UNIVERZITA KARLOVA

Právnická fakulta

Igor Grejták

Trestnoprávna zodpovednosť za šírenie protiprávneho obsahu v prostredí Internetu

Diplomová práca

Vedúci diplomovej práce: prof. JUDr. Bc. Tomáš Gřivna, Ph.D

Katedra: Katedra trestného práva

Dátum vypracovania práce (uzatvorenie rukopisu): 3. 2. 2024

Prehlasujem, že som predkladanú diplomovú prácu vypracoval samostatne, že všetky použité zdroje boli riadne uvedené a že práce nebola využitá k získaniu iného alebo rovnakého titulu.

Ďalej prehlasujem, že samotný text tejto práce vrátane poznámok pod čiarou má 191 029 znakov vrátane medzier.

Igor Grejták

V Prahe dňa 3. 2. 2024

Ďakujem vedúcemu diplomovej práce, prof. JUDr. Bc. Tomášovi Gřivnovi, Ph.D. za jeho cenné poznatky, rady a pripomienky pri tvorbe tejto diplomovej práce. Ďalej moje poďakovanie patrí mojím blízkym za vyjadrenú podporu počas celého štúdia.

Obsah

Zoznam použitých skratiek

ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
CDA	Communications Decency Act
CE	Značka CE
DDoS	Distribuované odmietnutie služby
DSA	Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách)
IP	Internet protocol
IT	Informačné technológie
MAC adresa	Media access control address
NS	Najvyšší súd Českej republiky
TCP	Transmission control protocol
EÚ	Európska únia
ESĽP	Európsky súd pre ľudské práva
VPN	Virtual Private Network
VHS	Video Home System (slov. Obrazový domáci systém)
Wi-Fi	Wireless Fidelity
ZSIS	Zákon č. 480/2004 Sb., o niektorých službách informačnej spoločnosti a o zmene a doplnení niektorých zákonov

Úvod

Hardvér prvých počítačov zaberal celé miestnosti a ich cena bola v rádoch desiatok miliónov korún. Prístup k nim bol pre túto vysokú cenu a používateľskú zložitosť obmedzený len na pomerne malý okruh technologických odborníkov. Vyvodzovanie trestnoprávnej zodpovednosti páchateľov v oblasti počítačovej kriminality nepredstavovalo v tom čase tak naliehavú a zložitú výzvu ako dnes.[1] Sprístupňovaním internetu novým používateľom, spolu s neustálym rozvojom informačných a komunikačných technológii, sa nielenže rozšírili možnosti páchania stávajúcej trestnej činnosti, ale taktiež so sebou prinieslo nové hrozby, ktoré sú typické práve pre online prostredie.

Veľké sociálne siete umožnili v podstate nekontrolovateľné šírenie obsahu, a to fakticky bez účinnej možnosti vyvodzovania zodpovednosti. Stali sa fórami na ktorých sa nekontrolovane šíri protiprávny obsah. Európa v tejto súvislosti zaznamenala v posledných rokoch opätovný vzostup militantných pravicovo-extrémistických skupín, nárast protiimigračného a islamofóbneho násilia, ako aj protivládnych útokov a útokov na politických oponentov, etnické a sexuálne menšiny. Protiprávny obsah na internete predstavuje vážne riziko pre spoločnosť, keďže môže viesť k radikalizácii jednotlivcov a skupín, a následne k zvyšovaniu rizika násilia v reálnom svete. A taktiež, novo nastupujúce technológie autonómnych strojov umožňujú samovoľné vytváranie a šírenie obsahu na internete.

Problematika vyvodzovania trestnoprávnej zodpovednosti za šírenie protiprávneho obsahu v prostredí internetu, ako súčasť počítačovej kriminality, sa tak pre svoju komplikovanosť a cezhraničný charakter stala jednou z najaktuálnejších výziev súčasnej právnej teórie. Pri posúdení trestnosti určitého konania páchateľa a pre správne vymedzenie jeho trestnoprávnej zodpovednosti v prostredí internetu, nestačí len podradenie jeho trestnoprávne relevantného konania pod určitú skutkovú podstatu, ale je nutné zároveň pochopiť častokrát zložitému fungovaniu informačných a komunikačných technológii ako takých, vrátane orientácie sa v nastupujúcich trendoch v tejto oblasti. Je otázne, do akej miery dokáže súčasná právna úprava reagovať na stále sa meniace výzvy, ktoré so sebou technologický pokrok prináša.

Primárnym cieľom tejto diplomovej práce je posúdiť dostatočnosť právnej úpravy, v súvislosti s vyvodzovaním trestnoprávnej zodpovednosti pri páchaní trestnej činnosti v prostredí internetu, so špecifickým zameraním sa na šírenie protiprávneho pornografického a inak sexualizovaného obsahu prostredníctvom neho. V spoločnosti dochádza k neustálemu rozvoju

[1] KLIMEK, L.; ZÁHORA, J. a HOLCR, K. *Počítačová kriminalita: v európskych súvislostiach*. Bratislava: Wolters Kluwer, 2016. s. 17. ISBN 978-80-8168-538-5.

nových funkcionalít internetu a tie so sebou zákonite prinášajú aj nové hrozby, ktoré už nemusí niekoľko rokov stará právna úprava dostatočne odrážať. Diplomová práca sa zameriava predovšetkým na právnu úpravu trestnej činnosti ohrozujúcu právo na sexuálne súkromie, pričom posudzuje jej aktuálnosť s ohľadom na nové trendy v spôsobe páchania trestnej činnosti v tejto oblasti.

Okrem primárneho cieľa, si diplomová práca kladie niekoľko čiastkových cieľov. V prvom rade definuje základné pojmy, ktoré sú potrebné pre pochopenie komplexnosti trestnoprávnej zodpovednosti v prostredí internetu. Častokrát sa v technologickej praxi stretávame s pojmami, ktoré aj napriek svojej dôležitosti nemajú svoju legálnu definíciu. V prvej časti si diplomová práca kladie za cieľ predstaviť čitateľovi jednotlivé míľniky pri vývoji internetu a v historickom exkurze poskytnúť informácie o vývoji v spôsoboch páchania počítačovej trestnej činnosti a prijímanej právnej úprave v tejto oblasti. Fenomén počítačovej kriminality, v súvislosti so šírením protiprávneho obsahu je čitateľovi predstavený takým spôsobom, aby reflektoval spoločenské a technologické zmeny, ktoré so sebou prinieslo rozšírenie používania digitálnych technológii. Cieľom tejto časti je predstaviť hrozby vyvstávajúce z rozširovania využívania internetu, a to aj s ohľadom na jeho cezhraničný charakter, ktorý sťažuje prácu orgánom vymáhania práva a zákonodarcom, pri zavádzaní legislatívneho rámca.

