věci uložení trestu odnětí svobody na doživotí byl konstatován závěr, že lze připustit jako pramen důkazu i vyjádření občanů na internetových stránkách. Dle mého názoru by bylo možné tento případ analogicky vztáhnout i na případ, kdy by se zjišťovala otázka, zda se jedná o dílo pornografického charakteru, tj. zjištění aktuálního stavu vnímání obecných standardů morálky ve společnosti.

<sup>18</sup> CLOUGH, J. *Principles of Cybercrime*. New York: Cambridge University Press, 2010, s. 265.

<sup>19</sup> K výkladu jednotlivých pojmů viz ŠAMAL, P. et al. *Trestní zákoník: komentář*. 2. díl (§ 140–421). 1. vydání. Praha: C. H. Beck, 2010, s. 1695.

<sup>20</sup> GRIVNA, T. Trestné činy proti lidské důstojnosti v sexuální oblasti v novém trestním zákoníku. *Bulletin advokacie*, 2009, č. 10, s. 70.

## 2. POJEM DÍTĚ

Pro účely dětské pornografie je důležité vyložit, kdo nebo co se rozumí pod pojmem dítě. Trestní zákoník v ustanovení § 126 uvádí, že dítětem se rozumí osoba mladší osmnácti let, pokud trestní zákon nestanoví jinak. V dřívějších trestněprávních předpisech pojem dítě definován přímo nebyl, výjimku bylo relativně možné spatřovat v ustanovení § 216b zákona č. 140/1961 Sb., trestní zákon, který stanovoval, že dítětem se rozumí osoba mladší než osmnáct let. Toto vymezení se ovšem vztahovalo pouze k trestnému činu únosu a obchodování s dětmi. Přestože pojem dítěte nebyl dříve legislativně vymezen, nečinil jeho výklad v praxi problémy.

Výše uvedená definice dítěte vychází z Úmluvy o právech dítěte,<sup>21</sup> která jej v čl. 1 definuje jako každou lidskou bytost mladší 18 let, pokud podle právního řádu, jenž se na dítě vztahuje, není zletilosti dosaženo dříve. V této souvislosti je třeba zmínit, že náš právní řád dovoluje nabytí zletilosti ještě před dosažením 18. roku věku, a to uzavřením manželství za podmínek stanovených zákonem.<sup>22</sup> Takovéto nabytí zletilosti však z hlediska trestního práva nemá vliv a osoba bude i nadále považována za dítě, dokud reálně, tj. plynutím času, nedosáhne 18. roku života.

Pojem dítě vymezuje i Rámcové rozhodnutí Rady EU o boji proti pohlavnímu vykořisťování dětí a dětské pornografii.<sup>23</sup> Podle čl. 1 písm. a) se pro účely tohoto rámcového rozhodnutí rozumí dítětem každá osoba mladší 18 let. Jiným významným dokumentem vymezujícím pojem dítě z hlediska dětské pornografie je Úmluva o kybernetické kriminalitě (dále jen „Úmluva“).<sup>24</sup> Úmluva nepoužívá pojem dítě, ale „nezletilá osoba“ (minor). V čl. 9 odst. 3 se uvádí, že pojem nezletilá osoba zahrnuje všechny osoby mladší 18 let. Smluvní strana Úmluvy může stanovit nižší věkovou hranici, která však nesmí být nižší než 16 let. Tímto vymezením Úmluva reaguje na situace, kdy zletilost je v jednotlivých státech nabyvána dříve než dosažením 18. roku života, tj. stanovuje nižší věkovou hranici pro chápání osoby jako dítěte. V české trestněprávní nauce je za nezletilou osobu považována osoba, která se nachází v životním období od 15. do 18. roku života. Takto věkově vymezená osoba je nazývána jako osoba mladistvá, i ta je však považována za dítě ve výše vyloženém významu.

V souvislosti s pojmem dítě a pornografie je nutné si uvědomit rozdílnost spočívající v dobrovolném souhlasu se zapojením do aktivního sexuálního života. V České republice je zákonné provádění sexuálních aktivit limitováno věkovou hranicí 15 let. I když od dosažení tohoto věku lze žít sexuálním životem, je nezbytnou podmínkou, aby takovéto jednání bylo beztrestné, souhlas osoby provádějící jakoukoliv sexuální aktivitu. Výjimku představuje právě dětská pornografie, neboť pokud by osoba mladší 18 let dala souhlas například se záznamem sexuální aktivity na videokameru, pak je takový souhlas zcela bezvýznamný a osoba, která stiskne nahrávání na videokameře,

<sup>21</sup> Úmluva o právech dítěte byla podepsána 20. 11. 1989 v New Yorku, pro ČR závazná od 6. 2. 1991 (sdělení č. 104/1991 Sb.).

<sup>22</sup> Ustanovení § 8 odst. 2 zák. č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů, dovoluje nabytí zletilosti ve věku 16 let.

<sup>23</sup> Rámcové rozhodnutí Rady 2004/68/SVV ze dne 22. 12. 2003 o boji proti pohlavnímu vykořisťování dětí a dětské pornografii.

<sup>24</sup> Úmluva o kybernetické kriminalitě byla podepsána dne 23. 11. 2001, ČR ji podepsala dne 4. 2. 2005, doposud nedošlo k její ratifikaci, a tudíž není prozatím pro Českou republiku závazná.

bude stíhána za trestný čin výroby dětské pornografie dle ustanovení § 192 trestního zákoníku. Osoba mladší 18 let si tedy může dobrovolně zvolit, že se zapojí do sexuálního života, ale nemůže si dobrovolně zvolit, že bude subjektem pornografického díla (dětské pornografie).

### 3. DĚTSKÁ PORNOGRAFIE

Pojem dětské pornografie není v našem právním řádu vyjádřen žádnou legální definicí, a proto je její výklad ponechán trestněprávní nauce a judikatuře. Za dětskou pornografii se považují taková pornografická díla, která znázorňují nebo jinak využívají dítě. Česká judikatura pak vymezila dětskou pornografii jako jakékoli zobrazování dítěte libovolnými prostředky při skutečných nebo předstíraných zřejmých sexuálních aktivitách či jakékoli zobrazování pohlavních orgánů dítěte k prvotně sexuálnímu účelům. Za dětskou pornografii jsou pak zejména považovány snímky obnažených dětí v polohách vyzývavě předvádějících pohlavní orgány za účelem sexuálního uspokojení, snímky dětí zachycující polohy skutečného či předstíraného sexuálního styku s nimi, popř. i jiné obdobně sexuálně dráždivé snímky dětí. Musí jít o pornografická díla veřejnoprávního charakteru, přičemž hlavní charakteristikou je skutečnost, že tato díla jsou primárně určena k sexuálnímu účelům, a musí pohoršovat průměrného pozorovatele. Z toho vyplývá, že za dětskou pornografii nejsou považovány rodinné snímky nahých dětí, neboť postrádají výše uvedené znaky. Za pornografické dílo dále není možno označit snímky, byť i zachycující částečně či plně obnažené děti, které působí sexuálně stimulujícím způsobem na jedince pohlavně deviantního, pokud nesplňují kritéria pornografického charakteru.<sup>25</sup> Z hlediska trestního práva není trestné ani pořizování snímků dětí při sportovních aktivitách nebo hrajících si v zábavních centrech nebo hřištích osobami trpících sexuální deviací, přestože tyto snímky budou na ně působit sexuálně stimulujícím způsobem. Takové snímky bývají nazývány jako tzv. doplňkové snímky dětské pornografie. Doplňkové snímky mohou mít z hlediska postihu dětské pornografie význam jen tehdy, pokud jsou umístěny v albu spolu se sexuálními snímky dětí, kdy navíc k nim mohou být přidány popisky, čímž může dojít ke změně významu těchto snímků, a jejich dominantní účel nebo charakteristika se stává nezaměnitelně sexuální z pohledu průměrného pozorovatele.<sup>26</sup> Doplňkové snímky v tomto kontextu nejsou trestně postižitelné, avšak mohou vést v procesu dokazování k závěru, že osoba trpí příslušnou sexuální deviací.

Dětskou pornografii vymezují i mezinárodní dokumenty. Opční protokol k Úmluvě o právech dítěte o prodeji dětí, dětské prostituci a dětské pornografii<sup>27</sup> v čl. 2 písm. c) rozumí dětskou pornografií zobrazování dítěte libovolnými prostředky při skutečných nebo předstíraných zřejmých sexuálních aktivitách či jakékoli zobrazování pohlavních orgánů dítěte k prvotně sexuálnímu účelům. Rámcové rozhodnutí o boji proti pohlav-

<sup>25</sup> Usnesení Nejvyššího soudu České republiky ze dne 28. 12. 2004 sp. zn. 7 Tdo 1077/2004-I, ASPI.

<sup>26</sup> CLOUGH, J. *Principles of Cybercrime*. New York: Cambridge University Press, 2010, s. 263.

<sup>27</sup> Opční protokol k Úmluvě o právech dítěte o prodeji dětí, dětské prostituci a dětské pornografii ze dne 20. 5. 2000 dosud Česká republika neratifikovala, a to z toho důvodu, že v našem právním řádu není dostatečným způsobem upravena odpovědnost právnických osob.



nímu vykořisťování dětí a dětské pornografii<sup>28</sup> v čl. 1 písm. b) vymezuje dětskou pornografii jako pornografický materiál, který zobrazuje skutečné dítě, skutečnou osobu se vzhledem dítěte a realistické znázornění neexistujícího dítěte, které se aktivně nebo pasivně účastní zjevně sexuálního jednání, a to včetně dráždivého vystavování přirození nebo ohanbí dítěte.

Úmluva o kybernetické kriminalitě vymezuje dětskou pornografii v čl. 9 odst. 2 jako pornografický materiál, který vizuálně zobrazuje nezletilého při zjevném sexuálním chování nebo osobu, která se jeví jako nezletilá při zjevném sexuálním chování, nebo realistické zobrazení nezletilé osoby při zjevném sexuálním chování. Výkladový problém by mohl vzniknout při vymezení pojmu „vizuální zobrazení“, kterým se pravděpodobně rozumí každé zobrazení, které může být pozorovatelné zrakem, tj. je viditelné jedním ze smyslů člověka. Smluvním státům je pak ponechána možnost trestně nepostihovat jednak obstarávání dětské pornografie pomocí počítačového systému pro svou potřebu či pro jiného, jednak držení dětské pornografie v počítačovém systému. Možnost výjimky je upravena i pro případ pornografického materiálu, jehož aktérem je osoba starší 18 let, avšak vypadající jako nezletilá, a také materiálu zobrazujícího realistické znázornění neexistujícího dítěte.

Pro všechny výše uvedené mezinárodní definice dětské pornografie je společný pojem „zjevné sexuální chování“, které pokrývá následující chování:

- a) skutečný nebo předstíraný sexuální styk (styk pohlavní, orální nebo anální) mezi nezletilými osobami navzájem nebo nezletilou a dospělou (zletilou) osobou, stejného nebo opačného pohlaví,
- b) skutečnou nebo předstíranou bestialitu,<sup>29</sup>
- c) skutečnou nebo předstíranou masturbaci (onanii),
- d) skutečné nebo předstírané sadistické nebo masochistické zneužívání v sexuálním kontextu,
- e) skutečné nebo předstírané lascivní (chlípné) vystavování genitálií nebo intimních částí (ohanbí) nezletilé osoby.

Výše uvedená chování jsou ve spektru dětské pornografie považována za nejzávažnější a jsou řazena mezi nejtěžší stupně všeobecně uznávané typologie COPINE.<sup>30</sup>

#### 4. VIRTUÁLNÍ DĚTSKÁ PORNOGRAFIE

Vedle tzv. *dětské pornografie skutečné*, tj. takové, která zobrazuje skutečné dítě z masa a kostí, existuje v současné technologicky moderní době i tzv. *dětská pornogra-*

<sup>28</sup> Rámcové rozhodnutí Rady ze dne 22. prosince 2003 o boji proti pohlavnímu vykořisťování dětí a dětské pornografii (2004/68/SVV).

<sup>29</sup> Anglický termín „bestiality“ lze přeložit také jako styk se zvířaty (sodomie).

<sup>30</sup> Combating Paedophile Information Network; jedná se o projekt vytvořený univerzitou College Cork v Irsku, který je zaměřen na výzkum problému zneužívání dětí na Internetu. Uvedená typologie je jedním z výstupů tohoto projektu a vychází z ní definice dětské pornografie obsažená v Úmluvě o kyberkriminalitě. Blíže viz Důvodová zpráva k Úmluvě o kyberkriminalitě přijatá Výborem ministrů Rady Evropy na svém 109. zasedání (8. listopadu 2001), dostupná z: <http://conventions.coe.int/treaty/en/reports/html/185.htm>; CLOUGH, J. *Principles of Cybercrime*. New York: Cambridge University Press, 2010, s. 259.

fie virtuální. V souvislosti s kyberprostorem pak můžeme pohlížet na dětskou pornografii ze dvou směrů:<sup>31</sup>

- a) *dětskou pornografii ve virtuálním prostředí*, kdy do této kategorie řadíme dětskou pornografii skutečnou, která je dále v rámci kyberprostoru,<sup>32</sup> zejména Internetu, rozšiřována,
- b) *virtuální dětskou pornografii*, tj. takovou, která nezobrazuje žádné skutečné dítě, ale jedná se o díla, jejichž ústředním motivem je zobrazení nereálného dítěte vytvořeného v rámci kyberprostoru, přičemž tuto není možné spáchat mimo virtuální prostředí.

V souvislosti s nazíráním na dětskou pornografii, která nezobrazuje skutečné dítě, je možné vycházet také z členění podle její podoby na:

- a) dětskou pornografii vytvořenou v rámci kyberprostoru (např. animace, fotografie nezobrazující skutečné dítě vytvořené pomocí počítačového programu – fotomontáž, vytvoření filmových postav jako tzv. kyborgů<sup>33</sup> nebo androidů<sup>34</sup>),
- b) chápání jejího vytvoření jako fikce, tj. i zde nevystupuje skutečné dítě, avšak jedná se o vytvoření mimo kyberprostor (např. literární díla, sochy).<sup>35</sup>

Virtuální dětská pornografie je nejširěji pojata v Úmluvě o kybernetické kriminalitě, a to jednak ve formě vymezení pornografického materiálu, který je považován za dětskou pornografii, jednak ve formě výčtu jednání spojených s dětskou pornografií, která mohou být trestným činem. Úmluva pokrývá jak dětskou pornografii ve virtuálním prostředí v rámci postihu vizuálního zobrazení sexuálního zneužívání skutečných dětí, tak i virtuální dětskou pornografii v souvislosti s postihem pornografického materiálu, které zobrazuje osobu, která se jeví jako nezletilá, nebo realisticky zobrazuje nezletilou osobu, která není skutečným dítětem, při zjevném sexuálním chování. Obdobně je tomu tak i v Rámcovém rozhodnutí o boji proti pohlavnímu vykořisťování dětí a dětské pornografii, které výslovně definuje jako dětskou pornografii materiál, který zobrazuje skutečné dítě, skutečnou osobu se vzhledem dítěte nebo realistické znázornění neexistujícího dítěte, které se aktivně nebo pasivně účastní zjevně sexuálního jednání, a to včetně dráždivého vystavování přirození nebo ohanbí dítěte.

Úmluva o kybernetické kriminalitě současně pro oba druhy virtuální dětské pornografie vymezuje jednání spočívající v úmyslné(m) protiprávní(m):<sup>36</sup>

<sup>31</sup> Uvedené dělení je pro tento příspěvek stěžejní a nadále v textu se z něj vychází.

<sup>32</sup> Kyberprostor se skládá ze stovek tisíců vzájemně propojených počítačů, serverů, směšovačů (router), přepínačů (switch) a optických kabelů; prostor, do něhož vstupují sociální aktéři, kteří používají ke vzájemné sociální interakci pokročilé informační technologie. Blíže srov. POLČÁK, R., ŠKOP, M., MACEK, J. *Normativní systémy v kyberprostoru*. 1. vydání. Brno: MU, 2005, s. 7 n.

<sup>33</sup> Původně živé-přírodní tělo obohacené o mechanické či elektronické části, jejichž montáž, popř. demontáž se provádí pomocí chirurgického zákroku. Podstatou je zde představa techniky parazitující na živém těle. Definice dostupná z: <http://cs.wikipedia.org/wiki/Kyborg>.

<sup>34</sup> Umělá, mechanická napodobenina člověka. *Akademický slovník cizích slov*, I. díl (A–K). Praha: Academia, 1995, s. 51.

<sup>35</sup> V tomto článku není nadále dětské pornografii, která nezobrazuje skutečné dítě, jako fikci věnována pozornost.

<sup>36</sup> Blíže viz Důvodová zpráva k Úmluvě o kyberkriminalitě přijatá Výborem ministrů Rady Evropy na svém 109. zasedání (8. listopadu 2001), dostupná z: <http://conventions.coe.int/treaty/en/reports/html/185.htm>; CLOUGH, J. *Principles of Cybercrime*. New York: Cambridge University Press, 2010, s. 281 n.

- a) výrobě dětské pornografie pro účely její distribuce prostřednictvím počítačového systému,
- b) nabízení nebo zpřístupňování dětské pornografie prostřednictvím počítačového systému,
- c) distribuci nebo přenášení dětské pornografie prostřednictvím počítačového systému,
- d) obstarávání dětské pornografie prostřednictvím počítačového systému pro sebe nebo jinou osobu (smluvní strana si může vyhradit právo zcela nebo zčásti toto jednání nepostihovat),
- e) držení dětské pornografie v počítačovém systému nebo na médiu pro ukládání počítačových dat (smluvní strana si může vyhradit právo zcela nebo zčásti toto jednání nepostihovat).

*Výrobou* se rozumí výroba dětské pornografie za účelem její distribuce prostřednictvím počítačového systému. Za výrobu je možné považovat vytváření fotografií a obrazových záznamů, vytváření reprodukcí existujících snímků kopírováním, skenováním, používání počítačových softwarů k vytvoření nereálného dítěte a další formy.

*Nabízení* má pokrýt poskytnutí možnosti jiným osobám získat dětskou pornografii, přičemž osoba, která takový materiál nabízí, jej může skutečně poskytnout. *Zpřístupněním* se rozumí činnost spočívající v uvádění a zpřístupnění dětské pornografie pro využití jinými osobami. Tyto formy se nemusí nutně týkat aktivního šíření dětské pornografie, ale jednoduše stačí nabídnout takové materiály jiným osobám, resp. širšímu okruhu osob například uveřejněním, ukazováním nebo inzerováním. Příkladem může být vytvoření webových stránek s dětskou pornografií či vytvoření nebo kompilace odkazů za účelem usnadnění přístupu na webové stránky s dětskou pornografií, přičemž se nevyžaduje, aby takový materiál byl ve skutečnosti z těchto stránek stažen.

*Distribuce* zahrnuje aktivní šíření dětské pornografie. Pod *přenášením* lze zařadit posílání dětské pornografie prostřednictvím počítačového systému jiné osobě. Distribuce a přenášení dětské pornografie představují jednu z nejvýznamnějších oblastí, kterou se snaží jednotlivé státy kriminalizovat s ohledem na vývoj informačních technologií a jejich běžné, časté, snadné a dostupné používání. V této souvislosti lze hovořit i o přepravování, dovážení a vyvážení z jednoho místa na druhé, které je spíše zažité pro fyzický pohyb věcí (zboží), avšak je možné na tento kontext nahlížet i z pohledu přepravování, dovážení a vyvážení dat jako ekvivalentu k fyzickému pohybu a přenosu (například přeshraniční stažení dětské pornografie).