V ďalšej časti sa diplomová práca zaoberá samotnou trestnoprávnou zodpovednosťou za šírenie protiprávneho obsahu v prostredí internetu. Cieľom tejto časti diplomovej práce je vymedziť trestnoprávnu zodpovednosť a zaradiť ju do kontextu stále aktuálnej problematiky jej vyvodzovania v prostredí internetu. S tým nepochybne súvisí aj problematika pôsobnosti práva v prostredí internetu a vymáhania práva na internete. Diplomová práca si v tomto kontexte pokladá otázku, či je možné uplatniť právny poriadok na právne vzťahy v prostredí internetu ako také, alebo je potrebné akceptovať jeho špecifiká a prispôsobiť tomu aj právnu úpravu.

V ďalšej časti, v kontexte vyvodzovania trestnoprávnej zodpovednosti, diplomová práca rozdeľuje jednotlivé subjekty ktoré pôsobia pri šírení obsahu v prostredí internetu a vymedzuje podmienky ich trestnoprávnej zodpovednosti. Konkrétne rozlišuje trestnoprávnu zodpovednosť samotného šíriteľa protiprávneho obsahu, trestnoprávnu zodpovednosť subjektov, ktoré v rámci svojej činnosti umožňujú šírenie protiprávneho obsahu tretími osobami, a v neposlednom rade reflektuje aj nastupujúci trend vyvodzovania trestnoprávnej zodpovednosti za konanie autonómnych systémov umelej inteligencie pri šírení obsahu.

V prípade trestnoprávnej zodpovednosti šíriteľa protiprávneho obsahu sa diplomová práca okrem všeobecnej definície trestnoprávnej zodpovednosti, zameriava na už zmienenú analýzu

súčasnej právnej úpravy v oblasti ohrozovania sexuálneho súkromia a protiprávneho šírenia pornografie, ako ho diplomová práca definuje v ďalších častiach, a jej aplikáciu na možné variácie páchania trestnej činnosti v tejto oblasti. Následne diplomová práca vymedzuje trestnoprávnu zodpovednosť poskytovateľov služieb informačných spoločností, ktoré v rámci svojej činnosti poskytujú služby, ktoré svojím používateľom umožňujú protiprávny obsah ukladať, šíriť a sťahovať. V tejto časti si diplomová práca kladie za cieľ popísať rozdiely súčasnej právnej úpravy a novo prijatej, priamo použiteľnej európskej právnej úpravy.

Posledná časť diplomovej práce sa zameriava na špecifiká trestnoprávnej zodpovednosti za protiprávne šírenie zo strany autonómnych strojov, predovšetkým umelej inteligencie. V tomto ohľade je potrebné dodať, že nie je primárnym cieľom komplexne popísať všetky aspekty zodpovednosti za autonómnu technológiu alebo umelú inteligenciu, pretože táto problematika by si vyžadovala pre svoju rozsiahlosť samostatné spracovanie. Cieľom tejto kapitoly je predovšetkým oboznámiť čitateľa s aspektom pôsobnosti daného subjektu, predstaviť mu definície základných pojmov, pripravovanú legislatívu v tejto oblasti a praktické príklady už páchanej trestnej činnosti zo strany umelej inteligencie a možné vyvodzovanie trestnoprávnej zodpovednosti za nich.

1. Pôsobnosť trestného práva v prostredí internetu

1.1. Vznik internetu a jeho vplyv na spoločnosť

Vznik internetu spôsobil bezpochyby revolúciu vo formách masovej komunikácie, vo fungovaní masmédií a obchode tým, že zmenil spôsob akým nahliadame na šírenie informácii. Samotný koncept, na ktorom je internet postavený pritom vznikol v Spojených štátoch len v 70. rokoch 20. storočia,[2] kedy bola do prevádzky uvedená prvá počítačová sieť s názvom ARPANET (*angl. Advanced Research Projects Agency Network*). ARPANET bol navrhnutý na zdieľanie informácií medzi výskumnými pracovníkmi, pôsobiacimi na rôznych univerzitách, s cieľom uľahčiť výmenu poznatkov, a tým zefektívniť ich vedeckú činnosť. Súbežne s ARPANETOM vznikali ďalšie prepojené počítačové siete, ktoré taktiež slúžili na prenos informácii medzi limitovaným okruhom subjektov.[3]

V sedemdesiatych rokoch vedci z organizácie ARPA, ktorá stojí za vývojom ARPANETU spoločne s vedcami zo Stanfordovej univerzity vyvinuli univerzálny programovací jazyk, ktorý umožnil rôznym počítačovým sieťam komunikovať a vymieňať si informácie medzi sebou. Tento programovací jazyk sa nazýva protokol pre riadenie prenosu alebo tiež širokej verejnosti viac známi ako internetový protokol (*angl. Transmission Control Protocol / Internet Protocol – TCP / IP*). Sieť ARPANET sa ďalej rozvíjala a postupne sa do jej štruktúr pripájali ďalšie počítačové siete, čím vznikol základ internetu, ako ho poznáme dnes.[4]

Internet, ako je už možné dedukovať z jeho samotného názvu, predstavuje celosvetový systém prepojenia počítačov a iných zariadení, ktorý im umožňuje medzi sebou komunikovať, prijímať a odosielať informácie. Internet funguje na základe systému protokolov, ktoré určujú na ktoré miesto v rámci siete sa má informácia preniesť. IP adresy sú jedinečné identifikátory, ktoré určujú umiestnenie konkrétneho počítača alebo zariadenia v rámci siete.[5] Samotný internet tak funguje na základe prepínania tzv. paketov, ktorými sú dáta rozdelené na menšie časti a prenášané cez sieť. Routery sú špecializované počítače, ktoré zabezpečujú, aby informácie dorazili na správne miesto v sieti, a aby ostatní používatelia neboli preťažení veľkým množstvom dát.[6]

---

[2]Porov. napr. definíciu pojmu Internet v portáli BRITTANICA [online]. [cit. 2023-5-20]. Dostupnú z https://www.britannica.com/technology/Internet.