*Obstaráváním* je míněno aktivní získávání dětské pornografie pro sebe nebo jiného, například stahováním. Pod obstaráváním je pak možné si představit relevantní chování spočívající v umožnění přístupu (zobrazení nebo prohlížení materiálu na počítači nebo jiný výstup v seznatelné podobě), požadování a obdržení (musí se jednat o vědomé obdržení vizuálního zobrazení stažením od jiné osoby nebo získáním z držení jinou osobou) materiálů zachycující dětskou pornografii.

*Držení* zde lze rozeznávat ve dvou formách. První formou je prostá držba, která sama o sobě může založit spáchání trestného činu, druhou formou je doplňková držba spočívající v úmyslu materiál s dětskou pornografií prodávat, dodávat nebo nabízet jiným osobám. Držení dětské pornografie podněcuje poptávku a nabídku po takovém

materiálu, a proto se jednotlivé státy snaží vymýtit tento jev, zejména pokud se jedná o držení v úmyslu materiál dále nabízet a šířit.

## 5. OTÁZKY SOUVISEJÍCÍ S VIRTUÁLNÍ DĚTSKOU PORNOGRAFIÍ

Jak bylo výše uvedeno, základem virtuální dětské pornografie je, že zde nedochází ke zneužívání či jinému využívání skutečného dítěte, ale dítěte ve skutečnosti neexistujícího. Vystává však otázka, zda virtuální pornografická díla mohou být předmětem trestního postihu, neboť primárním důvodem proč problematika dětské pornografie byla upravena, byl zájem na ochraně skutečných dětí před jejich zneužíváním a vykořisťováním v sexuální oblasti.

Původním objektem trestných činů souvisejících s dětskou pornografií byl a nadále i zůstává zájem společnosti na ochraně mravního vývoje dětí a jejich ochraně před sexuálním zneužíváním. Abychom mohli mluvit o virtuální dětské pornografii, musí být splněna podmínka, že se musí jednat o dílo, které má pornografický charakter ve smyslu trestního práva, tzn. že se musí jednat o charakter veřejnoprávní. Při takovém hodnocení totiž zejména zde vystupuje do popředí otázka zásahu do ústavně zaručeného práva na svobodu projevu.<sup>37</sup> Musí se jednat o dílo, jehož obsahem bude sexuální aktivita zneužívající nebo jinak využívající neexistující dítě. Z tohoto důvodu nemůžou být trestně například animace, které zobrazují sexuální chování dospělých animovaných osob, tj. starších 18 let.

V případě virtuální dětské pornografie zájem na ochraně před sexuálním zneužíváním dětí nelze přímo dovodit, neboť zde nevystupuje konkrétní skutečný jednotlivec, a proto primárním objektem je ochrana mravního vývoje dětí. Lze se setkat i s názorem, že individuálním objektem je ochrana společnosti před potencionálně nebezpečným jednáním, které může vést až ke skutečnému zneužívání dětí.<sup>38</sup> Někteří autoři zabývající se touto problematikou dovozují, že objektem ochrany v případě virtuální dětské pornografie nemá být mravnost, nýbrž ochrana dětí.<sup>39</sup> Pro ochranu mravního vývoje dítěte a tedy skutečnosti, jak může virtuální pornografie ovlivnit vztah dítěte k sexuálnímu životu, lze uvést argument, že když dítě uvidí sexuální animaci, v níž bude v sexuálním aktu jako aktér vystupovat například Lisa Simpson, která je vykreslena v seriálu Simpsonovi<sup>40</sup> jako kladná postava s pozitivními lidskými vlastnostmi, a tudíž v očích dítěte chápána jako „správná osoba“, přičemž můžeme předpokládat, že dítě nižšího věku není rozumově natolik vyspělé a sexuálně zralé, aby si bylo plně vědomo toho, co vidí, dítě pak může animaci vnímat tak, že když „to“ dělá Lisa, tak na tom není nic špatného a můžu „to“ dělat i já. Stejný vliv by samozřejmě mohla mít i animace pro

<sup>37</sup> Srov. Miller v. California 413 U.S. 15 (1973); BARTOŇ, M. Virtuální pornografie, limity svobody umělecké tvorby a svobody projevu a trestní zákon. *Právní rozhledy*, 2008, roč. 16, č. 17, s. 619–620.

<sup>38</sup> VOLEVEČKÝ, P., ŠUBRT, M. Dětská pornografie jako kybernetický trestný čin ve světle Úmluvy o počítačové kriminalitě. *Trestní právo*, roč. 2009, č. 4, s. 16.

<sup>39</sup> Srov. BARTOŇ, M. Virtuální pornografie, limity svobody umělecké tvorby a svobody projevu a trestní zákon. *Právní rozhledy*, 2008, roč. 16, č. 17, s. 624.

<sup>40</sup> Americký animovaný televizní seriál. Blíže viz: <http://www.csfd.cz/film/72489-simpsons-the>.

dospělé, tj. animace, v níž by aktérem sexuálního chování byla dospělá osoba, tj. osoba starší 18 let, například Sněhurka, která je rovněž v očích dětí chápána jako kladná postava. Argumentem proti výše uvedenému chápání animace je, že se jedná pouze o předpoklad, že animace ze strany dítěte bude tímto způsobem vykládána.<sup>41</sup> Na obdobném základě je postaven argument záležející v pozitivní možnosti ovlivnění pohlavních deviantů, neboť virtuální pornografie by mohla být pro řadu z nich alternativou, která by jim umožnila realizovat své potřeby na úrovni masturbačních fantazií, a tím by se snížilo riziko, že své potřeby skutečně realizují. Opačný argument, který se nabízí, je názor, že virtuální dětská pornografie jen zvyšuje chuť pedofilů a dodává jim odvalu účastnit se nezákonných činů.<sup>42</sup> V tomto případě již do popředí vystupuje zájem na ochraně dětí před jejich zneužíváním. Ve všech výše uvedených věcech se jedná pouze o předpoklady. Tyto situace můžeme srovnat s tvrzeními, která byla a jsou v poslední době prezentována vědci, teoretiky nebo sdělovacími prostředky, konkrétně, že násilí prezentované ve filmech a videohrách ovlivňuje chování a vnímání dětí ve skutečném životě. Samozřejmě i zde máme zastánce, kteří tuto teorii podporují, a na druhé straně ty, kteří ji nezastávají. Reálným faktem ovšem zůstává, že ve světě již existují případy, kdy jednání osob bylo ovlivněno počítačovými hrami, a to s přímým odkazem pachatelů na jejich názvy. Jedním z těchto případů je tzv. Kolumbijský masakr,<sup>43</sup> kdy dva studenti, po předchozím naplánování a přípravě, v kafetérii střední školy usmrtili několik svých spolužáků a jednoho profesora střelnými zbraněmi, které si s sebou přinesli do školy. Ještě před spácháním svého činu natočili domácí video, v němž přímo odkazují na počítačovou hru slovy: „Bude to jako ten podělanej Doom... Tahle podělaná brokovnice je jako vystřižená z Dooma!“<sup>44</sup> Zastánci teorie, že násilí ve virtuálním světě ovlivňuje chování dětí ve světě reálném, teď mají v ruce skutečný argument, kterým mohou operovat. Tímto případem mělo být demonstrováno, že i v případě virtuální dětské pornografie by neměl být opomíjen fakt, že virtuální svět je dnes každodenní běžnou součástí života, že se může promítat do reality a ovlivňovat chování a vnímání osob.

Jelikož v rámci virtuální dětské pornografie nejde o skutečné dítě, vyvstává otázka co, popř. kdo bude jejím předmětem. Možnost, že předmětem dětské pornografie bude neexistující dítě, upravuje Rámcové rozhodnutí Rady o boji proti pohlavnímu vykořisťování dětí a dětské pornografii, tzn. že v rámci Evropské unie je připuštěno, že předmětem dětské pornografie mohou být i virtuální pornografická díla. V daném případě je však podmínkou, že se musí jednat o realistické znázornění dítěte, tj. případ, kdy dílo z hlediska průměrného pozorovatele vypadá jako dokument o skutečném pohlavním zneužívání dítěte.<sup>45</sup> Důležitá bude míra realističnosti virtuálního pornografického díla. S ohledem na stále pokračující technický vývoj bude čím dál obtížnější rozeznat dítě skutečné a nereálné (tuto úvahu nelze vztáhnout na animace, neboť zde vždy víme, že se nebude jednat o skutečné dítě). Konzumenti takového díla by se mohli obhajovat právě

<sup>41</sup> Srov. McEWEN v. SIMMONS & ANOR (2008), New South Wales Supreme Court, NSWSC 1292, dostupné z: <http://lawlink.nsw.gov.au/scjjudgments/2008nswsc.nsf/2008ns>.

<sup>42</sup> HERCZEG, J. Virtuální dětská pornografie: Zločin bez obětí? In: VANDUCHOVÁ, V., GRIVNA, T. (ed.). *Pocta Otovi Novotnému k 80. narozeninám*. Praha: ASPI, 2008, s. 47.

<sup>43</sup> Informace dostupná z: [http://cs.wikipedia.org/wiki/Masakr\\_na\\_Columbine\\_High\\_School](http://cs.wikipedia.org/wiki/Masakr_na_Columbine_High_School).

<sup>44</sup> Informace dostupná z: <http://www.project-syndicate.org/commentary/singer26/Czech>.

<sup>45</sup> HERCZEG, J. Virtuální dětská pornografie: Zločin bez obětí? In: VANDUCHOVÁ, V., GRIVNA, T. (ed.). *Pocta Otovi Novotnému k 80. narozeninám*. Praha: ASPI, 2008, s. 43.

tím, že se nejedná o skutečné dítě.<sup>46</sup> Jako příklad lze uvést situaci, kdy bude natočen film se skutečnými lidskými bytostmi, přičemž jedním z aktérů bude virtuálně upravený a do filmu přidán android nebo kyborg, který bude prokazatelně mladší 18 let, přičemž následně u tohoto díla nevznikne pochybnost, že se jedná o dílo zachycující dětskou pornografii.<sup>47</sup> V tomto konkrétním případě by určitě bylo možné vzít v potaz hledisko společenské škodlivosti, které by zde mělo pravděpodobně větší váhu než v případě animace, resp. společenská škodlivost by zde mohla dosahovat menší míry než u animací, záleželo by však na konkrétních okolnostech případu.

Není pochyb o tom, že dítě je zároveň osobou, a proto další otázkou, která v souvislosti s virtuální dětskou pornografií vyvstává, je, zda kreslená postava může být považována za „osobu“ z právního hlediska. I zde se názory různí. Jedním z takových názorů je, že se o „osobu“ jednat nemůže, neboť by se jednalo o extenzivní rozšiřování trestní odpovědnosti na situace, které neměl zákonodárce v úmyslu postihovat.<sup>48</sup> Pojem osoby v právním významu lze považovat za pojem historický a obecně se jím rozumí fyzické a právnické osoby.<sup>49</sup> Fyzická osoba je dnes chápána jako skutečná osoba, tj. jednotlivec z masa a kostí. Vzhledem k době vzniku a utváření pojmu fyzické osoby rozhodně nebylo možné počítat s variantou virtuálního prostředí, neboť zákonodárci v době zavádění tohoto pojmu nebyla pravděpodobně známa. Kreslenou nebo animovanou postavu je však možné považovat za osobu ve smyslu právním za předpokladu, že taková postava se svým ztvárněním podobá člověku. V opačném případě by bylo nutné posoudit, jak moc se kreslená postava odchyľuje od ztvárnění člověka a zda je takové zobrazení způsobilé založit trestný čin. V daném případě by nestačilo pouhé přiřazení lidských vlastností například animovanému králíkovi nebo kachně, neboť takové zobrazení nelze chápat tak, že se jedná o vyjádření osoby, dokonce i když animovaný králík nebo kachna mají povahové rysy, které jsou zřetelně lidské.<sup>50</sup> Z pohledu postavení virtuálních osoby by právo nemělo být rigidní, resp. nemělo by být vykládáno zcela rigidně, ale naopak by mělo pružně reagovat na situace a prostředí v daném čase a místě. Rovněž by mělo reflektovat chápání a standardy společnosti. Jelikož virtuální svět překračuje pomyslnou hranici světa reálného, stává se jeho každodenní součástí, je možné brát v potaz i úvahy směřující k chápání kreslených postav jako právních entit, a tudíž by bylo možné rozšířit pojem osoby v právním významu. Samozřejmě i zde by musely platit určité hranice, kdy takové chápání kreslených postav jako právních entit by nebylo možné z povahy věci použít u všech skutkových podstat trestných činů (např. únos dítěte).

<sup>46</sup> Srov. BARTOŇ, M. Virtuální pornografie, limity svobody umělecké tvorby a svobody projevu a trestní zákon. *Právní rozhledy*, 2008, roč. 16, č. 17, s. 621.

<sup>47</sup> Jako příklad lze pro srovnání uvést filmové zpracování Jaws 3-D (Čelisti 3), ve kterém vystupují skuteční herci, a počítačově je zde pak upraven žralok. Dostupné z: <http://www.csfid.cz/film/19676-jaws-3d/>.

<sup>48</sup> VOLEVECKÝ, P., ŠUBRT, M. Dětská pornografie jako kybernetický trestný čin ve světle Úmluvy o počítačové kriminalitě. *Trestní právo*, 2009, č. 4, s. 19. Dále srov. McEWEN v. SIMMONS & ANOR (2008), New South Wales Supreme Court, NSWSC 1292 (blíže pojednáno v kapitole Případové studie).

<sup>49</sup> Právnická osoba však nemůže vystupovat jako předmět v rámci kontextu virtuální dětské pornografie. Naopak je však možné, že by mohla být pachatelem trestného činu souvisejícího s virtuální dětskou pornografií.

<sup>50</sup> Srov. McEWEN v. SIMMONS & ANOR (2008), New South Wales Supreme Court, NSWSC 1292, dostupné z: <http://lawlink.nsw.gov.au/scjgments/2008nswsc.nsf/2008ns>.

Další důležitou otázkou je, zda virtuální dítě (osoba) může mít věk. V daném kontextu není možné hovořit o věku v rámci plynutí času, ale v potaz lze brát tzv. „věk zdánlivý“, tj. věk, který může být virtuální osobě přisouzen na základě pozorovatelných tělesných znaků. Věk virtuálního dítěte lze odvodit z jeho vzhledu, přičemž může být jasné, že se jedná o dítě mladší 18 let (např. animované batole), a nebo nebude jisté, zda animovaná osoba je dítětem. Tato otázka bude v praxi představovat problém, který bude muset být řešen na základě konkrétních okolností a rysů animované postavy, tj. rysů vzhledových, kdy v potaz by mělo být bráno i vystupování a chování takové postavy, její oblečení apod. Uvedené rysy pak bude nutné vykládat ve vzájemné souvislosti, nikoliv jednotlivě. Další způsob určení věku představuje jeho odvození z charakteru animace, resp. ze souvislosti dějové linie. Konkrétně se může jednat o situaci, kdy přímo v animaci bude jasně řečeno, že se jedná o virtuální osobu mladší 18 let (např. Mach a Šebestová, kdy se ve znělce uvádí „My jsme žáci 3. B“ a současně lze z charakteru a vzhledu poznat, že se jedná o děti). Takové určení věku musí být v konkrétním případě nesporné. V případě, že by otázka věku animované postavy nebyla určena napevno, měla by být uplatněna zásada *in dubio pro reo*.<sup>51</sup>

## 6. TRESTNÍ POSTIH DĚTSKÉ PORNOGRAFIE A VIRTUÁLNÍ DĚTSKÉ PORNOGRAFIE

Právní úprava dětské pornografie je obsažena v současné době ve zvláštní části trestního zákoníku, konkrétně v ustanoveních § 191–193, zařazených do hlavy III. nesoucí název „Trestné činy proti lidské důstojnosti v sexuální oblasti“. Ustanovení § 191 upravuje trestný čin šíření pornografie, který se vztahuje jednak na pornografii tvrdou (odst. 1), a jednak na pornografii prostou (odst. 2). Úprava dětské pornografie je pak vyčleněna do samostatných ustanovení § 192 a 193 trestního zákoníku. Důvodem samostatné úpravy je fakt, že dětská pornografie je považována za nejškodlivější druh pornografie. Tuto skutečnost dokazuje i snaha jednotlivých států, daleko přesahující hranice evropského kontinentu, o regulaci této problematiky v celosvětovém měřítku. Výsledky těchto snah můžeme spatřovat v uzavření několika významných mezinárodních úmluv, které se daného problému dotýkají.<sup>52</sup> Všechny uvedené trestné činy mají společné, že po subjektivní stránce se vyžaduje úmyslné zavinění (§ 13 odst. 1 trestního zákoníku) a pachatelem může být kdokoliv. Rovněž u jednotlivých trestných činů jsou uvedeny okolnosti podmiňující použití vyšší trestní sazby (§ 191 odst. 3 a 4, § 192 odst. 3 a 4, § 193 odst. 2 a 3), mezi něž patří například spáchání trestného činu jako člen organizované skupiny nebo úmysl získat pro sebe nebo jiného prospěch (značný, velkého rozsahu).<sup>53</sup>

<sup>51</sup> CÍSAŘOVÁ, D., FENYK, J., GRÍVNA, T. et al. *Trestní právo procesní*. 5. vydání. Praha: ASPI, 2008, s. 83.

<sup>52</sup> Jedná se například o Úmluvu o právech dítěte, resp. Opční protokol k této úmluvě ze dne 25. 5. 2000, o Úmluvu o kybernetické kriminalitě ze dne 23. 11. 2001, o Úmluvu o ochraně dětí před sexuálním vykořisťováním a zneužíváním ze dne 25. 10. 2007 aj.

<sup>53</sup> Blíže viz ŠÁMAL, P. et al. *Trestní zákoník: komentář*. 2. díl. (§ 140–421). 1. vydání. Praha: C. H. Beck, 2010, s. 1702 n.

Ustanovení § 192 upravuje trestný čin výroby a jiného nakládání s dětskou pornografií. Objektem tohoto trestného činu je zájem společnosti na ochraně mravního vývoje dětí a ochraně před jejich sexuálním zneužíváním. Ustanovení § 192 upravuje v odst. 1 přechovávání dětské pornografie a v odst. 2 pak její šíření (nakládání) a kořistění z takového díla. Vzhledem k tomu, že šíření dětské pornografie je považováno za společensky škodlivější než její přechovávání a šíření ostatních druhů pornografických děl, je také přísněji trestáno, než je tomu u ostatních uvedených trestných činů, ve formě vyšších trestních sazeb. Dále jsou v tomto ustanovení uvedeny jednak způsoby šíření dětské pornografie (vyrobí, doveze, vyveze, proveze, nabídne, jinak jinému opatří apod.), a jednak podoby pornografického díla (fotografické, počítačové aj.).

Ustanovení § 193 upravuje trestný čin zneužití dítěte k výrobě pornografie, jehož objektem je zájem společnosti na ochraně dětí před sexuálním zneužíváním, zájem na řádném mravním a citovém vývoji dětí a svoboda rozhodování. Základem skutkové podstaty pak je, že pachatel přiměje, zjedná, najme, zláká, svede nebo zneužije dítě k výrobě pornografického díla nebo kořistí z účasti dítěte na takovém díle. Tento trestný čin lze spáchat jen za účasti skutečného dítěte, a tudíž je z povahy věci vyloučeno jeho použití z hlediska virtuální dětské pornografie. Určitou možnost odchylného výkladu představuje spojení „nebo zneužije dítě“, avšak s odkazem na předchozí výčet způsobu jednání (přiměje, najme, zláká) lze dovodit, že zákonodárce měl v úmyslu postihovat pouze aktivní jednání pachatele směřujícího k zneužití skutečných dětí, tzn. mělo by dojít ke skutečné vzájemné interakci mezi pachatelem a dítětem.

Základní otázkou zůstává, zda je možné v České republice trestně stíhat virtuální dětskou pornografii. Trestní zákoník nerozlišuje mezi dětskou pornografií skutečnou a virtuální. Dětskou pornografií ve virtuálním prostředí je možné stíhat podle ustanovení § 192 trestního zákoníku, tj. její výrobu a nakládání. K virtuální dětské pornografie se vztahuje okolnost podmiňující použití vyšší trestní sazby, která je spojována s nakládáním s dětskou pornografií prostřednictvím veřejně přístupné počítačové sítě. Ke stíhání virtuální dětské pornografie může dojít jen v případě, že bude připuštěno, že virtuální dítě lze subsumovat pod pojem dítě používaný v předmětném ustanovení trestního zákoníku. Lze konstatovat, že trestní právo tento přístup zastává, neboť na základě novely trestního zákoníku<sup>54</sup> byl rozšířen dosah skutkové podstaty ustanovení § 192 na osobu, jež se jeví být dítětem. Dle důvodové zprávy se jedná o transpoziční bod článku 1 písm. b) Rámcového rozhodnutí o boji proti pohlavnímu vykořisťování dětí a dětské pornografii, v němž se dětskou pornografií rozumí materiál, který znázorňuje skutečné dítě, ale i materiál obsahující realistické zobrazení neexistujícího dítěte. V rámci ustanovení § 192 je trestné i přechovávání pornografického díla, jež znázorňuje osobu, jež se jeví být dítětem. Vzhledem k argumentu, že virtuální dětská pornografie může u jedinců se sexuální deviací ve vztahu k dětem nahrazovat reálný stimul „k akci“, může být polemizováno, zda přechovávání takové dětské pornografie má být trestné.

V současné době je tedy možné postihovat virtuální dětskou pornografii z hlediska trestního práva. I podle dřívějšího výkladu se nabízela alternativa pro skutečnost, že virtuální dětská pornografie může být předmětem trestního stíhání. Lze tak dovodit

<sup>54</sup> Zákon č. 330/2011 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.



z použitého výrazu „jinak využívá dítě“, přičemž tento výraz se měl zřejmě vztahovat na pornografický materiál, u něhož z povahy věci chybí prvek zobrazení, avšak na druhé straně tento výraz vyžaduje, aby dítě bylo nějakým způsobem v díle přítomno, byť ne přímo zobrazeno.<sup>55</sup>

V souvislosti se zavedením trestní odpovědnosti právnických osob je vhodné na tomto místě zmínit vztah virtuální dětské pornografie a právnické osoby jako pachatele. Ze zcela všeobecného pohledu lze uvést, že oba uvedené pojmy mají společnou skutečnost, že jsou svou povahou dílem fikce. Právnické osoby nejsou skutečné, ale jejich chápání jako právních subjektů je již zažitě. Ustanovení § 7 zákona o trestní odpovědnosti právnických osob<sup>56</sup> obsahuje taxativní výčet trestných činů, pro něž je možné právnickou osobu v rámci trestního řízení případně postihnout. Mezi výčtem jsou i trestné činy výroby a jiného nakládání s dětskou pornografií a zneužití dítěte k výrobě pornografie (§ 192 a 193). Při posuzování, zda právnická osoba může být pachatelem těchto trestných činů bude platit to samé, co bylo řečeno výše, tzn. že pachatelem virtuální dětské pornografie může být i právnická osoba.

## 7. PŘÍPADOVÉ STUDIE

Z hlediska virtuální dětské pornografie se v právní praxi objevily zajímavé případy, v nichž na jednu stranu prosvítá nový koncept chápání virtuálního prostředí v právu, včetně jednání v něm uskutečňovaných, na druhé straně tyto případy naznačují, jak se virtuální svět stává součástí světa reálného, kdy se do něj v čím dál větší míře prolíná, a překračuje tak pomyslnou hranici mezi těmito světy.

Jedním z diskutovaných problémů ohledně virtuální dětské pornografie, je její dostupnost v Second Life.<sup>57</sup> Second Life je rozdělen do dvou virtuálních světů podle věku uživatele (avatara), a to na tzv. MainGrid, určený pro uživatele od dosažení věku 18 let a více, a na tzv. TeenGrid, určený pro věkovou skupinu v rozmezí od 13 do 18 let. Věk se zjišťuje při registraci, kdy uživatel je povinen vyplnit kolonku „age“, přičemž poté již v reálné situaci není nadále zkoumáno, zda je tato informace pravdivá či nikoliv. Není tedy vyloučeno, aby se v MainGrid nacházely osoby mladší 18 let a v TeenGrid osoby starší 18 let. Uživatelé si vytváří a průběžně mohou i měnit svou identitu neboli virtuální totožnost, tj. i osoba starší 18 let si může zvolit vzhled batolete, pokud bude mít zájem.

V roce 2007 německá stanice ARD odvysílala reportáž o dostupnosti dětské pornografie v Second Life,<sup>58</sup> a to jednak ve formě tradičního obrazového záznamu, a jednak přímo online jako hru, ve které byl avatar buď hlavním aktérem, nebo se hry mohl zúčastnit kterýkoli avatar jako divák. V některých případech bylo nutné zaplatit vstup-

<sup>55</sup> BARTOŇ, M. Virtuální pornografie, limity svobody umělecké tvorby a svobody projevu a trestní zákon. *Právní rozhledy*, 2008, roč. 16, č. 17, s. 623.

<sup>56</sup> Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim.

<sup>57</sup> Třírozměrný virtuální svět přístupný přes Internet, který měl na počátku roku 2008 více než 20 milionů uživatelů. Second Life je obrazem skutečného světa ve virtuálním prostředí. Informace dostupná z: [http://cs.wikipedia.org/wiki/Second\\_life](http://cs.wikipedia.org/wiki/Second_life).

<sup>58</sup> Reportáž je dostupná na: <http://www.youtube.com/watch?v=Wk8uNWF77gg>.

né.<sup>59</sup> Reportáž odhalila skupinu obchodující s dětskou pornografií, přičemž vyšetřování bylo současně zaměřeno na uživatele, kteří za virtuální sex zaplatili. Důvodem, proč se německé vyšetřovací orgány a státní zástupce touto kauzou zabývali, je skutečnost, že podle německého trestního práva je držení virtuální dětské pornografie trestné.<sup>60</sup> Společnost Linden Lab, která je tvůrcem Second Life, poskytla německým orgánům součinnost při zjišťování identity uživatelů, a to jednak těch, kteří za virtuální sex zaplatili, a jednak majitelů virtuálních pozemků, na kterých se virtuální dětská pornografie uskutečňovala.<sup>61</sup> Současně se zavázala upravit hru tak, aby bylo zabráněno virtuálním dětem (tj. uživatelům mladším 18 let, ale i uživatelům, jejichž virtuální totožnost představuje dítě) v provozování sexuálního jednání a zaměřila se na ověřování identity. Daný případ popisuje, že dětská pornografie ve virtuálním prostředí a zejména virtuální dětská pornografie není brána na lehkou váhu a naopak je v určitých státech chápána jako závažný negativní jev, který je nutné omezit a regulovat.

Jedním ze zajímavých soudních rozhodnutí zabývajících se otázkou virtuální dětské pornografie je rozhodnutí australského Nejvyššího soudu Nového jižního Skotska *McEwen v. SIMMONS & ANOR*,<sup>62</sup> které se zabývá otázkou, zda kreslené animované postavy (cartoon figures) mohou zobrazovat nebo vyjadřovat osobu (person). Pornografický materiál, který byl v předmětné věci posuzován, zobrazoval dětské členy rodiny Simpsonů při sexuálních aktivitách, přičemž měly jasně vyobrazeny lidské pohlavní orgány. *McEwen* byl soudem nižšího stupně v dané věci shledán vinným z trestného činu držení dětské pornografie (dle státního zákonodárství – State legislation) a trestným činem šíření a zpřístupnění dětské pornografie (dle zákonodárství Společenství – Commonwealth legislation). V odůvodnění uvedeného rozhodnutí se Nejvyšší soud nejprve vypořádal s otázkou posouzení věku dětských kreslených postav (*Bart* a *Lisa*), kdy konstatoval, že předpokládaný věk uvedených postav lze odvodit z televizního seriálu a není žádná pochybnost o tom, že se jedná o postavy ve věku mladším než 18 let,<sup>63</sup> a pravděpodobně také o postavy mladší 16 let.<sup>64</sup> Základní faktickou otázkou, kterou Nejvyšší soud posuzoval, bylo, zda fiktivní kreslená postava může být považována za osobu ve smyslu zákonem stanovených trestných činů.<sup>65</sup> Postavy nenapodobovaly žádnou skutečnou nebo fiktivní lidskou bytost. I když se vyznačovaly čtyřmi prsty, obličejem, tj. měly oči, nos a ústa, odlišovaly se od kterékoli možné lidské bytosti. Nejvyšší soud spatřoval základní rozdíl mezi zobrazením skutečné lidské bytosti a zobrazením fiktivní osoby. Pro objasnění rozdílu uvedl, že osoby zobrazené,

<sup>59</sup> V Second Life se obchoduje s virtuálními penězi, které je možné následně přeměnit ve skutečnou měnu a naopak.

<sup>60</sup> Informace dostupná z: <http://news.bbc.co.uk/2/hi/technology/6638331.stm>.

<sup>61</sup> V Second Life je možné vlastnit pozemky tohoto virtuálního světa, které si je možné koupit, a to buď za účelem bydlení, nebo obchodování s nimi.

<sup>62</sup> *McEWEN v. SIMMONS & ANOR* (2008), New South Wales Supreme Court, NSWSC 1292, dostupné z: <http://lawlink.nsw.gov.au/scjjudgments/2008nswsc.nsf/2008ns>.

<sup>63</sup> Commonwealth legislation pod pojmem dítě chápe osobu mladší 18 let [Section 9H(3) of Crimes Act 1900].

<sup>64</sup> State legislation pod pojmem dítě chápe osobu mladší (zdánlivě mladší) 16 let [Section 474.19 of Criminal Code Act 1995].

<sup>65</sup> Přestože se soud s touto otázkou vypořádal, konstatoval, že žádná jasná linie zahrnutí nebo vyloučení kreslených postav ve smyslu posouzení, zda se jedná o osoby z právního hlediska, nemůže být popsána.

například ve videohrách a komiksech, jsou osobami fiktivními, které jsou zapojeny do strašného násilí zahrnujícího mučení a smrt. Kdyby tyto osoby byly skutečné, takové zobrazení by nebylo nikdy povoleno, a jejich vytvoření by zakládalo trestný čin, tzn. že zobrazení jsou povolována jenom proto, že se jedná o fiktivní konstrukce. Skuteční lidé mohou být fiktivní a v tomto smyslu přijmout nebo hrát roli jiných než sebe samých či fiktivních postav, ale stále jsou to skuteční lidé. Z pohledu „Commonwealth legislation“ mohou být kresby a jiná zobrazení vyobrazením fiktivních nebo imaginárních postav.<sup>66</sup> Ačkoli hlavním cílem zákonodárství je boj proti přímému sexuálnímu vykořisťování a zneužívání dětí, zákonodárství rovněž počítá se zabráněním výroby takového materiálu (zahrnujícího i materiál kreslený) a jeho zpřístupněním na trh. V tomto ohledu Nejvyšší soud neshledal žádný důvod omezit význam osoby pouze na osobu skutečnou a do zobrazení nebo ztvárnění osob, na které definice odkazuje, zahrnuje jak kresby osob fiktivních (model, socha), tak i kreslených. Nejvyšší soud rovněž poukázal na fakt, že postava odchylovající se od rozpoznatelné podoby lidské existence, se může stát více méně osobou, a nebo také nemusí ztvárňovat osobu vůbec. Pouhé přiřazování lidských vlastností například králíkovi nebo kachně, nelze chápat tak, že se jedná o vyjádření osoby, dokonce i když králík nebo kachna mají povahové rysy, které jsou zřetelně lidské. Na druhé straně mnoho kreslených postav, ačkoli ne všechny, jsou kresleny, aby se podobaly skutečné lidské existenci. V případě, že se kreslená postava odchylová od ztvárnění člověka, je nutné posoudit, zda se stále ještě jedná o zobrazení osoby, a zda je způsobilé založit trestný čin. Nejvyšší soud připustil, že kreslená postava, která se bude odchylovat od ztvárnění člověka, může být zobrazením osoby ve smyslu zákonné definice Commonwealth legislation, avšak je nutné, aby zde byla přinejmenším nějaká podobnost lidské podoby. Pouhý symbol by ztvárněním osoby nebyl.

Pokud jde o posuzování významu slova „osoba“ z pohledu State legislation, vychází se z definice dětské pornografie, která používá pojem „zobrazuje nebo popisuje“ (depicts or describes). Při zavádění State legislation bylo konstatováno, že zobrazení nebo popis dítěte v sexuální kontextu je široká kategorie, která by měla pokrýt jednak situace, ve kterých je dítě zobrazeno v nemravné pozici nebo sledující jinou osobu zabývající se sexuální aktivitou. Požadavek, že materiál musí za všech okolností pohoršovat rozumné osoby, zajistí, že nevinné rodinné fotografie nahých dětí nebudou považovány za dětskou pornografii. Rovněž je pod tuto definici zařazován materiál, ve kterém je dítě obětí mučení, krutého nebo psychického zneužívání, i když se nejedná o čisté sexuální zneužívání, přesto však je takové jednání považováno za pohoršující. Nejvyšší soud se přiklonil k názoru, že slovo získává svůj význam až v daném kontextu, přičemž kontextem State legislation je ochrana dítěte před sexuálním vykořisťováním a zneužíváním. Na základě toho bylo konstatováno, že pojem osoba je v tomto kontextu způsobilá nejen k označení osoby skutečné, ale i fiktivní. V daném případě musí být kresba lidskou bytostí a jako taková musí být i rozpoznatelná, přičemž odklon od skutečnosti nemusí nutně znamenat, že nejde o zobrazení osoby v tomto smyslu.

<sup>66</sup> Fiktivní = vymyšlený, existující jen v příbězích; imaginární = smyšlený, existující pouze v myslí či vlastní představivosti. Oxford University Press – OALD dictionary. Dostupné z: <http://www.oup.com/elt/catalogue>.

Jelikož je však zobrazení osoby základním znakem trestného činu, musí být prokázáno nade vše pochybnost. I zde bylo zdůrazněno, že pouhé přiřazování lidských vlastností králíkovi, kachně nebo květině, by bylo nedostačující, pokud by i nadále subjektem zůstal králík, kachna nebo květina. Z tohoto výkladu lze dovodit, že fiktivní kreslené postavy, dokonce i ty, které se odlišují od rozpoznatelné lidské podoby, mohou být vyobrazením ve smyslu Crime Act.

Z výše uvedeného vyplývá závěr Nejvyššího soudu, že slovo „osoba“ (v rámci obou trestných činů podle obou zákonodárství) zahrnuje fiktivní nebo imaginární postavy a pouhý fakt, že postava je zobrazena odlišně od skutečného znázornění lidské bytosti, neznámá, že by taková postava nebyla osobou. Postavy v posuzovaném materiálu byly skutečně zobrazením osob ve smyslu zákonných definic. Za zmínku dále stojí, že v předmětném rozhodnutí Nejvyšší soud uvedl předchozí rozhodnutí ve věci Holland v. The Queen, v němž byl vyjádřen rozdíl mezi psaným dílem a dílem, jehož podstatou je zobrazení. V případě písemného díla nebude žádný rozdíl mezi tím, jestli spisovatel popisuje osobu, která je skutečná či nikoliv, neboť tento proces nevyžaduje přítomnost či dokonce existenci žádné skutečné osoby. V psaném díle není žádná osoba zobrazena, ale je popsána ve slovech. Psaný popis oku pozorovatele nikdy neposkytuje skutečně žijící osobu, může pouze předkládat její popis, přičemž osobou, která je v díle vyličeána, může být jak osoba skutečná, tak i osoba fiktivní nebo imaginární. Význam rozlišování mezi osobou skutečnou a fiktivní je pak základní otázkou v případě zobrazení. Dostupné důkazy ukazují, že jednoznačné sexuální materiály mohou být škodlivé, ať už zobrazují skutečné dítě či nikoli, a to zejména z důvodu, že s rostoucí stupněm technologického pokroku může být velice obtížné rozeznat skutečnou osobu od počítačové tvorby (výtvoru) nebo kompozice. Tímto případem měl být demonstrován vztah jiných států k virtuální dětské pornografii, zvláště pak skutečnost, že i v praxi dochází k rozšiřování pojmu osoby z právního hlediska.

Poslední virtuální případovou studii je případ z roku 2008, který byl rozhodován okresním soudem v Holandsku (Distrikt Court of 's-Hertogenbosch),<sup>67</sup> a jehož pachatel byl odsouzen k podmíněnému trestu odnětí svobody se zkušební dobou na 10 let.<sup>68</sup> V minutovém klipu nazvaném „Sexuální lekce pro mladé dívky“ (Sex lessons for young girls) bylo ukázáno, jak virtuální dívka provádí manuální sex na dospělé (rovněž virtuální) osobě. Animace byla zaměřena na mladé dívky a měla sloužit jako návod. Po dosažení orgasmu dospělého virtuálního muže se dívka usmívá do kamery, spustí se lavina nafukovacích balónků a muž tleská. Tato atmosféra animace měla demonstrovat, že se jedná o zábavnou činnost, kterou mohou mladé dívky provozovat. Otázka, která byla předmětem rozhodování, zněla, zda se jedná o realistické zobrazení neexistujícího dítěte, jak uvádí Úmluva o kybernetické kriminalitě<sup>69</sup> a holandský trestní zákoník,<sup>70</sup> jehož podstatnou změnu ve vnímání virtuální dětské pornografie přinesla novelizace

<sup>67</sup> BC3225, Rechtbank 's-Hertogenbosch, 01/845400-07. Dostupné z: [www.rechtspraak.nl/ljn.asp?ljn=BC3225](http://www.rechtspraak.nl/ljn.asp?ljn=BC3225).

<sup>68</sup> Nutno dodat, že pachatel byl stíhán současně za trestný čin ohrožování mravnosti a pohlavního zneužívání.  
<sup>69</sup> Holandsko Úmluvu o kybernetické kriminalitě podepsalo dne 23. 11. 2001, ratifikována byla dne 16. 11. 2006 a v účinnost vstoupila dne 1. 3. 2007.

<sup>70</sup> Čl. 240b (Artikel 240b Wetboek van Strafrecht).

v roce 2002. Z důvodové zprávy k trestnímu zákoníku vyplývá, že novela měla za cíl rozšířit čl. 240b o virtuální dětskou pornografii, což bylo učiněno včleněním pojmu „zdánlivý účastník“. Vláda v předmětném ustanovení záměrně ponechala slovo „zdánlivý“ (se zřetelem na věk), poněvadž důkaz týkající se věku virtuální osoby není možné podat, neboť ta žádný opravdový věk nemá. Odhad věku zobrazené osoby pak musí být proveden se zřetelem na všechny tělesné znaky (včetně pohlavních), které jediné mohou naznačovat věk této osoby. K posouzení „zdánlivé účasti“ ve virtuální dětské pornografii je dle důvodové zprávy postačující, že se zobrazená osoba podobá opravdovému dítěti. Naproti tomu se dají vyloučit zobrazení, z nichž je ihned patrné, že se jedná o upravovaná nerealistická zobrazení či o kreativní výtvar lidského ducha, a které tudíž nespádají pod čl. 240b holandského trestního zákoníku. V daném případě byl věk virtuální dívky odhadnut podle tělesných znaků, konkrétně podle nevyvinutých prs, ochlupení a nedorostlé postavy. Na základě toho soud konstatoval, že v animaci se jedná o virtuální dívku takřka pubertálního věku, která však nedosáhla věku 18 let. Z hlediska virtuální dětské pornografie je v Holandsku důvodem trestního postihu nejen ochrana vyobrazených mladistvých, ale i ochrana proti jednání, které může děti povzbudit nebo svést k tomu, aby se zúčastnili sexuálního chování nebo jednání, které je určeno pro subkulturu, která sexuální zneužívání dětí podporuje. V předmětné kauze soud usoudil, že dospělá osoba je sice schopná rozeznat zobrazené chování a osoby od pravých, avšak průměrné dítě tohoto schopno není.