[3] HARMADA, A. Predchodca internetu sa začal rozrastať presne pred 54 rokmi. In Živé.sk [online]. [cit. 2023-5-20] Dostupnú z https://zive.aktuality.sk/clanok/149753/predchodca-internetu-sa-zacal-rozrastat-presne-pred-54-rokmi/.

[4]GRIFFITHS, R. T. (n.d.). *The History of the Internet*. In Uniba.sk [online]. [cit. 2023-5-20]. Dostupné z http://edu.fmph.uniba.sk/~winczer/SocialneAspekty/GergelInternetHistoria.html.

[5] URAM, J. *Čo je to internet, ako funguje a aká je jeho história?* In Visibility.sk [online]. [cit. 2022-5-20]. Dostupné z: https://visibility.sk/blog/internet-existuje-uz-viac-ako-50-rokov-co-by-ste-mali-o-nom-vediet/.

[6] BARAN, P. *Paul Baran and the Origins of the Internet.* In Rand.org [online]. [cit. 2022-5-20]. Dostupné z: https://www.rand.org/about/history/baran.html.

Pochopenie spôsobu prenosu dát je podstatné z hľadiska určenia zodpovednosti poskytovateľov služieb informačných spoločností, ktorí priamo protiprávny obsah nešíria, ale poskytujú ich používateľom prostredie na jeho šírenie.[7]

Od pojmu internet, ktorý chápeme ako infraštruktúru, technologickú sieť, ktorá umožňuje na základe protokolov prenos dát medzi miliardami počítačov po celom svete, je potrebné rozlišovať pojem kybernetický priestor alebo kyberpriestor.

Kybernetický priestor je abstraktný termín, ktorý odkazuje na virtuálne prostredie, ktoré vzniklo vďaka internetu. Je to virtuálne miesto, na ktorom sa odohrávajú digitálne aktivity, akými sú online komunikácia, vytváranie a zdieľanie obsahu, elektronický obchod, kybernetická bezpečnosť a mnoho ďalších činností. Zjednodušene povedané, internet predstavuje fyzickú infraštruktúru siete, zatiaľ čo kybernetický priestor je digitálny ekosystém, ktorý je na tejto sieti postavený.[8] Legálnu definíciu kybernetického priestoru nájdeme v § 2 písm. a) zákona o kybernetickej bezpečnosti,[9] ktorý kybernetický priestor definuje ako digitálne prostredie, ktoré umožňuje vznik, spracúvanie alebo výmenu informácii. Toto digitálne prostredie je podľa definície tvorené informačnými systémami a službami sieti elektronických komunikácii.[10]

V súčasnosti sa rozvoj internetu spája predovšetkým s rozširovaním predmetov každodennej potreby, ktoré pri svojom fungovaní využívajú prístup k internetu. Jedná sa o tzv. chytré zariadenia, ktoré sú v právnej teórii označované ako internet vecí. Podľa európskej politiky internetu vecí sa predpokladá, že sa počet chytrých zariadení pripojených k internetu vecí zvýši z približne 40 miliárd v roku 2023 na 49 miliárd do roku 2026.[11] To predstavuje značnú výzvu pre zákonodarcov a orgány pre vymáhanie práva, ako sa postaviť k novým výzvam spojeným s rozširovaním internetu.

V roku 2023 podľa portálu *Statista* využívalo internet denne 5,18 miliardy ľudí po celom svete, čo predstavuje približne 65 percent svetovej populácie. Toto číslo bude s určitosťou narastať spolu s rozširovaním prístupu internetu do rozvojových častí sveta.[12] Globálna vlna rozvoja

---

[7] Porov. ďalšiu časť diplomovej práce, ktorá sa zaoberá zodpovednosťou poskytovateľov služieb informačných spoločností za šírenie protiprávneho obsahu.

[8] SARANGHAM, A. (2021): *Cyber Space: A Comprehensive Guide in 2021*. In UNext Learning Pvt. Ltd. 2020. online]. [cit. 2023-05-20]. Dostupné z: https://u-next.com/blogs/cyber-security/cyber-space/.

[9] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Ďalej v práci ako zákon o kybernetickej bezpečnosti.

[10] Pozri tiež časť I.3.1 tejto diplomovej práce.

[11] Porov. politiku Európskej komisie *Politika v oblasti internetu vecí v Európe*. In Europa.eu [online]. [cit. 2023-05-20]. Dostupné z: https://digital-strategy.ec.europa.eu/sk/policies/internet-things-policy.

[12] Štatistika vychádza z portálu Statista s názvom *Number of internet and social media users worldwide as of October 2023*. In Statista.com [online]. [cit. 2023-05-23]. Dostupné z: https://www.statista.com/statistics/617136/digital-population-worldwide/.

informačných a komunikačných technológií sa stala silnou hnacou silou v takmer každom aspekte rozvoja spoločnosti.[13] Pokiaľ ide o otázky kriminality, je nepochybné, že rozširovanie dostupnosti digitálnych technológií je neodmysliteľne spojené aj s nežiaducimi rizikami a výzvami, ktoré môžu mať významné následky pre bezpečnosť jeho používateľov a spoločnosti ako takej.

Zavádzanie nových informačných a komunikačných technológií mení ustálené vzorce správania sa v spoločnosti, a tým aj metódy a povahu vykonávania trestnej činnosti. Týmto spôsobom prenáša páchanie bežnej trestnej činnosti do kybernetického priestoru, ale zároveň predostiera aj nové formy trestnej činnosti, ktoré sú charakteristické pre digitálne prostredie. To so sebou zákonite prináša bezprecedentné výzvy pre zaistenie prevencie a riadne vyšetrovanie kriminality zo strany štátnych orgánov, ktoré sa musia zorientovať v častokrát komplexnej problematike fungovania nových technológii. Ústredným prvkom tejto dynamickej transformácie sa stal bezpochyby internet a technológie, ktoré sú s jeho využívaním spojené.[14] Zvyšovanie dostupnosti technológii v spoločnosti predovšetkým zvýšilo riziká protiprávnych konaní potencionálnych páchateľov, ktoré môžu viesť k narušovaniu ochrany súkromia a osobných údajov, šíreniu nezákonného a škodlivého obsahu, čo v sebe zahŕňa napríklad protiprávne šírenie pornografie (vrátane šírenia detskej pornografie), internetové pirátstvo, dezinformácie, počítačovú kriminalitu a kybernetické útoky.[15]