## 8. ZÁVĚR

Není pochyb o tom, že virtuální svět nabývá pro celé lidstvo, jednotlivé společnosti i jedince na stále větším významu. Začíná být chápán jako součást každodenního reálného života, a proto jej nelze nadále opomíjet, a to ani v oblasti práva. Vědomy jsou si toho všechny státy a některé z nich již na tuto skutečnost reagují a snaží se jí regulovat. Pro virtuální dětskou pornografii je důležité její chápání společností a zda tato problematika patří do jejich morálních standardů, které považuje za důležité chránit. Na jedné straně se lze setkat s podivením, že takováto jednání, jsou vůbec brána vážně, neboť spousta osob je považuje za zábavná. Na druhé straně při zamyšlení se nad závažností a dopadem tohoto fenoménu je shledáván zájem na jeho regulování a postihu.

Český právní řád obsahuje úpravu, která účinně postihuje dětskou pornografii a odpovídá mezinárodním standardům a závazkům, ke kterým se Česká republika zavázala. Současný platný a účinný trestní zákoník dovoluje postihovat jednak dětskou pornografii ve virtuálním prostředí, jejímž předmětem je skutečné dítě, přičemž virtuální prostředí zde vystupuje pouze jako jeden ze způsobů jejího šíření, jednak i virtuální dětskou pornografii, pod níž je subsumován též postih pornografického materiálu obsahujícího realistické zobrazení neexistujícího dítěte. Jedná se však o zcela nový fenomén, který v sobě skýtá mnoho otázek a problémů, které již vyvstaly nebo v budoucnu vyvstanou, a proto zde bude důležitou roli hrát připravenost a operativnost orgánů činných v trestním řízení.

## VIRTUAL CHILD PORNOGRAPHY

### Summary

Child pornography is a serious negative social phenomenon and countries are trying to fight against it effectively. Virtual child pornography constitutes a subset of child pornography. It is a new phenomenon with many unresolved questions and problems. This article firstly defines basic concepts which child pornography generally involves. Furthermore, it contains the definition of virtual child pornography from the perspective of Czech law and international law (especially from the perspective of the European Union). This article including a solution to various issues as the subject of virtual child pornography, status of virtual persons from the legal point of view, determination of their age and criminal punishment in law. Finally three case studies, reflecting current position of selected countries on the matter, are stated. These studies show how virtual child pornography is dealt with in practice. Virtual world is becoming a daily part of life and increasingly penetrating into the real world, and for this reason there is also an expanding number of society's moral values requiring protection.

*Key words:* criminal law, child pornography, cyberspace

*Klíčová slova:* trestní právo, dětská pornografie, kyberprostor

# TRESTNÍ POSTIH CYBERSTALKINGU

MICHAL SÝKORA

## 1. ÚVOD

Tento příspěvek si klade za cíl pojednat o současných možnostech trestněprávního postihu relativně nového negativního jevu vyskytujícího se ve společnosti, k jehož výraznému nárůstu došlo teprve v několika posledních letech, a sice o pojmu cyberstalkingu. Jak je patrné i z četných mediálních tuzemských i světových případů, nejedná se v žádném případě o problém latentní ani zanedbatelný, ale o problém, který se ve společnosti poměrně rychle rozšiřuje, k čemuž přispívá zejména i enormní rozvoj informačních technologií a elektronických prostředků komunikace.<sup>1</sup> Společně s dalšími negativními jevy, jakými jsou například cybergrooming, cybersquatting či cyberšikana, se i cyberstalking, ač předobraz tohoto jednání lze najít v reálném světě, odehrává výlučně v cyberprostoru, což vyvolává dosud neřešené otázky nebezpečnosti či protiprávnosti takového jednání a případného postihu ze strany státních orgánů.

S účinností nového trestního zákoníku č. 40/2009 Sb. (dále jen TrZ) lze uvést jednání primárně podřadit pod skutkovou podstatu trestného činu nebezpečného pronásledování podle § 354 TrZ. To však neznamená, že již dříve neexistovaly prostředky, jak taková jednání trestně postihovat v rámci předchozího trestního kodexu č. 140/1961 Sb. (dále jen tr. zák.), ač lze souhlasit s názorem odborné literatury, že tyto možnosti byly značně roztržité a nedostatečně refletovaly vlastní podstatu a charakteristické rysy tohoto jevu, a proto byly v praxi i neefektivní.<sup>2</sup> Na druhou stranu ani dnes nelze veškerá jednání odpovídající cyberstalkingu považovat za trestné činy, jednak pro přílišné kazuistické vyznění skutkové podstaty trestného činu nebezpečného pronásledování na straně jedné, jednak s obligátním přihlédnutím k zásadě subsidiarity trestní represe na straně druhé, kdy zjednodušeně řečeno nelze každý obtěžující e-mail či zprávu v rámci chatu považovat za cyberstalking, jakkoliv se může jevit nebezpečně či vulgárně.

<sup>1</sup> Lze souhlasit s názorem, že tento fenomén nabyl na rozsahu zvláště s nástupem a hromadným rozšířením informačních technologií v populaci, byť samozřejmě k němu docházelo i dříve, viz ŠAMAL, P. KORBEL, F. *Trestněprávní postih nebezpečného pronásledování, tzv. stalkingu*. ASPI, 2009.

<sup>2</sup> ŠAMAL, P. et al. *Trestní zákoník: komentář*. 2. díl (§ 140–421). 2. vydání. Praha: C. H. Beck, 2012, s. 3291.

## 2. POJMY STALKING A CYBERSTALKING

Při zkoumání jevu nazvaného cyberstalking je logickým krokem primární definice chování obecně označovaného jako *stalking*, které lze označit jako úmyslné, zlovolné a opakované pronásledování jiné osoby, kdy se pachatel zaměří na nějakého člověka, po kterém slídí, obtěžuje a pronásleduje jej, vyhrožuje mu, často jej i fyzicky napadá a někdy u své oběti svým chováním zároveň vyvolává i pocity strachu.<sup>3</sup> Nepatrně odlišná definice pak hovoří o tom, že stalking je obsesivní fixací známého nebo neznámého pachatele na určitou osobu, kterou pak obtěžuje systematicky a úporně nevyžádanou a nechtěnou pozorností.<sup>4</sup> Jinými slovy je i druhou definicí vyjádřeno v podstatě totéž a jsou potvrzeny určité základní rysy tohoto jevu. De lege lata je z pohledu trestněprávního v současné době určující definicí znění samotné skutkové nebezpečného pronásledování podle § 354 TrZ (viz níže).

Jak již název napovídá, cyberstalking je pak pouze jednou z forem stalkingu, specifickým druhem elektronického pronásledování, kdy pachatel k výše popsanému jednání využívá prostředky internetových komunikací, tedy typicky zahrnuje svou oběť nevyžádanými maily, rozesílá negativní zprávy prostřednictvím chatu či blogu, zasílá nadměrné množství spamů či provádí záměrné útoky na data v počítači oběti.<sup>5</sup>

## 3. MOŽNOSTI TRESTNÍHO POSTIHU CYBERSTALKINGU

Ke dni 1. ledna 2010 vstoupila v účinnost nová kodifikace trestního práva hmotného, zákon č. 40/2009 Sb., trestní zákoník. Vedle výrazných koncepčních změn (opuštění materiálně-formálního či formálně-materiálního pojetí trestného činu a přechod k formálnímu pojetí s hmotněprávním korektivem) i menších odlišností (změna názvu z „trestní zákon“ na „trestní zákoník“) převzal od svého předchůdce do své nové systematiky zvláštní části z podstatné části katalog trestných činů, přičemž některé trestné činy již do nové úpravy nezahrnul (řízení motorového vozidla bez řidičského oprávnění podle ustanovení § 180d tr. zák.), některé naopak zakotvil zcela nově (zabití podle ustanovení § 141 TrZ).<sup>6</sup>

Jednou z nejvýznamnějších a nejvíce diskutovaných novinek v katalogu trestných činů bylo zakotvení nového trestného činu **nebezpečného pronásledování**, jak zákonodárce jednání odpovídající stalkingu v trestním zákoníku označil, v ustanovení § 354 TrZ.

Historický vývoj zakotvení tohoto trestného činu není v tomto případě bez zajímavosti. Původní vládní návrh trestního zákoníku tento trestný čin nezahrnoval. V rámci

<sup>3</sup> VÁLKOVÁ, H. Česká podoba stalkingu podle § 354 TrZ v širších než jen trestněprávních souvislostech. *Trestněprávní revue*, 2009, č. 9, s. 257.

<sup>4</sup> ŠÁMAL, P., KORBEL, F. *Trestněprávní postih nebezpečného pronásledování, tzv. stalkingu*. ASPI, 2009.

<sup>5</sup> VANTUCH, P. K postihu stalkingu (nebezpečného pronásledování) podle § 354 trestního zákoníku. *Trestní právo*, 2011, č. 2, s. 5.

<sup>6</sup> NOVOTNÝ, O., VOKOUN, R., ŠÁMAL, P. et al. *Trestní právo hmotné. Zvláštní část*. 6. vydání, Praha: Wolters Kluwer ČR, 2010, s. 17 n.



projednávání návrhu nového trestního zákoníku v Ústavně právním výboru Poslanecké sněmovny Parlamentu České republiky však nakonec došlo ke schválení jediné nové skutkové podstaty trestného činu oproti vládnímu návrhu, a to právě trestného činu nebezpečného pronásledování. Ministerstvo spravedlnosti nakonec akceptovalo požadavky ústavně právního výboru Sněmovny a návrh příslušné skutkové podstaty trestného činu nechalo samo zpracovat pro účely poslaneckého pozměňovacího návrhu.<sup>7</sup>

Nebezpečné pronásledování je zařazeno v hlavě X. mezi trestné činy proti pořádku ve věcech veřejných, do dílu pátého zahrnujícího trestné činy narušující soužití lidí. Spolu s odbornou literaturou lze polemizovat nad vhodností zařazení trestného činu nebezpečného pronásledování právě mezi tyto trestné činy, když tento by spadal typicky spíše mezi trestné činy proti právům na ochranu osobnosti, soukromí a listovního tajemství (hlava II., díl 2.),<sup>8</sup> mezi trestné činy proti svobodě (hlava II., díl 1.) či mezi trestné činy proti lidské důstojnosti v sexuální oblasti (hlava III., zvláště když oběti trpí podobnými příznaky jako oběti, které čelily těžkému násilí, jako je přepadení nebo znásilnění.<sup>9</sup>

Plné znění skutkové podstaty trestného činu **nebezpečného pronásledování podle ustanovení § 354 TrZ** tedy zní:

- (1) Kdo jiného dlouhodobě pronásleduje tím, že,
  - a) vyhrožuje ublížením na zdraví nebo jinou újmu 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.

Jak vyplývá i z pouhého textu zákona, bude jednání odpovídající cyberstalkingu podřaditelné zejména pod písmeno c) odstavce 1, odpovídající alternativě *vytrvalému*

<sup>7</sup> ŠÁMAL, P., KORBEL, F. *Trestněprávní postih nebezpečného pronásledování, tzv. stalkingu*. ASPI, 2009.

<sup>8</sup> ŠÁMAL, P. et al. *Trestní zákoník: komentář*. 2. díl (§ 140–421). 2. vydání. Praha: C. H. Beck, 2012, s. 3293. Argument, že do hlavy X., dílu pátého spadá i trestný čin nebezpečného vyhrožování podle § 353 TrZ podle mého dostatečně neodůvodňuje záměr zákonodárce, který lze navíc vzhledem k absenci důvodové zprávy k § 354 TrZ pouze odhadovat.

<sup>9</sup> KRATOCHVÍL, V. et al. *Kurz trestního práva. Trestní právo hmotné. Zvláštní část*. 1. vydání. Praha: C. H. Beck, 2009, s. 489.

*kontaktu prostřednictvím prostředků elektronických komunikací.* I v této formě jednání je však třeba rozlišovat mezi jednáním, které lze označit jako cyberstalking (tedy pronásledování v cyberprostoru) a ostatními prostředky elektronické komunikace (typicky prostřednictvím mobilního telefonu, a to voláním či pouhým prozváněním oběti nebo zasláním sms či mms zpráv).

I pro toto jednání samozřejmě platí obecné znaky nebezpečného pronásledování, jež jsou společné všem formám jednání. Společnými znaky pro všechny formy jednání taxativně vypočtené v písmenech a) až e) je *dlouhodobé pronásledování*, které je způsobilé *vzbudit důvodnou obavu o život nebo zdraví nebo o život a zdraví osob blízkých.*

Dlouhodobostí je opakující se pronásledování, odborná literatura vyjádřila názor, že opakováním je zde více než 10 pokusů o kontakt v období minimálně čtyř týdnů.<sup>10</sup> Znakem dlouhodobosti u trestného činu nebezpečného pronásledování se již zabýval i Nejvyšší soud České republiky v usnesení sp. zn. 8 Tdo 1082/2011 ze dne 8. září 2011, přičemž však ke kvantifikaci dlouhodobosti nepřistoupil: „*Dlouhodobostí se u tohoto trestného činu rozumí přinejmenším několik vynucených kontaktů pachatele s poškozeným nebo pokusů o ně, které zároveň musí být způsobilé vyvolat v poškozeném důvodnou obavu. Tyto požadavky ovšem nesplňují ojedinělé nebo náhodné projevy byť jinak nežádoucího chování. Zpravidla se tedy bude jednat o soustavně, vytrvale, tvrdošijně a systematicky prováděná jednání pachatele, která vybočují z běžných norem chování a mohou v některých případech i nebezpečně gradovat.*“ Z uvedené definice Nejvyššího soudu se zdá, že i počet dvou takových útoků nebude i při velké intenzitě k naplnění skutkové podstaty tohoto trestného činu postačovat, avšak takových útoků nebude pravděpodobně zapotřebí více než výše uvedených deset. Ojedinělé útoky by pak mohly naplnit znaky přestupku, typicky například podle ustanovení § 49 odst. 1 písm. c) zákona č. 200/1990 Sb., o přestupcích.

Otázkou je však vztah pojmů *dlouhodobosti pronásledování*, který je obecným znakem nebezpečného pronásledování, a *vytrvalého kontaktování*, které je znakem alternativy pronásledování pomocí prostředků elektronických komunikací (písemně či jinak). Do jaké míry je nutno oba pojmy považovat za synonyma, kdy by zákonodárce zřejmě opomenutím stanovil duplicitně stejnou podmínku trestnosti činu, neřeší z logiky věci ani důvodová zpráva k trestnímu zákoníku (nebezpečné pronásledování nebylo v původním návrhu zákona obsaženo, viz výše), a dosud ani judikatura či odborná literatura.<sup>11</sup> Oba pojmy lze přitom považovat za synonyma, resp. je zřejmé, že i u ostatních forem musí být takové jednání pachatele vytrvalé (srov. výše uvedené usnesení Nejvyššího soudu), neboť jinak by nemohlo splňovat znak dlouhodobosti a vyvolat obavu o život či zdraví. Proto se domnívám, že podmínka *vytrvalosti* v kontaktování oběti je v trestním zákoníku uvedena u této formy jednání nadbytečně a praxi by časem mohla způsobit aplikační problémy, ač, jak vyplývá z dosavadní rozhodovací činnosti

<sup>10</sup> VANTUCH, P. K postihu stalkingu (nebezpečného pronásledování) podle § 354 trestního zákoníku. *Trestní právo*, 2011, č. 2, s. 5.

<sup>11</sup> Viz např. NOVOTNÝ, O., VOKOUN, R., ŠÁMAL, P. et al. *Trestní právo hmotné. Zvláštní část*. 6. vydání. Praha: Wolters Kluwer ČR, a. s., 2010, s. 464–465, ŠÁMAL, P. et al. *Trestní zákoník: komentář*. 2. díl (§ 140–421). 2. vydání. Praha: C. H. Beck, 2012, s. 3290 n., či JELÍNEK, J. et al. *Trestní právo hmotné*. 1. vydání. Praha: Leges, 2009, s. 787–788.

Nejvyššího soud, se tak v soudní praxi doposud zřejmě nestalo, otázkou je však přístup jiných orgánů činných v trestním řízení, zejm. policejních orgánů při případné snaze o rozlišování pojmů *dlouhodobosti* a *vytrvalosti*.

I vzhledem k výše uvedenému lze konstatovat, že právě u této formy stalkingu se projevila skutečnost, že tento trestný čin byl do trestního zákoníku zakotven až na poslední chvíli a jaksi narychlo, neboť i z hlediska slovosledu zní věta „*kdo jiného dlouhodobě pronásleduje tím, že vytrvale jej prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontaktuje*“ spíše archaicky v kontrastu se zbylým textem trestního zákoníku. Stejně tak není zřejmě záměrem zákonodárce, že takové jednání pachatele musí k naplnění skutkové podstaty tohoto trestného činu vzbudit v jiném důvodnou obavu o jeho život **nebo** zdraví, avšak v případě osob jemu blízkých je zapotřebí vzbudit obavu o život **a** zdraví (tedy výkladem *ad absurdum* by i za splnění všech ostatních podmínek by důvodná obava pouze o zdraví blízkých osob nezakládala trestní odpovědnost pachatele podle § 354 TrZ, je však nutno přihlídnout ke skutečnosti, že výkladem *ad minore ad maius* je uvedená konstrukce vyloučena).

Pojem *důvodné* obavy není v trestním zákoníku nový. Byl již jedním ze znaků skutkové podstaty trestného činu násilí proti skupině obyvatel a proti jednotlivci podle ustanovení § 197a tr. zák. a i nyní je součástí skutkové podstaty trestného činu nebezpečného pronásledování podle ustanovení § 353 TrZ, neboť tato skutková podstata se z původního § 197a tr. zák. (dnes § 352 TrZ) vymanila jako samostatný trestný čin. Důvodnou obavu definuje Nejvyšší soud ve shora citovaném usnesení tak, že „*vyjadřuje stav poškozeného, který je objektivně způsobilý vyvolat u něj vyšší stupeň obav, úzkosti nebo jiného tísnivého pocitu ze zla, jímž pachatel působí na poškozeného, přičemž však není nutné, aby byl takový pocit v poškozeném skutečně vyvolán*“. Jinými slovy oběť nemusí nutně mít obavu o svůj život či zdraví, nemusí se o jednání pachatele dokonce ani dozvědět, a důvodná obava tak ve výsledku u oběti ani nemusí vzniknout, ovšem její vznik musí být reálný.<sup>12</sup> Pokud by poškozený bral pronásledování jako pouhé příkoří, které není způsobilé vzbudit obavu o život či zdraví, nepůjde o trestný čin nebezpečného pronásledování.<sup>13</sup>

Jak již bylo uvedeno výše, do kategorie chování spočívající v dlouhodobém pronásledování prostředky elektronických komunikací patří například opakované zasilání nevyžádaných e-mailových zpráv (často s vulgárním či agresivním obsahem), zahlcování elektronické pošty nevyžádanými zprávami (tzv. spamem), záměrná distribuce počítačových virů, opakované vzkazy, nevyžádaná volání jak na mobilní telefon, tak na pevnou telefonní linku apod.<sup>14</sup> Ne všechna tato jednání lze samozřejmě podřadit pod pojem cyberstalkingu, který je užším pojmem než pronásledování prostřednictvím prostředků elektronických komunikací, a je tak specifickým druhem tohoto elektronického pronásledování. Z výše uvedených příkladů konkrétního jednání pachatele zahrnuje cyberstalking podle odborné literatury takové aktivity, jakými jsou nevyžádané e-mailové zprávy, rozesílání negativních zpráv prostřednictvím chatu, blogu a jiné způsoby

<sup>12</sup> ŠÁMAL, P. et al. *Trestní zákoník: komentář*. 2. díl (§ 140–421). 2. vydání. Praha: C. H. Beck, 2012. Viz i Vážný č. 3532 tr.

<sup>13</sup> JELÍNEK, J. et al. *Trestní právo hmotné*. 1. vydání. Praha: Leges, 2009, s. 788.

<sup>14</sup> Viz usnesení Nejvyššího soudu České republiky sp. zn. 8 Tdo 1082/2011 ze dne 8. září 2011.

virtuálního šíření pomluv a informací poškozujících pověst oběti (dobré jméno, rodinné poměry a profesní bezúhonnost), zaslání spamů a záměrné útoky na data v počítači oběti (zavirování, zablokování, nepřipustné získávání jejich osobních dat).<sup>15</sup> Taková jednání však musí mít určitou intenzitu (srov. výše), a tak ani pokud k nim dochází opakovaně, nelze je automaticky považovat za cyberstalking v trestněprávním smyslu (což však nevylučuje označit takové jednání jako cyberstalking v jiném odvětví lidské činnosti, například ve smyslu psychiatrickém při diagnóze pacienta s určitou chorobou, mezi jejíž průvodní znaky patří pronásledování jiných, stalking je pojmem širším, než jak ho vymezuje trestní zákoník).

Některá výše uvedená jednání mohou odpovídat spíše pojmu cyberšikany, jejíž trestněprávní zakotvení v českém právním řádu doposud chybí, a jež nelze považovat za pouhé synonymum k pojmu cyberstalking (viz níže). Jen obtížně si lze totiž představit, že pouhé zaslání většího množství zpráv či zahlcení e-mailové schránky splní předpoklady dlouhodobého pronásledování, které je způsobilé vzbudit důvodnou obavu o život či zdraví. Možnost postihu pachatele pro trestný čin nebezpečného pronásledování bude vždy záviset především na konkrétním obsahu nevyžádané e-mailové zprávy, která může být zaslána buď jako samostatná opakovaně, tak ve větším množství (tedy nikoliv opakovaně, avšak v řádech desítek odeslaných zpráv se stejným obsahem v jednom okamžiku), které mohou zcela zahltit elektronickou poštu a tím znemožnit alespoň po nějakou dobu její funkčnost. Právě druhá možnost odpovídá jednání typickému pro cyberšikany, neboť pouhé formální zahlcení emailové schránky samo zřejmě o sobě není způsobilé vyvolat v někom obavu o jeho život či zdraví. Rovněž tak rozesílání negativních zpráv prostřednictvím chatu, blogu či jiné „virtuální pomlouvání“ a šíření informací poškozujících pověst oběti spadá typicky pod pojem cyberšikany a lze si představit trestní postih pachatele pro trestný čin pomluvy podle ustanovení § 184 TrZ (například pro kvalifikovanou skutkovou podstatu podle odstavce 2, tedy spáchá-li pachatel tento čin tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobným účinným způsobem) či křivého obvinění podle ustanovení § 345 TrZ (například pro kvalifikovanou skutkovou podstatu podle odstavce 2 písmena b), který obsahuje stejné okolnosti spáchání činu jako kvalifikovaná skutková podstata trestného činu pomluvy) nebo domáhání se ochrany podle ustanovení § 11 a násl. zákona č. 40/1964 Sb., občanský zákoník, které slouží na ochranu osobnosti, tedy zejména života, zdraví, občanské cti, lidské důstojnosti, jakož i soukromí, jména a projevu osobní povahy fyzické osoby.

Za typické projevy cyberstalkingu lze označit vzhledem k výše uvedenému označit opakované vytrvalé zaslání e-mailových zpráv, jejichž obsah může v oběti vyvolat strach o jeho zdraví či život, například přímou výhrůžkou smrti či ublížení na zdraví, ale i výhrůžkami nepřímými („*nebudeš-li mě milovat, uvidíš, jaké to pro tebe bude mít následky...*“). Důvodnou obavu může vzbudit i hromadné zaslání prázdných e-mailových zpráv od pachatele, který již dříve svou oběť kontaktovat jinými způsoby a dal zřetelně najevo svou přílišnou náklonnost k oběti či naopak nevraživost až nenávisť. Dalšími projevy je kontakt prostřednictvím chatu, kdy pachatel, skrývající svou identi-

<sup>15</sup> ŠÁMAL, P. et al. *Trestní zákoník: komentář*. 2. díl (§140–421). 2. vydání. Praha: C. H. Beck, 2012, s. 3297.

tu a z tohoto důvodu vystupující pod různými jmény, kontaktuje svou oběť vulgárním či vyhrožujícím obsahem svých zpráv a je schopen v ní vyvolat i pocit „přesily“, kdy tato netuší, že autorem takových zpráv je pouze jediná osoba. V praxi jsou jednání odpovídající cyberstalkingu často doprovázeny jevy ostatních jednání nebezpečného pronásledování, kdy pachatel, který svou oběť pronásleduje fyzicky (sleduje ji při cestě do práce, snaží se ji pozorovat z ulice přes ona jejího domu apod.), ji zároveň kontaktuje i prostřednictvím e-mailu či chatu. Jak již bylo řečeno výše, tato forma komunikace mu umožňuje skrýt svou pravou identitu, a oběť tak často ani nemůže tušit, že je pronásledována jedinou osobou (tuto skutečnost může odhalit až při delším pronásledování na základě určitých indicií). Naopak pachatel se zde dostává do značné výhody, ať už vědomé nebo nevědomé, neboť se nemusí omezovat pouze na fyzické pronásledování, jež je pro něj především časově i jinak náročné, ale při cyberstalkingu se může svého jednání dopouštět takřka kdykoliv a bez fyzické námahy. Rovněž snižuje riziko nebezpečí, že oběť pozná, o koho se jedná, resp. že se jedná pouze o jednu osobu. V tomto ohledu lze cyberstalking označit za velmi nebezpečný, neboť zvyšuje možnosti a rafinovanost pronásledující osoby.

Skutečnost, že jednání odpovídající cyberstalkingu spadá primárně pod jednání popsané v odstavci 1 písm. c) ovšem neznamená, že tímto svým jednáním pachatel zároveň nemůže naplnit i jinou alternativu uvedenou v tomto ustanovení. Lze si například představit, že pachatel zasílá své oběti opakovaně větší množství e-mailových zpráv, v nichž jí nebo osobám jí blízkých<sup>16</sup> vyhrožuje smrtí. Zároveň ve svých výhrůžných zprávách vyzývá svou oběť, aby za žádných okolností „*nevycházel ze svého bytu po setmění, jinak vše nabere rychlý spád*“. Oběť ze strachu skutečně přestane po setmění vycházet z bytu, čímž se například může narušit i její pracovní činnost (může se jednat o umělkyni absentující v divadelních představeních či o hlídače noční služby, který tímto přichází o své příjmy). V takovém případě by bylo možno kvalifikovat jednání pachatele podle ustanovení podle písmena a) (vyhrožuje ublížením na zdraví), písmena c) (využívá k tomu vytrvalého kontaktu prostřednictvím prostředků elektronické komunikace) i podle písmena d) (tím, že se oběť bojí vycházet po setmění ze svého bytu, je omezoována v obvyklém způsobu života). Takové souběhy ostatně nebudou v praxi ničím výjimečným. Omezení v obvyklém způsobu života spočívá v takovém omezení dosavadního života poškozeného, ke kterému dojde proti jeho vůli nežádoucími zásahy pachatele do sféry osobního, rodinného, ale i profesního života poškozeného, může jít o omezení v rovině zájmové, kulturní, sportovní apod.<sup>17</sup> Oběť by tak ani sama profesně nemusela vykonávat uměleckou činnost, stačila by ta skutečnost, že by ze strachu z ublížení na zdraví přestala po dobu několika měsíců navštěvovat divadelní představení, ač dříve byla náruživým divadelním fanouškem.

Vzhledem k tomu, že k zakotvení trestného činu nebezpečného pronásledování došlo až relativně na poslední chvíli (viz výše), neřešila se detailněji otázka, zda některé formy jednání, uvedených v odstavci 1, které nyní spadají pod základní skutkovou podstatu, nejsou natolik typově závažné, že by zasluhovaly být kvalifikovanou skutkovou

<sup>16</sup> K pojmu osoby blízké viz ustanovení § 125 TrZ.

<sup>17</sup> Viz usnesení Nejvyššího soudu České republiky sp. zn. 8 Tdo 1082/2011 ze dne 8. září 2011.

podstatou se zvýšenými hranicemi trestů. Pachatelovo jednání je podle současného znění posuzována jako kvalifikovaná skutková podstata trestného činu nebezpečného pronásledování, pokud je spácháno vůči dítěti či těhotné ženě, se zbrání nebo nejméně se dvěma osobami.

Úvaha posuzovat některé formy nebezpečného pronásledování přísněji by se podle mého názoru týkala právě cyberstalkingu, který lze považovat za důmyslnější, nebezpečnější a pro oběť ponižující způsob pachatelova působení na pronásledovaného, tedy za formu výhodnější pro pachatele se závažnějšími dopady na oběť, a to především z těchto důvodů:

Oproti fyzickému pronásledování má pachatel při kontaktu oběti pomocí e-mailové komunikace, v diskusních či chatovacích fórech nebo formou sms zprávy **značnou výhodu anonymity**, neboť si může vytvořit zcela **novou identitu**, kterou není oběť zpravidla schopna pomocí technických prostředků rozklíčovat (takové možnosti mají orgány činné v trestním řízení), což u ní zvyšuje pocit strachu z neznámého pachatele. Ten si navíc může vytvořit dokonce i **více identit**, například v rámci jednoho diskusního fóra, kdy pachatel může vytvořit zdání útoku více osob, ač se za jednotlivými přezdívkami skrývá pouze on sám, a tím své působení na oběť násobit. Ta netuší, že je pod vlivem nikoliv několika, ale pouze jednoho pachatele, což jí podstatně ztěžuje možnosti tohoto pachatele konkretizovat, na rozdíl od situace, kdy by bylo zřejmé, že pachatel je pouze jeden, neboť oběť by jej pravidelně vídala například na ulici či slyšela stejný hlas v telefonu. Taková situace zvyšuje pocit značné nejistoty a strachu a doléhá na oběť velmi tísnivě, neboť nevědomost o tom, kdo a z jakých důvodů ji pronásleduje, je pro oběť horší a je pro ni jistě i složitější se chránit, než když jde o jí známého útočníka.

Pachatel má rovněž lepší možnosti svůj útok na oběť **rafinovaně stupňovat**, což i posiluje jeho sebevědomí a utvrzuje ho nejen ve správnosti rozhodnutí útok podniknout, ale umožňuje mu jej i rozvíjet a zesilovat. Právě tato promyšlenost útoků činí jeho jednání nebezpečnější s dalekosáhlejšími důsledky.

Pachatel si rovněž v případě cyberstalkingu troufne i na **mnohem slabší oběť**, ať už fyzicky či mentálně, jíž by jinak bez použití elektronických či technických prostředků neměl odvahu kontaktovat. V cyberprostoru může udat libovolný věk, pohlaví, váhu, povolání, známosti a schopnosti. Uvedené je nutno chápat i z opačného hlediska, nejen, že pachatel si může vybrat slabší oběť (ať tato osoba skutečně zejména psychicky slabší či zranitelnější je nebo se tak pachatel pouze domnívá), ale zároveň s tím tato oběť může pachatele vnímat jako toho silnějšího v rámci jejich kontaktu, ačkoliv ve skutečnosti tak tomu vůbec být nemusí. Využitím forem cyberstalkingu se tak stírají rozdíly patrné v reálném životě a snadnou obětí se může stát i sebevědomý jedinec, naopak útočníkem i mentálně slabší osoba, která přesto vyvolá ve své oběti pocity strachu.

Tento kontakt rovněž může probíhat kdykoliv a kdekoliv, v jakémkoliv okamžiku, který pachatele napadne, samozřejmě za předpokladu, že pachatel i oběť jsou v tomto okamžiku dosažitelní elektronickým prostředky, v poměru k **relativní fyzické náročnosti „běžného“ útoku mimo cyberprostor**. Lze konstatovat, že se zde zcela stírá problém dosažitelnosti oběti. Útočníkem tak může být osoba vzdálená i stovky kilometrů, útok může být bez nadsázky i „mezikontinentální“. Jedinou podmínkou dosažitelnosti

samozřejmě zůstává výskyt osoby v kyberprostoru, což ale v současné době představuje marginální problém vzhledem ke skutečnosti, že v cyberprostoru se běžný člověk pohybuje v podstatě neustále (např. i prostřednictvím svého mobilního telefonu).

Zajímavou úvahu v tomto případě skýtá smysl kvalifikované skutkové podstaty podle ustanovení § 354 odst. 2 písm. c) TrZ, tedy spáchání trestného činu nebezpečného pronásledování nejméně se dvěma osobami. Zákonodárce v rámci trestního zákoníku u vybraných trestných činů považuje spáchání více osobami (nejméně dvěma) za natolik společensky závažné, že je těmto jednáním vymezena kvalifikovaná skutková podstata těchto činů (jedná se například o trestný čin mučení a jiné nelidské a kruté zacházení podle ustanovení § 149 odst. 2 písm. d) TrZ, trestný čin vydírání podle ustanovení § 175 odst. 2 písm. b) TrZ, trestný čin porušování domovní svobody podle ustanovení § 178 odst. 3 TrZ, trestný čin sexuálního nátlaku podle ustanovení § 186 odst. 3 písm. b) TrZ, trestný čin násilného překročení státní hranice podle ustanovení § 339 odst. 2 písm. b) TrZ a další). Lze konstatovat, že je tomu tak proto, že u těchto vybraných trestných činů je natolik zvýšená jejich typová škodlivost vůči poškozené osobě, že je tato konstrukce zákonodárce logická a dobře pochopitelná.<sup>18</sup> Na poškozenou osobu je takovým jednáním více osob vyvíjen větší psychický nátlak a může u této osoby zvyšovat i tísnivý pocit ze zla. Právě tento závažnější a krutější dopad na poškozeného je i jedním z důvodů uvedené konstrukce. Vzhledem k výše řečenému, že pachatel využívající prostředky elektronických komunikací může v poškozeném vyvolat pocit, že jednání se dopouští více osob (přičemž poškozená osoba by mohla mít za to, že jedna osoba ji pronásleduje na ulici, další ji kontaktuje e-mailovými zprávami a třetí telefonickými hovory, nad to by poškozená osoba nemohla vědět, zda těchto „více“ osob jedná po vzájemné dohodě či zda je pronásledována nezávisle na sobě více osobami), je na škodu, že na takovéto jednání nelze vztáhnout ustanovení § 354 odst. 2 písm. c) TrZ, ač dosahuje stejného efektu, jako kdyby se na jednání skutečně podílelo více pachatelů (či pachatel a účastníci).<sup>19</sup> Dosah tohoto ustanovení samozřejmě nelze vztáhnout na jednu osobu, která vystupuje pod identitou více osob, což je však důvodem hovořícím pro to, aby nebezpečné pronásledování ve formě cyberstalkingu či obecně ve formě kontaktu prostřednictvím prostředků elektronických komunikací bylo kvalifikovanou skutkovou podstatou, neboť při možnosti uložit trest odnětí svobody maximálně pouze na jeden rok je pro soud obtížné zohlednit při ukládání trestu rozdílnou nebezpečnost jednotlivých útoků.

Co se týče možnosti naplnění skutkových podstat jiných trestných buď v jednočinném souběhu s trestným činem nebezpečného pronásledování, v úvahu přicházejí trestné činy omezování osobní svobody podle § 171 TrZ, porušování domovní svobody podle § 178, pomluvy podle § 184 TrZ, poškození cizí věci podle § 228, výtržnictví § 358 a teorie dovozuje i možnost naplnění skutkové podstaty trestného činu týrání zvířat podle § 302 TrZ.<sup>20</sup> Tyto široké možnosti jednočinného souběhu jsou dány tím, že i jednání pachatele, který nebezpečně pronásleduje jinou osobu, je poměrně různorodé a lze si v praxi představit mnoho různých situací, které jsou schopni pachatelé vytvořit. Co se týče trestných činů proti životu a zdraví (vražda podle § 140 TrZ, těžké ublíže-

<sup>18</sup> ŠÁMAL, P. et al. *Trestní zákoník: komentář*. 2. díl (§140–421). 2. vydání. Praha: C. H. Beck, 2012, s. 3013.

<sup>19</sup> Tamtéž.

<sup>20</sup> Tamtéž, s. 3300.

ní na zdraví podle § 145 TrZ, ublížení na zdraví podle § 146 TrZ), či trestných činů zbavení osobní svobody podle § 170 TrZ, zavlčení podle § 172 TrZ, loupeže podle § 173 TrZ, vydírání podle § 175 TrZ, útisku podle § 177 TrZ, neoprávněného nakládání s osobními údaji podle § 180 TrZ, znásilnění podle § 185 TrZ a obecného ohrožení podle § 272 TrZ, objevil se v teorii názor, že při zachování téhož skutku pachatelem zpravidla dojde k faktické konzumpci nebezpečného pronásledování, nebude-li třeba zvláštní povahu nebo závažnost vyjádřit souběhem těchto trestných činů.<sup>21</sup> Takovou variantu lze připustit u trestného činu vraždy či těžkého ublížení na zdraví, ale např. při souběhu nebezpečného pronásledování s trestným činem útisku by taková kvalifikace byla spíše méně pravděpodobná. Lze však konstatovat, že zkoumání konkrétních možností jednočinných souběhů s trestným činem nebezpečného pronásledování je úkolem zejména budoucí judikatury Nejvyššího soudu.

#### 4. ZÁVĚR

Lze obecně konstatovat, že zakotvení stalkingu, resp. cyberstalkingu, do českého právního řádu v rámci trestného činu nebezpečného pronásledování je ze strany odborné veřejnosti vnímáno jako pozitivní krok. Na základě ustanovení § 354 odst. 1 písm. c) TrZ tak lze stíhat jednání, k jehož výraznému nárůstu sice došlo teprve v několika posledních letech, ale u něhož je na základě jeho závažnosti i možnosti, jež pachatel ke svým útokům získává, vhodné upravit jeho trestněprávní postih.

*Zvláštní poděkování patří Mgr. et Mgr. Kateřině Lukášové.*

#### CYBERSTALKING

#### Summary

This contribution analysis the possibilities of criminal prosecution of a new phenomenon called Cyberstalking in the Czech legislation. These possibilities have expanded especially after establishing the crime of stalking in the new Penal code no. 40/2009 Coll. For this reason the contribution focuses on this new legislation and is based primarily on the current Czech literature and existing case law of The Supreme Court of the Czech republic.