1.2. Začiatky regulácie internetu

Právne poriadky jednotlivých štátov vznikali na princípe, že právne normy daného štátu sa aplikujú v rámci územia alebo na osoby, na ktoré dopadá dosah štátnej moci.[16] Pôsobnosť právnych noriem v prostredí internetu predstavuje isté špecifikum zavedeného spoločenského konsenzu. Používatelia internetu vnímali internet ako miesto, na ktoré nedopadajú zavedené normy spoločnosti a akékoľvek snahy o reguláciu zo strany štátu považovali za nemysliteľné. Pokusy o reguláciu internetu, boli preto častokrát zo strany jeho používateľov vnímané ako

[13] SALIFU, A. (2012): *The impact of internet crime on development*, Journal of Financial Crime. In Emerald.com, [online]. [cit. 2023-05-24]. Dostupné z: https://www.emerald.com/insight/content/doi/10.1108/13590790810907254/full/html.

[14] Porov. MAJID, J. (2916): *Online Crime*. In Oxford Research Encyclopedia of Criminology. [online]. [cit. 2023-05-24]. Dostupné z: https://www.academia.edu/33173425/Online_Crime_In_Oxford_Research_Encyclopedia_of_Criminology_2016_DOI_10_1093_acrefore_9780190264079_013_112.

[15] Diplomová práca tieto pojmy rozoberá v ďalších častiach.

[16] RAMEŠOVÁ, K. (2023): *Právní regulace kybernetické bezpečnosti a její meze. 1. vydanie*. Praha: C. H. Beck, s. 56, marg. č. 106. ISBN: 978-80-7400-931-0.

neprimeraný zásah štátnej moci do slobody jednotlivca, čoho vyjadrením je napríklad dokument s názvom *Deklarácia nezávislosti kybernetického priestoru*.[17]

Zástancovia deklarácie nezávislosti kybernetického priestoru zastávali anarchistický prístup k regulácii internetu, na základe ktorého zdôrazňovali, že spoločenské a právne vzťahy, ktoré vznikajú v rámci internetového prostredia, by nemali byť viazané žiadnou formálnou spoločenskou zmluvou. Práve naopak, spoločenstvo používateľov internetu bolo podľa tvorcov a zástancov deklarácie považované za samoregulatívne, a z tohto hľadiska by nemalo spadať pod žiadnu autoritatívnu reguláciu zo strany štátnej moci. [18] Kritici tohto prístupu však poukazovali na to, že s nárastom počtu používateľov internetových služieb a ich rozmanitosti sa pôvodné predstavy o samoregulácii začali javiť ako nerealistické, ba dokonca až ako utopické. Navyše odmietnutie uplatnenia práva v online prostredí by predstavovalo bezprecedentný zásah do právnej istoty jednotlivca a porušenie princípu zákazu *denegatio iustitiae*. So spomínaným nárastom počtu používateľov internetu vzrástla aj potreba regulácie jednotlivých aspektov jeho používania, ktoré sa postupom času začali javiť ako problematické.[19]

Prvotné snahy o reguláciu internetu sme zaznamenali v 90. rokoch 20. storočia, v súvislosti s reguláciou odvetvia telekomunikácií.[20] Časom dochádzalo k zintenzívneniu dozoru nad obsahom na internete, pričom zákonodarcovia reagovali na konkrétne hrozby, ktoré vznikali s rozšírením používania internetu.

Jedným z prvých pokusov o obmedzenie škodlivého obsahu na internete bol zákon o slušnosti v komunikácii (angl. *Communications Decency Act - CDA*) ktorý bol schválený v Spojených štátoch amerických ako súčasť zákona o telekomunikáciách z roku 1996. CDA bol navrhnutý s cieľom regulovať a riadiť obsah na internete, pričom sa špecificky zameriaval na riešenie obáv týkajúcich sa distribúcie neslušného, obscénneho alebo urážlivého obsahu. CDA bol prijatý predovšetkým v reakcii na vzostup šírenia pornografie na internete. Konkrétne vymedzoval trestnosť konania jednotlivcov, ktorí šírili pornografický obsah osobám mladším ako osemnásť rokov. Okrem toho priniesol CDA vylúčenie zodpovednosti pre poskytovateľov internetových služieb za obsah zdieľaný prostredníctvom ich platforiem používateľmi. Jeho znenie vychádzalo

[17] Sloboda jednotlivca v kybernetickom priestore sa stala ústrednou témou deklarácie kybernetického priestoru, americkej organizácie Electronic Frontier Foundation, ktorá bola založené v roku 1990 aktivistom J. P. Barlowom.
[18] BARLOW, J. P. *A Declaration of the Independence of Cyberspace*. In EFF [online]. [cit. 2023-05-22]. Dostupné z: www.eff.org/cyberspace-independence.
[19] Porov. napr. dokument vlády Spojených štátov Declaration for the Future of the Internet. In State.gov [online]. [cit. 2023-05-22]. Dostupné z https://www.state.gov/declaration-for-the-future-of-the-internet.
[20] Napríklad v roku 1992 vstúpil v USA do platnosti zákon o telekomunikáciách (*H.R.2977 - Public Telecommunications Act of 1992*), ktorý mimo iného upravoval aj niektoré otázky týkajúce sa internetu.

z predpokladu, že nikto nesmie byť zodpovedný za konanie tretej osoby. Zároveň by akýkoľvek postih prevádzkovateľov internetových služieb mohol viesť k ich vypínaniu, a tým by mohlo dôjsť k ohrozeniu slobody prejavu používateľov.[21] Pred prijatím CDA bol zodpovedným za protiprávny obsah práve poskytovateľ internetovej služby.