*Key words:* cyberstalking, Penal code, Supreme Court of the Czech republic

*Klíčová slova:* kyberstalking, trestní zákoník, Nejvyšší soud ČR

---

<sup>21</sup> Tamtéž, s. 3301.



## VIRTUÁLNÍ VLASTNICTVÍ – VLASTNICTVÍ ZA ČASŮ *IUS DOWNLOADENDI*

ROBERT KABÁT\*

„Lidé nejsou zneklidňováni věcmi, nýbrž svými vlastními názory o věcech.“

Epiktétos<sup>1</sup>

### 1. ÚVOD

Když Čchiou Čcheng-wej<sup>2</sup> přišel na úřadovnu čínské policie v Šanghaji oznámit, že mu jeho někdejší přítel Ču Cchao-jüan<sup>3</sup> zpronevěřil něco moc vzácného, mohlo to jen stěží pro něj dopadnout nespravedlivěji. Onou cenností byla totiž tzv. dračí šavle, mocná virtuální zbraň z mnohohráčské internetové hry na hrdiny *Legend of Mir 3*. Policisté se odmítli Čchiouovým oznámením zabývat, s náležitým výsměchem a prostým vysvětlením: virtuální zbraň není skutečným majetkem. Navzdory tomu, že Ču tuto zbraň prodal na eBay jinému hráči za 7200 čínských jüanů (cca 22 000 Kč)<sup>4</sup> a odmítl Čchiouovi vydat dokonce i peníze, které za dračí šavli utřžil. Čchiou si cestu ke „spravedlnosti“ nakonec našel: jedné noci v říjnu 2004 vnikl do Čuova bytu a skutečnou zbraní (!) jej ubodal k smrti.<sup>5</sup>

\* Autor je doktorandem na katedře trestního práva Právnické fakulty Univerzity Karlovy v Praze a externím spolupracovníkem Centra pro právní komparatistiku.

<sup>1</sup> EPIKTÉTOS. *Rukojet' rozpravy*. Přeložil Rudolf Kuthan. 2. vydání. Praha: Svoboda, 1972, kapitola V, s. 29.

<sup>2</sup> V příspěvku je užitá česká transkripce čínštiny, která lépe vystihuje výslovnost. V zahraničí i v české literatuře lze ovšem častěji najít podobu jeho jména dle oficiálního čínského transkripčního systému pchin-jin: Qiu Chengwei.

<sup>3</sup> Dle pchin-jin: Zhu Caoyuan.

<sup>4</sup> Přepoččet vychází z kurzu koruny k jüanu v roce 2004, kdy se případ stal (viz <http://www.kurzy.cz>, [cit. 2012-09-30]). Pro srovnání: průměrný měsíční výdělek v čínských městech se v roce 2004 pohyboval okolo 5100 jüanů (výpočet dle údajů dostupných na <http://www.worldsalaries.org/china.shtml> a <http://x-rates.com/d/CNY/USD/hist2004.html>; [cit. 2012-09-30]).

<sup>5</sup> Viz BBC. Číňan zabil muže kvůli virtuální krádeži v onlinové hře. *BBC Czech* [online]. 30. březen 2005. Dostupné z: [http://www.bbc.co.uk/czech/worldnews/story/2005/03/050330\\_china\\_cyber\\_murder\\_1725.shtml](http://www.bbc.co.uk/czech/worldnews/story/2005/03/050330_china_cyber_murder_1725.shtml); BBC. 'Game theft' led to fatal attack. *BBC News* [online]. 31. březen 2005. Dostupné z: <http://news.bbc.co.uk/2/hi/technology/4397159.stm>; TAIPEI TIMES. Games player killed friend over online 'dragon saber'. *Taipei Times* [online]. 1. duben 2005. Dostupné z: <http://www.taipetimes.com/News/world/archives/2005/04/01/2003248619>; FINLAYSON, A. – REUTERS. Online gamer killed for selling virtual weapon. *The Sydney Morning Herald* [online]. 30. květen 2005. Dostupné z: <http://www.smh.com.au/news/World/Online-gamer-killed-for-selling-virtual-weapon/2005/03/30/1111862440188.html>; LI, Cao. Death sentence for online gamer. *China Daily* [online]. 8. červen 2005. Dostupné z: [http://www.chinadaily.com.cn/english/doc/2005-06/08/content\\_449600.htm](http://www.chinadaily.com.cn/english/doc/2005-06/08/content_449600.htm). Všechny stránky jsou citovány podle stavu k 30. září 2012.

Příběh Čchioua Čcheng-weje, tolik oblíbený mezi zájemci o kyberkriminalitu, vyvolává mnoho otázek. Jednou z těch, která stojí u základu celého případu, je, *zda mohou být virtuální předměty počítány mezi majetek v právním slova smyslu*. Na tuto otázku hledá zahraniční a – typicky v omezené míře – i domácí právní věda odpověď neustále. Ukazuje se, že virtuální předměty zkouší pevnost po léta precizovaných hranic mezi jednotlivými právními kategoriemi: smlouvou, věcí, nehmotnými statky, autorskými díly.

Zatřídění má však dalekosáhlé *právní důsledky*. Z pohledu soukromého práva nejde jen o postavení hráčů a provozovatelů daného virtuálního světa, ale rovněž i o použitelnost jednotlivých civilních žalob či jiných systémů eventuální nápravy. Na občansko-právní závěry dále navazují normy ostatních právních oblastí. V mezinárodním právu soukromém má právní kvalifikace virtuálního majetku rozhodující význam při určení rozhodného právního řádu. V trestním právu je zase důležitá pro vymezení dosahu jeho skutkových podstat; ačkoli – jak dokazují zkušenosti s rozdílným pojetím věci v právním smyslu<sup>6</sup> – nemusí být trestněprávní terminologie a skutkové podstaty přesně navázány na civilistické pojmy. Konečně nelze opominout ani vliv na otázku eventuálního zdanění virtuálního majetku a jeho převodů.

Je přitom nepochybné, že ani z *praktického hlediska* nejde o okrajový problém. Počet uživatelů jednotlivých virtuálních světů celosvětově dosahuje až k deseti milionům.<sup>7</sup> Odhaduje se, že v roce 2009 jen v Asii dosáhla hodnota směřených virtuálních předmětů 400 milionů amerických dolarů (cca 7,6 miliardy Kč).<sup>8</sup>

Cílem tohoto příspěvku není prozkoumat všechny nastíněné aspekty virtuálních světů. Zaměřuje se toliko na pojem „virtuálního majetku“ a zařazení virtuálních předmětů v systému majetkového práva, což má následně vliv i v dalších oblastech práva. Oproti dosavadním zpracováním této problematiky je hlavní důraz kladen na české právo.

## 2. OBECNĚ K VIRTUÁLNÍMU MAJETKU

### 2.1 CHARAKTERISTIKA VIRTUÁLNÍCH SVĚTŮ

Koncept virtuálního majetku je skutečně neoddelitelně spjat s virtuálními světy, které determinují jeho povahu. Virtuální světy jsou uměle vytvořená prostře-

<sup>6</sup> Trestní právo se odklonilo od pojetí věci jako výlučně hmotného předmětu ještě za účinnosti trestního zákona z roku 1961, když mezi věci zařadilo i peněžní prostředky na účtu. Srov. rozhodnutí Rt 14/2006, vydané ještě před novelou č. 253/2006 Sb., a Rt 4/2008, reflektující již stav po novele. Ani jiná majetková hodnota nemá stejný význam v trestním a soukromém právu; pojem obsažený v § 89 odst. 2 trestního zákoníku pokrývá dvě civilistické kategorie předmětů právních vztahů dle § 118 odst. 2 občanského zákoníku z roku 1964: (1) práva i (2) jiné majetkové hodnoty.

<sup>7</sup> Kupř. nejoblíbenější mnohohráčská hra na hrdiny *World of Warcraft*, zasazená do fantazijního prostředí pseudostředověku, eviduje k prosinci 2011 10,2 milionů předplatitelů, z toho (dle čísel k roku 2008) přibližně 2 miliony v Evropě, 2,5 milionu v Severní Americe a 5,5 milionu v Asii. Viz WIKIPEDIA. *World of Warcraft*. *Wikipedia* [online]. Dostupné z: [http://en.wikipedia.org/wiki/World\\_of\\_Warcraft](http://en.wikipedia.org/wiki/World_of_Warcraft) [cit. 2012-09-30]. Počet uživatelů tematicky jinak zaměřeného virtuálního světa *Second Life* v uplynulém roce čítal jeden milion. Viz WIKIPEDIA. *Second Life*. *Wikipedia* [online]. Dostupné z: [http://en.wikipedia.org/wiki/Second\\_Life](http://en.wikipedia.org/wiki/Second_Life) [cit. 2012-09-30].

<sup>8</sup> ŠTIKOVÁ, M. More than Just a Game: User Expectations v. Operator Interests. *Masaryk University Journal of Law and Technology*, 2010, roč. 4, č. 1, s. 48. Dostupné z: <http://mjlt.law.muni.cz> [cit. 2012-09-30].

dí založená na počítačové simulaci fyzického světa.<sup>9</sup> Nejde o světy pouhé imaginace, namísto fyzikálních zákonů v nich panuje počítačový kód. A zatímco fyzický svět se skládá z atomů, virtuální svět z počítačového kódu.<sup>10</sup>

Nefyzičnost virtuálních světů je důvodem, proč lidé nemohou do těchto světů vstupovat přímo, ale jen pomocí prostředníků. Počítač jednak zprostředkovává smyslové vnímání virtuálního světa<sup>11</sup> a jednak umožňuje uživateli působit ve virtuálním prostoru prostřednictvím tzv. avatára, virtuálního alter ega.<sup>12</sup>

Hodnota a síla avatára se odvíjí od jeho úrovně, vlastností, schopností a vybavení, které získává v průběhu hry. Vylepšování avatára je postupný proces, vyžadující zpravidla hodně úsilí, času nebo peněz.

„Klíče“ k virtuálnímu světu patří jeho tvůrci/provozovateli. Uživatelem může být jen ten, koho provozovatel do svého světa pustí; jejich vztah je vztahem smluvním. Neboť virtuální světy mají podobu počítačových programů, chráněných jako autorská díla nebo patenty, má smlouva povahu zpravidla úplatného<sup>13</sup> licenčního ujednání. Charakteristika daného trhu, kde se setkává poměrně malý počet provozovatelů virtuálních prostředí na straně nabídky s nepoměrně větším počtem potenciálních uživatelů na straně poptávky, vede k tomu, že licenční smlouvy jsou unifikované a uzavírané adhezním způsobem.<sup>14</sup>

## 2.2 DEBATA O VIRTUÁLNÍM MAJETKU

V posledních deseti letech se zejména v zahraničí rozvíjí debata o tom, že by regulace virtuálních světů neměla být ponechána jako dosud toliko adhezní uzavíráním licenčních smlouvám mezi provozovateli a uživateli. Nevyvážené postavení uživatelů a provozovatelů není jediným důvodem. Nepochota provozovatelů přiznávat uživatelům absolutní oprávnění k předmětům virtuálního světa, motivovaná obavami z případných žalob proti nim samým, se odráží i v nejistém právním postavení uživatelů ve vztahu k jimi ovládaným částem virtuálních světů vůči třetím osobám (ostatním uživatelům).

<sup>9</sup> Různé definice přisuzují termínu virtuální majetek různě široký obsah. Tato práce si bere za své úzké pojetí, které za virtuální majetek považuje pouze to, co nelze oddělit od virtuálních světů ve výše popsaném smyslu; tedy (1) virtuální předměty – předměty obsažené ve virtuálním světě, (2) avatary – herní postavy a (3) účty uživatelů virtuálního světa; nikoliv internetové domény, adresy elektronické pošty apod.

<sup>10</sup> MACH, P. *Virtuální vlastnictví* [online]. Diplomová práce. Brno: Masarykova univerzita. Právnická fakulta. Katedra právní teorie, 2009, s. 3. Vedoucí práce: Radim Polčák. Dostupné z: <http://is.muni.cz> [cit. 2012-09-30].

<sup>11</sup> S rozvojem technologií se *možností smyslového vnímání* virtuálních světů neustále rozšiřují: pomocí obrazovky lze virtuální svět (jeho grafické zobrazení) vidět, reproduktory přinášejí zvukové vjemy, herní ovladače (tzv. gamepady) umějí dokonce zprostředkovávat otřesy. Důvodem není jen zvýšení prožitku, ale i zprostředkování virtuálního světa ve formě snadno a rychle pochopitelné pro člověka, aby mohl v tomto světě pohotově reagovat na podněty. Způsoby zprostředkování virtuálních světů nejsou omezeny pouze na smyslové cesty. Komunikace mezi uživatelem a virtuálním světem může například probíhat pomocí textových výpisů a příkazů. Z povahy věci jsou však takové způsoby méně lákavé i efektivní.

<sup>12</sup> Avatár je spíše konvenční než nutnou součástí virtuálních světů; příznačný je zejména pro hry na hrdiny.

<sup>13</sup> Typická výše měsíčních poplatků za užívání World of Warcraft činí 15 amerických dolarů (cca 280 Kč).

<sup>14</sup> Pro *smlouvy uzavírané adhezním způsobem* (též adhezní smlouvy) je příznačný způsob jejich vzniku. Nevznikají tak, že by si strany obsah smlouvy sjednaly, ale tak, že jedna strana předloží druhé hotový text smlouvy a ta má možnost návrh buď přijmout, anebo odmítnout. Slovo adhezní odkazuje na to, že druhá smluvní strana k návrhu smlouvy pouze *přistupuje*. Adhezní smlouvy tedy nemají nic společného s adhezním řízením, částí trestního řízení, v níž se projednává právo poškozeného na náhradu škody způsobené trestným činem.

Jednotlivé právněteoretické náhledy na kvalifikaci virtuálních předmětů nejsou podmíněny jen favorizováním uživatelů nebo na druhé straně provozovatelů. Valně má na ně vliv též země původu toho, kdo daný náhled zastává, a tamní soukromoprávní koncepty.

Co je – alespoň pro střední proud těchto názorů – společné, jsou pochyby o tom, že závazková práva z licenčních smluv postačují k dostatečné ochraně uživatelů před zásahy třetích osob, které nejsou stranou smlouvy. Tato obava se opírá o chápání závazků jako souboru relativních práv a povinností, které působí pouze mezi stranami smlouvy, ne už na osoby mimo ni. Proto většina autorů hledí (dle zásad jejich domovského právního řádu) přiznat uživatelům určité absolutní právní postavení ve vztahu k virtuálnímu majetku či alespoň k určité jeho části (virtuálním předmětům, avatárovi či přihlašovacímu účtu). V pozadí jejich úvah často stojí též snaha chránit i držbu těchto statků.<sup>15</sup>

Americká právní teorie zná vlastnictví jak hmotných, tak nehmotných věcí. Proto tamní autoři tíhnou k přiznávání vlastnického oprávnění k virtuálním předmětům. I u nás hojně citovaný<sup>16</sup> Joshua Fairfield dokazuje, že virtuální statky jsou svojí povahou bližší hmotným věcem, spíše než předmětům duševního vlastnictví. Nachází tři společné znaky virtualit a hmotných věcí: (1) omezenost zdroje – nemohou být současně užívány neomezeným počtem subjektů; (2) jsou trvalé; (3) fakticky mohou přijít do styku i s jinými subjekty nebo předměty. Fairfield volá po aplikaci norem majetkového práva i na virtuální majetek a přiznání vlastnických práv k virtuálním předmětům uživatelům.<sup>17</sup>

Že právně dogmatické zvyklosti mají zásadní vliv na teoretické uchopení virtuálních statků, lze dobře ilustrovat na příkladu *Německa*. Pojetí věci a vlastnictví je v německé civilistice natolik spojeno s hmotnými předměty,<sup>18</sup> že virtuální vlastnictví představuje pro většinu německých teoretiků v podstatě protimluv.<sup>19</sup>

Německá autorka Pamela Koch doporučuje zvlášť řešit problematiku herní postavy (avatára) a zvlášť jednotlivých virtuálních předmětů. Herní postava je podle ní výsledkem tvůrčí činnosti uživatele, který do jejího vývoje investuje čas, peníze i vlastní

<sup>15</sup> V českém právním prostředí není zřídka představa, že *držba* je součástí vlastnictví. Tuto představu ještě umocňuje systematika platného občanského zákoníku, pojednávající o držbě mezi ustanoveními o vlastnictví. To neodpovídá povaze držby (*possessio*), neboť jde za prvé o institut obecnější než vlastnictví (držet lze i jiná práva než vlastnické) a za druhé s vlastnictvím mimoběžný. Zatímco vlastnictví vyžaduje oprávnění k věci, tedy právní stav; držba označuje faktický stav. Vlastníkem je ten, kdo je *oprávněn* k výkonu vlastnických práv (ať už je ve skutečnosti vykonává nebo ne); držitelem je ten, kdo tato práva *vykonává*, jakoby mu patřila (ať už je k tomu oprávněn či nikoliv). Vlastník a držitel tedy nemusí být jednou a touže osobou (drží např. i zloděj nebo nabyvatel věci na základě neplatné smlouvy). Vlastníkovi ovšem vždy svědčí právo věc držet (*ius possidendi*), které může proti držiteli prosadit vlastnickou žalobou. Od držitele třeba navíc lišit detentora, který sice má věc ve faktické moci (příp. vykonává obsah určitého práva), avšak buď nikoliv pro sebe, protože vykonává držbu pro někoho jiného (např. nájemce detinuje pronajatý byt, ale držitelem je pronajímatel-vlastník bytu), nebo danou věc nelze podle právního řádu vlastnit (např. návykové látky nebo části lidského těla).

<sup>16</sup> Viz např. MACH, P., *cit. dílo* nebo HARAŠTA, J. Virtuální vlastnictví. In: ŽATECKÁ, E. et al. (ed.). *Cofola 2011: The Conference Proceedings*. Brno: Masarykova univerzita, 2011, s. 1305–1322.

<sup>17</sup> FAIRFIELD, J. A. T. Virtual Property. *Boston University Law Review*, 2005, roč. 85, s. 1050 a 1094.

<sup>18</sup> Viz § 90 a 903 německého občanského zákoníku (BGB) a WIELING, H. J. *Sachenrecht*. 5. vydání. Berlin/Heidelberg: Springer, 2007, s. 21.

<sup>19</sup> Viz GRAMLICH, L. Preliminary Thoughts on Online Property. *Masaryk University Journal of Law and Technology*, 2009, roč. 3, č. 1, s. 183–186; a PEUKERT, A. (rec.). BERBERICH, M. *Virtuelles Eigentum*. Tübingen: Mohr Siebeck, 2010. *UFITA*, 2011, č. 1, s. 204–208.

energii. Tím přidává k původnímu, „blanketnímu“ avatárovi hodnotu, kterou nevytvořil provozovatel virtuálního světa. A právě díky této přidané hodnotě by měl avatár být více než jen částí počítačového programu provozovatele. Je nutno ho kvůli tomu považovat za samostatný nehmotný statek náležející uživateli. Právním pojítkem, které spojuje uživatele s nehmotným avatárem, nemůže být dle německého práva vlastnictví. Je třeba proto konstruovat zvláštní absolutní majetkové právo k nehmotným statkům, které však svým obsahem prakticky odpovídá vlastnickému právu.