Na svoju dobu predstavovalo CDA pomerne pokrokovú legislatívu, ktorá do veľkej miery pripomína princípy súčasnej legislatívy v oblasti zodpovednosti používateľov internetu a poskytovateľov internetových služieb. Časť CDA, ktorá regulovala zodpovednosť používateľov za „neslušný" obsah šírený na internete, však bola zrušená v dôsledku porušenia prvého dodatku ústavy Spojených štátov v prípade *Reno v. ACLU*.[22]

S plynutím času vzniklo množstvo právnych predpisov s cieľom regulovať rôzne aspekty používania internetu. Ide najmä o národné a nadnárodné právne normy, ktoré upravujú konkurenčné prostredie na internete a obmedzujú nelegálny obsah šírený prostredníctvom neho.[23]

V súčasnosti je ústredným prvkom problematiky regulácie internetu úloha, ktorú zohráva pri procese globalizácie a s tým súvisiaca problematika rozvoja internetovej kriminality. Tieto globálne výzvy si vyžadujú plnú angažovanosť a medzinárodnú spoluprácu ako v rozvinutých, tak aj v rozvojových krajinách sveta. Dôvodom je skutočnosť, že vyšetrovanie internetovej kriminality si častokrát vyžaduje zhromažďovanie dôkazov a vykonávanie vyšetrovacích krokov v rôznych suverénnych jurisdikciách. Medzinárodná spolupráca pri presadzovaní práva v internetovom prostredí tak predstavuje v dnešnej globalizovanej digitálnej ére zložitú a naliehavú výzvu, a to predovšetkým s ohľadom na rozdiely v právnych systémoch a právnych rámcoch jednotlivých krajín, ktoré komplikujú proces trestného stíhania internetovej kriminality, ktorá býva častokrát páchaná cezhranične.

---

[21] § 230 CDA chráni poskytovateľov internetových služieb, ako sú sociálne médiá, diskusné fóra, a iné online platformy, pred zodpovednosťou za obsah, ktorý na ich platformách zverejňujú používatelia. Toto ustanovenie im umožňuje poskytovať priestor pre voľnú výmenu informácií a názorov bez toho, aby za obsah, ktorý publikujú ich užívatelia, niesli zodpovednosť. Toto ustanovenie má významný vplyv na fungovanie internetu a na právnu reguláciu obsahu online. Je to teda kľúčové ustanovenie v oblasti ochrany slobody slova a práva na vyjadrovanie na internete v Spojených štátoch. Porov. napríklad iniciatívu *Electronic Frontier Foundation* ohľadom § 230 CDA dostupnú z: https://www.eff.org/issues/cda230.

[22] Najvyšší súd Spojených štátov rozhodol, že ustanovenie CDA týkajúce sa obscénneho materiálu sú v rozpore s prvým dodatkom Ústavy Spojených štátov, ktorý zaručuje slobodu prejavu. Toto rozhodnutie v podstate zrušilo časť CDA, ktorá by mohla obmedziť obsah na internete. Súdu prekážalo jeho plošné uplatnenie, keďže jeho pôsobnosť nebola obmedzená na konkrétny obsah, skupiny používateľov ani na konkrétne spôsoby šírenia. Práve táto plošná regulácia bola prehlásená za protiústavnú. Porov. napr.: https://www.oyez.org/cases/1996/96-511.

[23] Európska únia schválila v polovica roka 2022 súbor nariadení, ktorých cieľom je regulácia poskytovateľov digitálnych služieb a nezákonného obsahu, vrátane šírenia dezinformácii. Jedná sa nariadenia o digitálnych službách a digitálnom trhu. Diplomová práca sa bližšie zaoberá jednotlivými nariadeniami v ďalších kapitolách.

V praxi tak vznikajú situácie, kedy právny rámec jednej krajiny nemusí dostatočne účinne reflektovať riziká daného trestného činu, čo umožňuje páchateľom uniknúť trestnej zodpovednosti. Ďalším problémom je nedostatok spoločných medzinárodných noriem a dohôd o internetovej kriminalite a presadzovaní práva v prostredí internetu. To znamená, že orgány presadzovania práva majú obmedzené možnosti prístupu k údajom uloženým v zahraničí, čo môže výrazne spomaliť vyšetrovanie a proces presadzovania práva. Okrem toho vo svete, kde je technologický pokrok rýchlejší ako zmeny v právnych predpisoch, je ťažké držať krok s novými formami internetových hrozieb a trestných činov. Isté regulátorné snahy možno vidieť v rámci Európskej únie, ktorá v svojich politikách a legislatívnej činnosti stále viac odráža nastupujúce trendy v oblasti ochrany pred hrozbami, ktoré so sebou zákonite prináša spoločenský rozvoj internetu a informačných technológii.

Na základe uvedeného je nepochybné, že v dnešnej dobe nie je možné internet považovať za akési právne vákuum, ale skôr ako prostriedok, na ktorý dopadá právny poriadok ako celok, vrátane práva trestného. Niektoré existujúce právne normy, predovšetkým z ohľadom na dobu ich prijatia, ale nie je možné aplikovať na právne vzťahy v prostredí internetu bez ďalšieho, je preto nevyhnutné aby súdy pristúpili k rozšírenej interpretácii právnych noriem a zákonodarcovia by mali reagovať na do tejto doby neupravené právne vzťahy prijatím nových právnych predpisov.

1.3. Pôsobnosť právnych noriem trestného práva v prostredí internetu

Pôsobnosť právnych noriem vyjadruje okruh spoločenských vzťahov, na ktoré sa vzťahujú právne normy a podmienky, za ktorých sa tieto normy uplatnia.[24] Správne vymedzenie okruhu spoločenských vzťahov v prostredí internetu, na ktoré dopadne regulácia českého právneho poriadku môže v niektorých prípadoch predstavovať zložitú otázku. Pre vymedzenie okruhu trestnoprávne relevantných konaní osôb, ktoré spočívajú v šírení protiprávneho obsahu je predovšetkým podstatné si vymedziť aplikovateľnosť ustanovení o miestnej a osobnej príslušnosti a vymedziť ich špecifiká na internete. V ďalších častiach sa preto nebudeme zaoberať kritériami pôsobnosti časovej a vecnej, ktoré nevyvolávajú pri posúdení trestnoprávnej zodpovednosti páchateľa v prostredí internetu tak zásadné problémy.[25]

(a) Miestna príslušnosť

Všeobecne platí, že sa podľa trestného práva Českej republiky posudzujú tie trestné činy, ktoré sú spáchané na jej území. Definične je táto zásada rozšírená v § 4 ods. 2 trestného zákonníka,

[24] GERLOCH, A. *Teorie práva. 4. upravené vydání*. Plzeň: Aleš Čeněk, 2007, s. 68 - 73. ISBN 978-80-7380-023-9.
[25] Porov. § 1 až 3 trestného zákonníka.

ktorý za činy spáchané na území Českej republiky považuje taktiež tie trestné činy, ktorých sa páchateľ dopustil aspoň z časti na území Českej republiky, aj keď ich následok mal nastať v zahraničí. A taktiež, ak porušil záujmy chránené trestným zákonníkom v zahraničí za predpokladu, že následok jeho konania nastal alebo mal nastať aspoň z časti na území Českej republiky.[26] Právne predpisy nevymedzujú špecifické podmienky na určenie miestnej príslušnosti pre trestné činy spáchané prostredníctvom internetu, a preto pri posúdení trestnoprávnej zodpovednosti vychádzame z týchto všeobecných pravidiel.

Na základe vyššie uvedenej definície miestnej príslušnosti je pomerne jednoduché vymedziť trestnosť konania páchateľa, a s ňou spojenú trestnoprávnu zodpovednosť v prípade, ak páchateľ šíri protiprávny obsah v prostredí internetu za fyzickej prítomnosti v Českej republike, to znamená prostredníctvom pripojenia sa k internetu v Českej republike.

Všeobecne tak môžeme zhrnúť, že v prípade ak páchateľ šíri nezákonný obsah prostredníctvom internetu, posúdi sa trestnosť jeho konania podľa českého trestného práva v prípade, ak sa fyzický zdržiava na území Českej republiky a využíva internetové pripojenie v nej. To znamená, že páchateľ využíva internet z pripojenia na území Českej republiky. Podľa judikatúry Najvyššieho súdu Českej republiky[27] je pre určenie miestnej príslušnosti dôležitá IP adresa, z ktorej sa páchateľ prihlasoval k internetu prostredníctvom počítača.[28] IP adresa počítača ale nie je jediným rozhodným ukazovateľom miesta spáchania trestného činu, a to najmä v prípade, ak páchateľ pri trestnom konaní využil tzv. služby VPN.

VPN (angl. *Virtual Private Network*) je technológia, ktorá umožňuje používateľom možnosť šifrovaného pripojenia sa k internetu. Aj keď technológia VPN nedokáže používateľovi poskytnúť úplnú anonymitu, môže ju čiastočne zvýšiť tým, že skryje jeho skutočnú IP adresu. Pri posúdení naplnenia znakov miestnej príslušnosti, tak bude potrebné vychádzať aj z ďalších skutočnosti. Nie je možné sa spoliehať len na sieťové identifikátory.[29]

Pre spoľahlivé určenie miestnej príslušnosti bude problematické predovšetkým posúdenie trestných činov, ktoré boli spáchané v zahraničí, a ktoré zároveň vyvolávajú účinok v Českej republike. Takýto spôsob trestného konania býva v trestnoprávnej teórii označovaný ako dištančný delikt. Dištančné delikty sú typické tým, že medzi miestom, kde došlo k trestnoprávne relevantnému konaniu páchateľa, a miestom, kde došlo alebo malo dôjsť k trestnoprávne

[26]Porov. § 4 trestného zákonníka
[27] V ďalších častiach je Najvyšší súd Českej republiky označovaný tiež len ako Najvyšší súd alebo niekde ako NS.
[28] Uznesenie Najvyššieho súdu zo dňa 16.12.2015, sp. zn. 7 Td 73/2015.
[29] V predmetnej veci (NS sp. zn. 7 Td 73/2015) vychádzal pri posúdení miestnej príslušnosti Najvyšší súd Českej republiky aj z miesta bydliska, v ktorom sa obvinená zdražievala.

relevantným následkom, existuje určitá fyzická vzdialenosť.[30] Tento aspekt posúdenia trestnoprávnej zodpovednosti má dopad predovšetkým pri určovaní príslušnosti súdov. V tejto súvislosti môžeme konštatovať, že miestna príslušnosť trestného práva na páchateľa dopadne, pokiaľ aspoň čiastočne konal na území Českej republiky, alebo ak následok ním spáchaného trestného činu nastal aspoň čiastočne na tomto území, alebo tu eventuálne mal nastať. Nezáleží pritom akú podstatnú úlohu toto konanie alebo následok predstavovalo pre celkovú trestnú činnosť páchateľa.

Všeobecne môžeme na základe vyššie uvedeného zhrnúť, že pri posúdení uplatnenia príslušnosti Českého trestného práva pri trestných činoch páchaných prostredníctvom šírenia protiprávneho obsahu na internete, vychádzame z posúdenia zodpovednosti za tzv. dištančné delikty.

Isté špecifikum v posúdení miestnej príslušnosti predstavuje tzv. **zásada aktívnej personality**, podľa ktorej sa pôsobnosť trestných zákonov vzťahuje aj na trestné činy spáchané občanmi Českej republiky, vrátane osôb s trvalým pobytom, v cudzine. Táto zásada vychádza z princípu štátnej zvrchovanosti, kedy štátna moc špecifikovala určitý okruh spoločensky škodlivých konaní, ktorého zákaz je pre spoločnosť tak dôležitý, že nie sú dovolené ani v zahraničí. Prakticky tak môže nastať situácia, kedy Český občan koná v zahraničí v súlade s tamojším právom ale jeho konanie je trestnoprávne relevantné podľa trestných zákonov v Českej republike. Druhé špecifikum v posúdení miestnej príslušnosti predstavuje tzv. **zásada pasívnej personality**, ktorá býva označovaná aj ako zásada ochrany občana. Táto zásada rozširuje pôsobnosť trestných zákonov na trestné činy, ktoré boli spáchané v zahraničí, cudzím štátnym príslušníkom a ktoré smerujú voči občanovi Českej republiky, za predpokladu, že je dané jednanie trestné podľa lokálnych trestných zákonov.[31]

1.3.2. Osobná príslušnosť

Druhú kategóriu predstavujú podmienky osobnej príslušnosti, ktoré stanovujú výnimky zo všeobecne zavedenej pôsobnosti trestného práva. Osoby vyňaté z pôsobnosti trestného práva sú buď z časti alebo úplne beztrestné, v takom prípade hovoríme o hmotnoprávnej imunite tzv. indemnite, kedy nie je možné vôbec stíhať určité konanie osoby, aj keď by ho bolo možné považovať za trestné. Od hmotnoprávnej imunity je nutné rozlišovať bezostyšnosť, ktorá spočíva