Naproti tomu ve virtuálních předmětech se nijak nezračí žádná hodnota přidaná uživatelem, jsou součástí herního software a není tedy důvod je prohlašovat za zvláštní předmět majetkového práva, který by měl navzdory licenční smlouvě náležet uživateli.<sup>20</sup>

České příspěvky do diskuze o povaze virtuálního majetku jsou sporé a nelze hovořit o nějakém specifickém českém přínosu. Čeští a slovenští autoři zhusta přebírají závěry anglo-americké právní vědy.<sup>21</sup> Přitom však zapominají, že české právo spadá do té části kontinentu, která – alespoň pokud jde o účinný občanský zákoník z roku 1964 – je ovlivněna německým pohledem na věc v právním smyslu.

### 3. VIRTUÁLNÍ MAJETEK PODLE ČESKÉHO PRÁVA

#### 3.1 VLASTNICKÉ PRÁVO A JEHO PŘEDMĚT

Obecně vlastnické právo vyjadřuje dvojí: (a) právní přináležitost předmětu (věci) k subjektu (osobě) a (b) pojmovou možnost (oprávnění) subjektu libovolně nakládat s předmětem v mezích daných objektivním právem a ostatní z tohoto nakládání vyloučit.<sup>22</sup>

Již z toho plyne základní požadavek na předmět vlastnického práva, *odlišnost od subjektu*.<sup>23</sup> Ostatní požadavky se v zásadě liší podle příslušného právního řádu. Česká doktrína vyžaduje, aby předmět vlastnického práva byl objektivně *ovladatelný, užitečný (hodnotný)*<sup>24</sup> a nebyl vyloučený z právního obchodu (nikoliv *res extra commercium*).

Pro účely tohoto příspěvku má rozhodující význam, zda předmět vlastnického práva musí být též *hmotný, či nikoliv*.<sup>25</sup> V České republice se odpověď na tuto otázku bude

<sup>20</sup> KOCH, P. Die rechtliche Bewertung virtueller Gegenstände auf Online-Plattformen. *JurPC Web-Dok* [online], 2006, č. 57. Dostupné z: <http://www.jurpc.de/aufsatz/20060057.htm> [cit. 2012-09-30].

<sup>21</sup> Šrov. GÁBRIS, T. Definičia veci a výzvy modernej vedy. *Justičná revue*, 2008, roč. 60, č. 4, s. 529–540; MACH, P. *Cit. dílo*; HARAŠTA, J., KOČÍ, M., ŠMERKL, P. Virtual Money in China. *Masaryk University Journal of Law and Technology*, 2010, roč. 4, č. 2, s. 191–204. Dostupné z: <http://mujlt.law.muni.cz> [cit. 2012-09-30]; HARAŠTA J. *Cit. dílo*; ŠTIKOVÁ, M. *Cit. dílo*.

<sup>22</sup> ELIÁŠ, K. Vlastnické právo: Paradigmata českého pojetí pod zkušebními kameny kontinentální právní kultury. *Právní rozhledy*, 2005, č. 22, s. 807 an.

<sup>23</sup> GAMBARO, A. Property Rights in Comparative Perspective: Why Property Is So Ancient and Durable. *Tulane European & Civil Law Forum*, 2011, roč. 26, s. 226.

<sup>24</sup> Jde o obecné vlastnosti věci. Viz KNAPP, V., KNAPPOVÁ, M. *Cit. dílo*, s. 239 a ELIÁŠ, K. In: ELIÁŠ, K. et al. *Občanský zákoník: Velký akademický komentář, § 119*. Praha: Linde, 2008, s. 477.

<sup>25</sup> V odpovědi na tuto otázku se jednotlivé jurisdikce nejvíce liší. Je oblíbeným omylem, že častější je v Evropě výlučně hmotná koncepce vlastnictví (jak se kupř. tvrdí na straně 20 legislativního záměru slovenského občanského zákoníku, schváleného slovenskou vládou 4. srpna 2008. Dostupné z: <https://lt.justice.gov.sk> [cit. 2012-09-30]). Výlučně hmotné vlastnictví je typické pouze pro právní řády inspirované německým občanským právem (kam lze však řadit i většinu zemí tzv. východního bloku). Naproti tomu v zemích galo-románského právního okruhu (Francie, Belgie, Lucembursko, Itálie, Španělsko, Por-

lišit podle toho, bude-li měřítkem občanské či trestní právo,<sup>26</sup> a ještě více bude-li se rozhodovat podle platné a účinné občanskoprávní úpravy či podle nového občanského zákoníku.<sup>27</sup>

Zatímco totiž § 118 občanského zákoníku z roku 1964<sup>28</sup> člení předměty majetkového práva v objektivním smyslu do tripartice: (1) věci (hmotné), (2) majetková práva (v subjektivním smyslu) a (3) jiné majetkové hodnoty, přičemž předmětem vlastnického práva jsou dle většinového názoru pouze věci; nový občanský zákoník bere za své široké pojetí věci a vlastnického práva. Za věci výslovně prohlašuje i práva a jiné nehmotné statky a všechny je činí předmětem vlastnického práva.

### 3.2 VIRTUÁLNÍ STATKY JAKO MAJETKOVÝ PŘEDMĚT A VLASTNICKÉ PRÁVO K NIM

Jsou virtuální statky věcmi v právním smyslu, či nikoliv? Oprostíme-li se od požadavku hmotnosti, vidíme, že virtuální předměty splňují všechny znaky: existují nezávisle na subjektu, jsou ovladatelné a penězi ocenitelné (slouží potřebám lidí).<sup>29</sup>

Zdá se tedy, že by mohly být i předmětem vlastnického práva, či jiného obdobného absolutního majetkového práva.

Způsobilost být předmětem určitého práva ovšem ještě neznamená, že toto právo svědčí uživateli předmětu. Aby bylo možno o někom říci, že je vlastníkem, musí se jím nejprve stát, *musejí nastat určité skutečnosti, s nimiž objektivní právo spojuje vznik vlastnictví*. A zde vyvstává jeden z velkých problémů virtuálního vlastnictví – na základě jakého právního důvodu vznikne vlastnictví uživatelů?

David Sheldon podrobil empirickému výzkumu *smluvní licence* patnácti nejoblíbenějších virtuálních světů, *vlastnické právo* k virtuálním předmětům uživatelů *nezakládá* žádná z nich. Sheldon zkoumal, jak licenční ujednání rozvrhují tři klasická vlastnická oprávnění: právo věc užívat, vyloučit ostatní a právo věc převést. Zjistil, že uživatelům je zásadně přiznáváno pouze právo užívat virtuální předměty, ostatní práva jsou buď výrazně omezena, nebo vyhrazena provozovateli daného virtuálního světa.<sup>30</sup>

Uživatelé se tedy na základě licenční smlouvy s provozovatelem stávají spíše nájemci-pachtýři virtuálních statků; v žádném případě není jejich právní postavení souměřitelné s jednotným vlastnickým právem.

Krom toho si provozovatelé navíc vyhrazují právo jednostranně měnit smluvní podmínky a zabavovat virtuální předměty či celé uživatelské účty. To spolu s adhezí

---

tugasko, Rumunsko a Malta), anglo-amerického práva (Anglie, Irsko a Kypr) a většinově též v severských (Dánsko, Švédsko) a pobaltských státech (Litva a Lotyšsko) hmotnost či nehmotnost předmětu nehraje žádnou roli v konstrukci vlastnického práva.

<sup>26</sup> K tomu srov. pozn. pod čarou č. 6.

<sup>27</sup> Zákon č. 89/2012 Sb.

<sup>28</sup> Platný a účinný zákon č. 40/1964 Sb.

<sup>29</sup> Virtuality mají hodnotu, poněvadž jim lidé hodnotu přisuzují a jsou ochotni je směniti za peníze. Z tohoto hlediska se neliší od hmotných věcí. Mylná je představa, že hmotné věci mají hodnotu jaksi samy o sobě, hodnotu věcem připisují lidé (viz Epiktétův citát na začátku tohoto příspěvku). Ustrženy nehet bude mít pokaždé jinou hodnotu, bude-li pocházet od bezdomovce na hlavním nádraží, anebo od Karla Gotta či Natalie Portman.

<sup>30</sup> SHELDON, D. P. Claiming Ownership, But Getting Owned: Contractual Limitations on Asserting Property Interests in Virtual Goods. *UCLA Law Review*, 2007, roč. 54, s. 763–773.

povahou smluv vede k spravedlnostním úvahám o vyrovnávání postavení uživatelů a provozovatelů buď v soudních řízeních, nebo cestou kogentní zákonné úpravy.

Proti tomu však vyvstává několik logických protiargumentů.

Aplikace korekčních mechanismů svěřených soudům (např. dobrých mravů) může sloužit k „otupení nejostřejších hrotů“, tj. k omezení určitých práv provozovatele (např. svévolně rušit uživatelské účty či zabavovat virtuální majetek), ale stěžít může vést ke vzniku vlastnického oprávnění uživatelů, které před smlouvou neměli.

Kogentní založení vlastnických práv zákonnou úpravou navzdory výslovnému licenčnímu ujednání, představuje výrazný zásah do smluvní autonomie. Jakýkoliv takový zásah vyžaduje silný důvod. Tradičně tomu je tam, kde se smlouva týká životně či společensky důležitého statku, jako např. u nájemní nebo pracovní smlouvy, nebo kde by opačné ujednání představovalo rozpor s dobrými mravy nebo veřejným pořádkem. O nic takového v případě virtuálních světů ovšem nejde. Virtuální světy slouží především počítačovým hrám. Bez provozovatelů by ani nemohly fungovat.<sup>31</sup>

Nezdá se tedy, že by existoval dostatečný důvod, proč by měl zákon přepisovat smlouvu a zcela obracet rozvržení vlastnických práv k virtuálním statkům. Přiznání úplného vlastnického práva představuje nejvýraznější právní omezení ostatních ve vztahu k vlastněnému předmětu. Mají-li být uživatelé chráněni před zásahy třetích osob do jejich virtuálního majetku a svévolnými zásahy provozovatele, lze tohoto efektu dosáhnout i proporcionálnější cestou.

James Grimmelmann si všímá, že rozdělení práv ve virtuálních světech připomíná lenní držbu (*seisin*),<sup>32</sup> jakoby provozovatel dával uživateli část virtuálního světa v léno a zavázal se při tom, že bude jeho léno chránit proti vnějším zásahům. Podle Grimmelmanna lze v oživení lenní držby vidět rozumné uspořádání právních vztahů ve virtuálním světě. Externí soudy by se do virtuálních světů měly vměšovat co nejméně a v zásadě až tehdy, kdy se uživatelé nedomohli spravedlivé nápravy, resp. spravedlivého procesu u provozovatele.

Anglické lenní držbě na českém území korespondoval institut *děleného vlastnictví*, jehož pozůstatky se zachovaly ještě ve všeobecném občanském zákoníku (ABGB).<sup>33</sup> Půda v děleném vlastnictví měla dva vlastníky: (1) vrchního, kterému náleželo vlastnictví k podstatě, a (2) užitkového, kterému náleželo vlastnictví k užitku. S rozpadem feudálních svazků byla koncepce děleného vlastnictví opuštěna, i když i bez vazby na virtuální světy se připomíná, že jde o obecný pojem, který může být stále nosný.<sup>34</sup> Jeho nespornou výhodou je přiznání věcněprávního, tudíž absolutního, postavení užitkovému vlastníkovi.<sup>35</sup>

<sup>31</sup> Jsou to často sami uživatelé, kdo se domáhá zásahu provozovatele, např. v případě, kdy je obtěžuje jiný uživatel.

<sup>32</sup> GRIMMELMANN, J. *Virtual World Feudalism. Yale Law Journal Pocket Part*, 2009, roč. 118, s. 126–130. Dostupné z: <http://yalelawjournal.org/the-yale-law-journal-pocket-part/property-law/virtual-world-feudalism> [cit. 2012-09-30].

<sup>33</sup> Vyhlášen císařským patentem č. 946/1811 ve Sbírce zákonů soudních.

<sup>34</sup> Názorným a praktickým příkladem ze současnosti, kde by bylo dělené vlastnictví dobře využitelné, může být vztah leasingového pronajímatele a nájemce k předmětu leasingu.

<sup>35</sup> HORÁK, O. Tzv. dělené vlastnictví v 19. a 20. století: K proměněným chápání tradičního pojmu v domácí právní vědě. In: DÁVID, R., SEHNÁLEK, D., VALDHANS, J. (ed.). *Dny práva 2010 = Days of Law 2010*. Brno: Masarykova univerzita, 2010, s. 1513–1523.

Dělené vlastnictví se tak skutečně jeví jako ideální řešení majetkových poměrů ve virtuálních světech, které by vyhovovalo jak zájmům uživatelů, tak provozovatelů. Kondicionál je na místě, neboť v českém právu koncept děleného vlastnictví naráží na velmi zásadní překážky.

První je rozpor s Listinou základních práv a svobod, která jednoznačně normuje, že vlastnické právo všech vlastníků má stejný zákonný obsah (čl. 11 odst. 1 věta druhá). To z povahy věci není u děleného vlastnictví možné.

I kdyby postavení uživatele nemělo být založeno na děleném vlastnictví, nýbrž na jiném, ad hoc vytvořeném věcném právu, nelze přehlédnout závažný problém s takovým postupem spojený. Absolutní práva se na rozdíl od závazkových práv bezprostředně dotýkají postavení třetích osob, a z tohoto důvodu je nelze vytvářet jinak než zákonem (platí pro ně numerus clausus).<sup>36</sup> Bez zásahu zákonodárce tedy nepřichází žádná zvláštní věcné právo vůbec do úvahy.

Budeme-li se držet platného práva, je stále zjevnější, že přiblížení právního postavení uživatelů absolutním právům, jakkoli bohubíbé, nemůže vést přes ztotožňování vlastnictví přímo s virtuálními předměty. A nemá-li tento příspěvek skončit ve zbytečných radách zákonodárci, je třeba hledat cestu jinudy.

### 3.3 VIRTUÁLNÍ MAJETEK JAKO AUTORSKOPRÁVNÍ LICENCE

Vraťme se nyní zpět na začátek, kdy jsme hovořili o tom, že *virtuální světy jsou v podstatě počítačovými programy*. Z nedostatku jiné vhodné ochrany je právo chránit jako literární autorská díla a pohlíží na ně tak, jakoby dily byly (§ 2 odst. 2 věta první autorského zákona).<sup>37</sup> Počítačové programy nemusejí splňovat všechny předpoklady kladené na autorská díla. Stačí, jsou-li původní (originální) v tom smyslu, že jsou autorovým vlastním duševním výtvorem (nejde o plagiát, rozmnoženinu nebo napodobeninu).<sup>38</sup> Autorskoprávně chráněny jsou i jednotlivé části, splňují-li samy podmínku původnosti (§ 2 odst. 3 autorského zákona); ostatní části jsou chráněny jako součást celku – počítačového programu.<sup>39</sup>

Nabízí se tedy chránit zájmy uživatelů ve virtuálním světě jako autorskoprávní licenci k počítačovému programu, event. k jeho částem.

V čem je výhoda tohoto pojetí, které tu bylo od počátku a které jsme už použili jako odrazový můstek k tomu, abychom našli nějaké absolutní právní postavení uživatelů k virtuálním statkům?

<sup>36</sup> V teorii se objevují hlasy, které zpochybňují dělení majetkových práv na absolutní a relativní. V Čechách mezi ně v období první republiky patřili čeští normativisté – František Weyr a Jaromír Sedláček, v padesátých a šedesátých letech Viktor Knapp. V poslední době se jejich názory ožívají v pracích Jiřího Spáčila. Srov. SPAČIL, J. *Věcná břemena v občanském zákoníku*. Praha: Beck, 2006, s. 1–7. Pochybnosti panují i o účelnosti uzavřeného počtu věcných práv (principu numerus clausus), k tomu viz WORTHINGTON, S. *The Disappearing Divide Between Property and Obligation: The Impact of Aligning Legal Analysis and Commercial Expectation*. *Texas International Law Journal*, 2007, roč. 42, s. 925 n. Ačkoliv tyto názory mají racionální jádro, drží se tato práce většinového náhledu, podle něhož působí závazková práva bez dalšího pouze vůči smluvním stranám a nezakládají navenek (vůči třetím osobám) povinnost zdržet se zásahů do smlouvou založených práv.

<sup>37</sup> Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

<sup>38</sup> TELEČ, I., TŮMA, P. *Autorský zákon: komentář*. Praha: Beck, 2007, s. 35.

<sup>39</sup> ŠVESTKA, J., DVORÁK, J. (ed.). *Občanské právo hmotné*. 3. díl. Praha: Wolters Kluwer, 2009, s. 176.



První plus dlužno spatřovat už v tom, že se nejméně protiví licenčním dohodám mezi uživateli a provozovateli virtuálních světů.

Další veledůležitou výhodou autorskoprávních licencí, tj. užívacích práv k autorským dílům, oproti jiným užívacím právům (např. nájmu),<sup>40</sup> je, že jsou v nauce českého soukromého práva jednohlasně brány za v zásadě obchodovatelný majetkový statek.

*Podle nového občanského zákoníku* tím odpadají prakticky všechny komplikace: licence je nehmotnou věcí (§ 489, 496 odst. 2), kterou lze vlastnit (§ 1011).<sup>41</sup> Proti zásahům do vlastnického práva se může vlastník bránit vlastnickými žalobami (zápůrčí žalobou a žalobou na vydání věci).<sup>42</sup> K ochraně držby vlastnického práva k licenci má uživatel k dispozici i žalobu posesorní.<sup>43</sup>

V případě *účinného občanského zákoníku z roku 1964* je situace složitější. Právní věda z něj vycházející považuje v duchu § 118 licenci za jinou majetkovou hodnotu,<sup>44</sup> či majetkové právo.<sup>45</sup> Podstatné je, že ani to ani ono není podle převažujícího náhledu předmětem vlastnického práva. Namísto toho teorie nabízí zbytečnou a pochybnou scholastiku: toho, komu patří majetkové právo nebo jiná majetková hodnota, nazývá majitelem a jeho poměr k předmětu majitelstvím. Dělítkem mezi vlastnickým právem a majitelstvím je právě a jen (ne)hmotnost předmětu. Netřeba zdůrazňovat, že zákoník sám úpravu práv a povinností majitele nestanoví. Nemá-li být majitelství jen bezobsažnou nálepkou, aplikují se na něj v důležitých otázkách analogicky ustanovení o vlastnickém právu.<sup>46</sup> Soudní praxe přihlíží k povaze jednak majetkové hodnoty a jednak pravidla, které má být na základě obdoby aplikováno.<sup>47</sup> Charakter licence k virtuálním světům – její zásadní podobnost k hmotným movitým věcem<sup>48</sup> – si žádá připuštění jejího vydržení i vlastnických žalob na její ochranu.

<sup>40</sup> Ke kritice možného chápání nájemního práva jako nehmotné věci srov. MELZER, F. Pojem věci v návrhu občanského zákoníku. *Právník*, 2007, č. 11, s. 1217–1229.

<sup>41</sup> Shodně TELEČ, I. Duševní vlastnictví a jeho vliv na věc v právním smyslu. *Právní rozhledy*, 2011, č. 12, s. 444 n.

<sup>42</sup> Může vyvolávat pochyby, zda přichází v úvahu žaloba na vydání věci u nehmotné věci. Třeba však mít na zřeteli, že právní obchod se týká převodů práv a oprávnění a umožnění držby těchto práv, věc sama se nemusí hnout z místa. Vyhraje-li žalobce reivindikační spor, musí žalovaný ukončit vlastní držbu a umožnit ji žalobci. V případě licence to znamená, že musí přestat užívat licenci způsobem, který je v rozporu s právy žalobce a případně odevzdat žalobci nástroje, jimiž licenci využíval (např. přístupové kódy k uživatelskému účtu).