[30] PROVAZNÍK, J. § 4 [Zásada teritoriality]. In: ŠČERBA, F. a kol. *Trestní zákoník. 1. vydanie (2. aktualizácia)*. Praha: C. H. Beck, 2022, marg. č. 12. ISBN 978-80-7400-807-8.
[31] ŠÁMAL, P; NOVOTNÝ, O; GŘIVNA, T; HERCZEG, J; VANDUCHOVÁ, M et al. *Trestní právo hmotné*. 9., prepracované vydanie. Praha: Wolters Kluwer, 2022, 91 a 92 s. 1 ISBN 978-80-7598-764-8.

v nemožnosti stíhať určitú osobu z titulu výkonu jej funkcie a to za splnenia určitého predpokladu alebo až do konca výkonu tejto funkcie.[32]

Hmotne právnou indemnitou podľa článku 27 ods. 2 Ústavy Českej republiky[33] disponujú poslanci a senátori, ktorých nie je možné trestne stíhať za prejavy v Poslaneckej snemovni alebo Senáte alebo v ich orgánoch. Dané ustanovenie ale neplatí bez výnimky. Poslanci a senátori sú trestnoprávne zodpovední, ak ich prejav smeruje voči tretej osobe. To znamená, že ak by poslanec šíril protiprávny obsah z pléna poslaneckej snemovne napríklad prostredníctvom sociálnej siete, bolo by možné vždy dovodiť jeho trestnoprávnu zodpovednosť. V tejto súvislosti Európsky súd pre ľudské práva (ESĽP) rozhodol, že poslanecká imunita pre politické prejavy nemôže dopadať na verbálne útoky alebo iné prejavy v súkromných konfliktoch medzi osobou s poslaneckou imunitou a treťou stranou.[34] Podobne sa vyslovil aj Ústavný súd, ktorý vo svojom rozhodnutí k rozsahu poslaneckej imunity dospel k záveru, že poslanecká imunita náleží Parlamentu ako celku, a chráni ho ako debatné fórum medzi poslancami a senátormi. Imunita nie je určená na individuálnu slobodu prejavu alebo osobné výsady jednotlivých poslancov alebo senátorov. Prejav, ktorý je chránený imunitou, nesmie byť zameraný výhradne navonok, musí sa týkať účastníkov parlamentnej diskusie, ako sú iní poslanci, senátori alebo iné osoby, ktoré majú právo sa zúčastniť na jednaní komory alebo jej orgánov.[35]

Z uvedených rozhodnutí môžeme dovodiť, že v prípade šírenia protiprávneho obsahu poslancami alebo senátormi na internete je možné vyvodiť ich trestnoprávnu zodpovednosť podľa všeobecných kritérií, keďže už samotná podstata jeho šírenia prostredníctvom internetu smeruje voči dopredu neurčenému počtu subjektov mimo Poslaneckú snemovňu alebo Senát. Nad rámec uvedeného dodávame, že v prípade akýchkoľvek pochybností o vyňatí určitej osoby z pôsobnosti trestného práva rozhoduje spory Najvyšší súd.[36]

1.4. Internet v skutkových podstatách trestných činov

Trestný zákon síce nehovorí o internete ako takom, ale v rámci definícii a jednotlivých skutkových podstát trestných činov sa vysporadúva so špecifikami, ktoré táto technológia v praxi prináša. Trestný zákon problematiku páchania trestných činov v prostredí internetu reguluje z viacerých pohľadov. V prvom rade upravuje spôsob páchania trestných činov na internete, kedy

[33] Ústavný zákon č. 1/1993 Sb., Ústava Českej republiky. V ďalšej časti diplomovej práce len ako Ústava.
[34] Porov. rozsudok Európskeho súdu pre ľudské práva zo dňa 30. 1. 2003, 40877/98, vo veci *Cordova proti Taliansku*, č. 1, bod 62. Dostupné z: https://www.stradalex.com/nl/sl_src_publ_jur_int/document/echr_40877-98.
[35] Nález Ústavného súdu zo dňa 16. 6. 2015, sp. zn. I. ÚS 3018/14 – 1.
[36] Porov. § 10 ods. 2 trestného zákonníka.

trestný čin spáchaný prostredníctvom verejne prístupnej počítačovej siete považuje za verejne spáchaný trestný čin (§ 117 písm. a) trestného zákonníka).

Verejne prístupnú počítačovú sieť všeobecne judikatúra definuje ako funkčnú prepojenú sieť, ktorá bola vytvorená s cieľom vytvoriť informačný systém pracujúci so vzdialeným prístupom. Internet ako informačný a komunikačný systém, ktorý je prostriedkom na verejné šírenie informácií, bezpochyby naplňuje vyššie stanovené znaky a je preto zrejmé, že ho je možné považovať za počítačovú sieť, ktorá funguje ako prenosové médium umožňujúce využívanie určitých služieb, z ktorých najdôležitejšou je prenos informácií.[37] Na základe uvedeného môžeme konštatovať, že v prípade šírenia protiprávneho obsahu v prostredí internetu sa bude jednať o trestný čin spáchaný verejne. Pre splnenie kritéria verejnosti musí byť konaním dosiahnutá úroveň zrovnateľná so spáchaním trestného činu médiami ako tlač, film, rozhlas alebo televízia. To znamená, že tento znak nebude naplnený napríklad pri šírení pornografických diel elektronickou poštou medzi tzv. e-mailovými schránkami chránenými heslom. Judikatúra dospela k záveru, že naopak by bol znak verejnosti naplnený v prípade, kedy by došlo zo strany páchateľa k rozoslaniu protiprávneho obsahu na veľký počet e-mailových adries, ktorý by už naplnil znak verejnosti.[38]

Podľa rozhodnutia Ústavného súdu Českej republiky,[39] je pojem verejnej dostupnosti na internete potrebné posudzovať nielen v súvislosti s možnosťami používateľov internetu zobraziť konkrétny obsah, pokiaľ ide o ich prístupové práva, ale aj v kontexte ich schopnosti sa o tomto obsahu dozvedieť vôbec po prvý raz. Toto zahrňuje informácie získané z príspevkov na diskusných fórach a chatoch, obsahu webových stránok indexovaných vyhľadávacími službami alebo aj prostredníctvom vloženia obsahu na profil používateľa sociálnej siete na internete, ktorý následne môže byť zdieľaný s ďalšími používateľmi tejto siete. V uvedenom rozhodnutí Ústavný súd taktiež konštatoval, že samotné rozoslanie obsahu prostredníctvom súkromnej správy na sociálnej sieti znak verejnosti nenaplní a súdy by mali pri rozhodovaní o tomto znaku najskôr presne vyjasniť, aké funkcionality mal páchateľ k dispozícii, ako ich skutočne využil, a aký bol vplyv tohto využitia na rozsah trestnej činnosti.[40]

[37] Porov. rozhodnutie Najvyššieho súdu zo dňa 30. 1. 2013, sp. zn. Tpjn 300/2012.
[38] ŠÁMAL, P. § 117 [Veřejné spáchání trestného činu]. In: ŠÁMAL, P. a kol. *Trestní zákoník. 3. vydanie*. Praha: C. H. Beck, 2023, s. 1684, marg. č. 5. ISBN: 978-80-7400-893-1.
[39] V ďalších častiach diplomová práca Ústavný súd Českej republiky označuje tiež len ako Ústavný súd.
[40] Nález Ústavného súdu zo dňa 20. 8. 2013, sp. zn. I. ÚS 1428/13.