<sup>43</sup> Výhodou posesorních žalob je, že držitel nemusí prokazovat platný vlastnický titul, ale toliko nabytí držby, že nenabyl držbu násilím, lstí nebo výprosu.

<sup>44</sup> Tak ELIÁŠ, K. et al. *Občanský zákoník*, § 118, s. 471 nebo ŠVESTKA, J. et al. *Občanský zákoník*, § 118, s. 642.

<sup>45</sup> TELEČ, I. *Právo duševního vlastnictví. Výkon práv duševního vlastnictví (licenční právo)* [online]. 2009. Dostupné z: [http://is.muni.cz/do/1499/el/estud/praf/ps09/ppv09/web/law/pdv/tisk/vykon\\_prav.pdf](http://is.muni.cz/do/1499/el/estud/praf/ps09/ppv09/web/law/pdv/tisk/vykon_prav.pdf) [cit. 2012-09-30].

<sup>46</sup> Jiří Špáčil hovoří v souvislosti s rozlišením mezi majitelstvím a vlastnictvím o pokroku právní vědy. Těžko v tom však spatřovat něco víc než projev aplikační schizofrenie, když se nejprve určité předměty vyloučí z dosahu vlastnického práva teleologickou redukcí nebo i jen restriktivním výkladem, aby tam později mohly být vráceny analogií. Není-li rozdíl v obsahu institutů, ale jen v jejich předmětu, pak se rozumný význam štěpení ztrácí. Proč není stejnou logikou na dva různé instituty rozděleno i vlastnické právo k věcem movitým na jedné straně a nemovitým na druhé a obdobně k věcem zužititelným a nezužitelným nebo k věcem určeným individuálně a věcem určeným druhově? Možných členění se najde celá řada, přesnost právní vědy se nijak neztrácí, připojí-li se k vlastnictví rozlišovací adjektivum: vlastnictví movité vs. nemovité, hmotné vs. nehmotné atd. Srov. k tomu ŠVESTKA et al. *Občanský zákoník*, před § 123, s. 681.

<sup>47</sup> Zatímco u obchodního podílu (jiná majetková hodnota) Nejvyšší soud dovodil, že může být vydržen za stejných podmínek jako věci movité (Rc 50/2008), v případě pohledávky (majetkové právo) už dříve tentýž senát vyloučil možnost užití žaloby na vydání věci (Rc 28/2002).

<sup>48</sup> Srov. výše shrnutý postřeh Fairfieldův.

K právě naznačenému je třeba učinit několik vysvětlujících poznámek.

*Za prvé* se nijak nezpochybnují výsledky teorií, které zdůrazňují rozdíl mezi autorským dílem a počítačovým kódem a v kódu vidí obdobu hmotného podkladu, jímž je dílo vyjádřeno.<sup>49</sup> Jde ovšem o náhled, který neodpovídá současnému pojetí ochrany počítačových programů. Jestliže se počítačový program, tj. ucelený a funkčně ohraničený soubor počítačového kódu, chrání jako dílo literární, pak hledět na program a na kód jako na dva odlišné předměty dává stejný smysl jako rozlišovat mezi románem a písmeny, slovy nebo větami v knize. Nepomůže ani odvolání na binární zápis, je jedno, jakým jazykem je počítačový program vyjádřen, pořád jde o týž program. Rozdíl je možno najít teprve mezi programem a jeho zachycením na datovém úložišti (pevném disku serveru). V případě virtuálních světů rozhodující roli hraje užívání programu, ne konkrétní datové úložiště (kde je program uložen je zcela lhostejné).

*Za druhé* se nastíněným řešením nezatemňuje ani skutečnost, že programy, jež pohybují virtuálními světy, využívají ke svému chodu databázi a že jednotlivé virtuální předměty jsou zjednodušeně řečeno položkami v těchto databázích.<sup>50</sup> Bylo by však chybou odhlížet od vlastního fungování virtuálních světů, uživatelé je neužívají jako databáze, ale jako programy. Že program využívá databáze, nepředstavuje víc než technické řešení, jímž se oddělují obsahová data od abstraktního algoritmu („hmota od procesu“). Uživatelé nemají možnost využívat databáze mimo program; databáze slouží programu, ne uživatelům.

*Za třetí* mít licenci znamená mít právo užívat licencovaný předmět stanoveným/dohodnutým způsobem v určitém rozsahu. Sporné může být, zda mohou být virtuální předměty licencovatelné samostatně. Přání se snadno stává „otcem“ špatné myšlenky: jakkoli liberálním a pro posuzovaný případ vhodným řešením by se jevila možnost mít samostatné licence k jednotlivým virtualitám, je třeba dle platného práva přisvědčit opaku. Autorský zákon nepřipouští pochyby, že definice autorských děl a kvasi-autorských děl (vč. počítačových programů) a tedy objektů autorskoprávních licencí je kogentní. Na virtuální předměty lze nahlížet jako na části programu, též chráněné autorským právem, nicméně licencovatelné pouze jako součást celku.

Podmínky užívání virtuálního světa se řídí jednak licenčním ujednáním (ev. obchodními podmínkami), jednak povinností respektovat licence ostatních uživatelů. Licence neznamená právo užívat celý virtuální svět výhradně; jaké části a v jakém rozsahu má uživatel k dispozici a jak se může dobat i dalších částí virtuálního světa, je dáno právě písemnou smlouvou, povinností respektu k právům druhých a pravidly a zvyklostmi fungování daného virtuálního světa.

*Za čtvrté* stranou úvah byly dosud ponechány virtuální předměty vytvořené uživateli (inkorporaci těchto předmětů do virtuálního světa dovoluje Second Life). Třeba ovšem na ně rovněž pohlížet jako na součást počítačového programu, který se stává dílem spojeným. Vypořádání autorských práv je věcí smluvní dohody mezi tvůrcem věci a provozovatelem virtuálního světa.

*Za páté* při konstruování systému právní ochrany nelze odhlížet od kontextu. Zájmy uživatelů ve virtuálních světech musejí být chráněny s respektem k principu proporcio-

<sup>49</sup> MACH, P. *Cit. dílo*, s. 34.

<sup>50</sup> SHELDON, D. *Cit. dílo*, pozn. pod čarou č. 41.

nality a účelu těchto světů. Ochrana individuálních uživatelských práv by v konečném důsledku neměla vést k narušení smyslu existence virtuálních světů, jímž většinou bývá hra. Uživatelé přistupují na pravidla hry, proto by se soudní zásahy měly týkat toliko jednání mimo kontext hry, byť to může vést ke zdánlivým paradoxům. Dovoluje-li hra přemoci avatára jiného uživatele a vzít si předměty z jeho inventáře, je třeba to právně respektovat jako dovolené jednání. Naproti tomu porušení slibu vrátit zapůjčený virtuální meč – není-li výjimečně porušování slibů nebo podvádění připuštěno herními pravidly –, bude představovat delikt. Pravidla či herní zvyklosti ovšem nejsou nedotknutelná a mohou být podrobeny přezkumu souladu s dobrými mravy či veřejným pořádkem.

#### 4. TRESTNĚPRÁVNÍ DŮSLEDKY

Zde zastávaný náhled na virtuální vlastnictví jako na autorskoprávní licenci se promítá i do trestního práva.

Je nutno poopravit pohled trestněprávní nauky, která připodobňuje virtuality hmotným věcem a trestné činy, jejichž předmětem je virtuální majetek, klasifikuje jako klasické majetkové trestné činy.<sup>51</sup>

Trestní zákoník<sup>52</sup> vychází z kategorizace předmětů majetkových práv zavedené občanským zákoníkem z roku 1964, i když se nedrží úplně věrně občanskoprávní tripartice. První odchylkou je už to, že rozlišuje pouze mezi věcmi a jinými majetkovými hodnotami (kam spadají i majetková práva). Za druhé věci nechápe jen jako hmotné předměty, když mezi ně řadí i prostředky na účtu (což je v podstatě pohledávka za bankovním ústavem, tedy dle občanského práva majetkové právo). Trestní zákoník však z prostředků na bankovním účtu činí věc jako výjimku z pravidla; ostatní nehmotné předměty spadají do skupiny jiných majetkových hodnot (jinak by byla tato kategorie zbytečná).

Autorskoprávní licence je proto i v trestním právu nutno řadit mezi jiné majetkové hodnoty a jednání, jež se jich týkají, nemohou být větnány do skutkových podstat, v nichž je předmětem útoku pouze věc a nikoliv jiná majetková hodnota. To je případ skutkových podstat loupeže (§ 173) a krádeže (§ 205), naopak například skutkové podstaty zpronevěry (§ 206) nebo neoprávněného užívání cizí věci (§ 207) pamatují jak na věci, tak na jiné majetkové hodnoty.<sup>53</sup>

Jednání, která by až na předmět útoku, naplňovala skutkovou podstatu krádeže, dlužno posuzovat jako trestný čin porušení autorského práva dle § 270. „Virtuální loupež“ by měla být trestná jako souběh porušení autorského práva s vydíráním (§ 175).

<sup>51</sup> Srov. GRÍVNA, T. Virtual Crimes. *Masaryk University Journal of Law and Technology*, 2008, roč. 2, č. 1, s. 97–104. Dostupné z: <http://mjlt.law.muni.cz>; GRÍVNA, T. Existují virtuální trestné činy? In: VANDU-CHOVÁ, M., GRÍVNA, T. (ed.). *Pocta Otovi Novotnému k 80. narozeninám*. Praha: ASPI, 2008, s. 28–35; POBOŘILOVÁ, M. *Virtuální trestné činy*. Diplomová práce. Praha: Univerzita Karlova. Právnická fakulta. Katedra trestního práva, 2010, s. 40–49. Vedoucí práce: Tomáš Grívna.

<sup>52</sup> Zákon č. 40/2009 Sb.

<sup>53</sup> Nakolik připadá do úvahy použití zpronevěry u virtuálních předmětů, není jisté. Jednání, které má zpronevěřovací charakter, by totiž ve skutečnosti vedlo pouze k poklesu hodnoty licence k virtuálnímu světu jako celku, nikoliv ke ztrátě celé licence (i za předpokladu, kdyby zapůjčení virtuálního meče znamenalo zřízení podlicence). Proto i tady bude na místě aplikovat spíše skutkovou podstatu trestného činu dle § 270 trestního zákoníku.

## 5. ZÁVĚR

Mnohouživatelské virtuální světy vyvolávají velmi podobné majetkové otázky, jaké ve světě lidí vyvolávají od nepaměti, kde rovněž pluralita subjektů soutěží o užívání omezených majetkových hodnot. Tradiční majetkové právo je oním nástrojem, který sleduje rozvržení subjektivních práv coby možných způsobů nakládání s majetkovými hodnotami mezi subjekty. Čistě teoreticky vyhovuje klasický majetkoprávní koncept vlastnictví i virtuálním světům. V praxi se však postavení uživatelů virtuálních světů co do obsahu jejich práv k virtualitám natolik liší od pozice vlastníka, že o vlastnictví nelze dost dobře mluvit.

Eventuální přiznání úplného vlastnického práva uživatelům zákonem by bylo nejhrubším zásahem do dosavadních právních poměrů mezi uživateli a provozovateli virtuálních světů. Takové rozřešení, které obrací naruby vztahy založené smlouvou, se navíc nejeví ani nutné ani ospravedlnitelné, neboť je projevem neuctivosti k zájmům provozovatelů virtuálních světů. Jak už před sto lety napsal český kriminalista Josef Prušák: „*Úkolem práva jest úprava lidského spolužití a ne bezohledný boj jedněch proti druhým.*“<sup>54</sup> Právní řád nemá absolutizovat práva jedněch na úkor druhých.

Bez investice provozovatelů do vytvoření, udržování, spravování a inovací virtuálních prostředí, by virtuální světy nemohly nikdy ani existovat. Zásahy provozovatelů do chodu světa se často dějí v zájmu samotných uživatelů, např. při vyloučení těch, kteří obtěžují ostatní. Hledět na uživatele jen jako na oběti vydané na milost a nemilost „zlym a temným padouchům“ – provozovatelům, se jeví nejen přehnané, ale i jako nedostatečný důvod pro totální převrácení vlastnických práv.

Se zneužívajícími klauzulemi v textech licenčních smluv si lze poradit za pomoci nástrojů smluvního závazkového práva o smlouvách uzavíraných se spotřebitelem a adhezních smlouvách.

Život ve virtuálních světech připomíná svým uspořádáním někdejší feudální lenní svazky. Má-li být respektováno postavení provozovatelů a současně uživatelům přiznáno vlastnické právo k virtuálním statkům, je dělené vlastnictví patrně nejlepším prostředkem. Obnovení děleného vlastnictví v českém právu by však vyžadovalo zásadní změny právního řádu, které se ani nezdají reálné.

Odhlédnuto od fantazijních změn právního řádu lze i v českém právu nalézt způsob, jakým poskytnout uživatelům ochranu jejich virtuálního majetku i vůči třetím osobám.

V této práci je za východisko zvolena licence, která je zvnitřku relativním právem k užívání virtuálního světa a navenek majetkovým statkem, který může být předmětem absolutního majetkového práva. Uživatelé (třetí osoby) nemohou porušit smlouvu mezi provozovatelem a jiným uživatelem, kde nejsou smluvníky. Mohou pouze zasáhnout do vlastnického práva, jehož předmětem je licence. Naproti tomu provozovatel se vůči uživateli může dopustit porušení jak smlouvy, tak – subsidiárně – vlastnického práva, v závislosti na charakteru jednání.

Nepochybnou předností českého práva je systém držby podděděný ze starého rakouského práva. Držba není svázána s věcí, nýbrž s právem: držba práva spočívá v jednání,

<sup>54</sup> PRUŠÁK, J. *Rakouské právo trestní. Díl všeobecný*. Praha: Spolek českých právníků Všeherd, 1912, s. 153.

keré je obsahem daného práva. Držitel vlastnického práva se fakticky chová jako vlastník (třebaže vlastníkem není), obdobně držitel užívacího práva k autorskému dílu jedná, jakoby byl licencionářem. Svou držbu licence k virtuálním světům může tedy uživatel v každém případě chránit držebními žalobami, aniž by bylo třeba (jako ve většině jiných jurisdikcí) vymýšlet, že drží (virtuální) věc.

Český právní řád nabízí mnoho cest k řešení problematiky virtuálního vlastnictví, jinou otázkou je, kdy se dle kolizních pravidel mezinárodního soukromého práva na virtuální vztahy použije úprava obsažená v českých předpisech. Na vztahy mezi uživateli a provozovateli se nejspíše použije právo, jímž se řídí licenční smlouva (což bude český právní řád jen výjimečně). Delikt ní nároky mezi uživateli, které nepředstavují porušení smlouvy, by se však měly vypořádat podle práva místa, kde se delikt stal (kde došlo ke škodné události). V případě deliktů, které se staly na internetu, to může být řada míst (umístění serveru, místo, kde se nachází škůdce nebo poškozený). Výběr konkrétní jurisdikce bude patrně na poškozeném.<sup>55</sup> Výběr rozhodného soukromého práva nemá vliv na působnost trestního práva, která je stanovena kogentně a tradičně široce tak, že virtuální trestné činy mohou spadat pod režim českého trestního zákoníku poměrně často.<sup>56</sup>

#### VIRTUAL PROPERTY – PROPERTY IN THE TIME OF *IUS DOWNLOADENDI*

##### Summary

This part deals with a new kind of property, property in virtual worlds, and its consequences in the real (physical) world. In comparison to existing works, it focuses more on law in force rather than philosophical thoughts about property. Although theoretical concepts may be important for defining what property is and what could be an object of ownership, they cannot by themselves establish property rights of a particular subject. This is role of applicable law. Here, particular attention is paid to Czech private law, but implications in the criminal law are not overlooked.

An author does not deny that virtual objects can be property in legal sense, and thus fall within the scope of property law. Users may own them, but they do not regularly own them. License agreements which govern the relationships between providers and users concerning virtual worlds grant users property rights to virtual things almost never.

Ideal allocation of rights between providers and users may resemble an feudal concept of seisin (or divided ownership). However, enactment of divided ownership within Czech law is exposed to such obstacles that it is better to search for another concept. This part examines possibilities of a license agreement.

*Key words:* property, virtual property, intangibles

*Klíčová slova:* vlastnictví, virtuální vlastnictví, nehmotné vlastnictví

<sup>55</sup> Srov. POLČÁK, R. *Právo a evropská informační společnost* [online]. Brno: Masarykova univerzita, 2009, s. 70–76. Dostupné z: <http://www.polcak.com> [cit. 2012-09-30].

<sup>56</sup> Tamtéž, s. 60–68. Viz § 4–9 trestního zákoníku.

## REDAKČNÍ RADA

*Předseda:* prof. JUDr. Pavel Šturma, DrSc.

*Tajemnice:* Ludmila Matoušková

### *Členové:*

doc. JUDr. PhDr. Ilona Bažantová, CSc.

prof. JUDr. Miroslav Bělina, CSc.

prof. JUDr. Stanislava Černá, CSc.

doc. JUDr. Jaroslav Drobník, CSc.

prof. JUDr. Marie Karfíková, CSc.

doc. JUDr. Vladimír Kindl

prof. JUDr. Zdeněk Kučera, DrSc.

prof. JUDr. Václav Pavlíček, CSc., dr. h. c.

prof. JUDr. Jiří Švestka, DrSc.

prof. JUDr. PhDr. Michal Tomášek, DrSc.

prof. JUDr. Petr Tröster, CSc.

JUDr. Marie Vanduchová, CSc.

prof. JUDr. Alena Winterová, CSc.

### *Externí členové:*

prof. JUDr. Michael Bogdan (Lund)

prof. JUDr. Jiří Boguszak, DrSc. (Praha)

prof. Dr. Władysław Czapliński (Varšava)

doc. JUDr. Taisia Čebišová, CSc. (Praha)

prof. JUDr. Jan Filip, CSc. (Brno)

prof. Dr. Michael Geistlinger (Salzburg)

prof. JUDr. Mahulena Hofmannová, CSc. (Giessen/Heidelberg)

prof. JUDr. Pavol Holländer, DrSc. (Brno)

prof. JUDr. Dalibor Jílek, CSc. (Brno/Bratislava)

Dr. Kaspar Krolop (Berlín)

prof. JUDr. Jan Musil, CSc. (Brno)

prof. JUDr. Jan Svák, CSc. (Bratislava)

prof. Dr. Jiří Toman (Santa Clara)

JUDr. Peter Tomka, CSc. (Haag)

prof. JUDr. Helena Válková, CSc. (Plzeň/Praha)

prof. Dr. Miroslav Vítěz (Subotica)

doc. JUDr. Ladislav Vojáček, CSc. (Brno/Bratislava)



ACTA  
UNIVERSITATIS  
CAROLINAE

---

IURIDICA 4/2012

## KYBERNETICKÁ KRIMINALITA

Prorektor-editor: prof. PhDr. Ivan Jakubec, CSc.  
Vědecký redaktor: prof. JUDr. Jiří Jelínek, CSc.  
Recenzovali: doc. JUDr. Tomáš Grivna, Ph.D.  
doc. JUDr. Radim Polčák, Ph.D.  
Obálku navrhla Jarmila Lorencová  
Graficky upravila Kateřina Rezáčová  
Vydala Univerzita Karlova v Praze  
Nakladatelství Karolinum, Ovocný trh 3–5, 116 36 Praha 1  
<http://cupress.cuni.cz>  
Praha 2013  
Sazba DTP Nakladatelství Karolinum  
Vytiskla tiskárna Nakladatelství Karolinum  
Periodicita: 4×/rok  
Vydání 1. Náklad 300 výtisků  
ISSN 0323-0619  
MK ČR E 18585