1.5. Definícia a rozvoj počítačovej kriminality v súvislosti so šírením obsahu

Rozvoj internetu so sebou priniesol nielen nové spôsoby možnosti páchania trestnej činnosti ale taktiež rozšíril možnosti páchania súčasných trestných činov, vrátane tých najzávažnejších, akými sú napríklad obchodovanie s ľuďmi, obchodovanie s drogami, nedovolené obchodovanie so zbraňami, podvody s finančnými prostriedkami a tak podobne. Počet obetí počítačovej kriminality sa približuje k 1 miliónu obetí denne a vo svojej podstate ide o výnosnejší druh kriminality ako napríklad kriminalita v oblasti predaja drog, marihuany, kokaínu a heroínu dohromady.[41]

Pojem počítačová kriminalita predstavuje súhrnný pojem, ktorý označuje typovo podobne trestné činy, ktoré vykazujú určité spoločné znaky. Počítačová kriminalita, tiež niekedy označovaná ako kybernetická kriminalita,[42] z anglického výrazu *cyber crime,* ktorý bol prvýkrát použitý v Spojených štátoch v 70. rokoch 20. storočia v dielach od D. B. Parker. Parker počítačovú kriminalitu chápal ako kriminalitu páchanú prostredníctvom počítačov alebo kriminalitu, ktorej predmetom útoku je počítač.[43] V súčasnosti definovanie pojmu počítačová kriminalita predstavuje pomerne náročnú úlohu a definícia od Parkera, tak už nedokáže zreteľne odrážať komplexnosť problematiky počítačovej kriminality. Všeobecne možno počítačovú kriminalitu definovať ako kriminalitu, ktorá prebieha prostredníctvom počítača, ako súhrnu hardvérového a softvérového vybavenia, vrátane dát v ňom obsiahnutých, alebo iba prostredníctvom niektorých jeho komponentov, prípadne väčšieho množstva počítačov operujúcich samostatne alebo prepojených do počítačovej siete, a to buď ako predmet trestnej činnosti alebo ako nástroj trestnej činnosti.[44]

Počiatky počítačovej kriminality možno datovať do obdobia 60. a 70. rokov minulého storočia, teda do obdobia kedy vznikajú prvé počítače a základy dnešného internetu. Je samozrejmé, že hrozby, ktoré predstavovali počítače a internet v danej dobe boli od dnešných hrozieb odlišné. Hardvér prvých počítačov zaberal celé miestnosti a ich cena bola v rádoch desiatok miliónov českých korún. Prístup k nim pre vysokú cenu a zložitosť používateľského rozhrania bol obmedzený na relatívne malý okruh technologických odborníkov. Tento obmedzený prístup mal za následok, že vyšetrovanie možnej trestnoprávnej zodpovednosti v oblasti počítačovej kriminality nepredstavovalo v tej dobe tak naliehavú výzvu, pretože páchateľom

[41] KLIMEK, L.; ZÁHORA, J. a HOLCR, K. 2016, op. cit., s. 19.
[42] V tomto kontexte je nutné dodať, že niektorí autori rozlišujú medzi pojmami počítačová kriminalita a kybernetická kriminalita, kedy kybernetickú kriminalitu chápu ako nástupcu počítačovej kriminality.
[43] VAN DER MERWE, D. P. (2000). *Computers and the law*. In: Barkley Law, 166 s. ISBN 0702150878. alebo porov. aj dielo Parker, D. B. *Fighting computer crime: A new framework for protecting information*. In John Wiley & Sons, 1998. ISBN 978-0471163787.
[44] SMEJKAL, V. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. s. 33. ISBN 978-80-7380-849-5.

počítačovej kriminality mohli byť len odborne zdatné osoby, ktoré mali zároveň prístup k počítačom.[45]

Prvá trestná činnosť v oblasti počítačovej kriminality predstavovala predovšetkým neoprávnené rozširovanie softvéru a poškodzovanie hardvéru počítačov. Prvý trestný čin v oblasti počítačovej kriminality v Československu je datovaný do 80. rokov dvadsiateho storočia, kedy jeden zo zamestnancov Úradu dôchodkového poistenia poškodil magnetom záznamy na magnetických páskach, ktoré slúžili na ukladanie dát poistencov. Vtedajšia právna úprava posudzovala daný trestný čin ako sabotáž, keďže pochopiteľne trestný zákon z roku 1961 neobsahoval úpravu trestných činov v oblasti počítačovej kriminality. V tom čase išlo o najčastejšie odhaľované trestné činy v tejto oblasti.[46] Kým v tom čase trestné činy v oblasti počítačovej kriminality boli pomerne ojedinele v dnešnej dobe je situácia úplne odlišná.

V počiatkoch používania počítačov bolo pre páchateľa veľmi zložité zdieľať protiprávny obsah, a kriminalita sa sústreďovala predovšetkým na fyzické poškodenie počítača alebo fyzickú krádež softvéru. Bezpochyby mala na túto problematiku vplyv aj rýchlosť internetu, kedy pri možnostiach danej doby, napríklad na počiatkoch masového využívania internetu, predstavovala jeho rýchlosť iba jednotky kilobajtov.

S postupom času a zvyšujúcou sa dostupnosťou zariadení, ktoré je možné pripojiť k internetu, došlo aj k značnému rozšíreniu možnosti páchania trestnej činnosti. Na túto skutočnosť reagovali aj zákonodarcovia, ktorí začali počítačovú kriminalitu postupne regulovať. Napríklad Európska únia počítačovú kriminalitu zaradila v rámci vytvoreného priestoru slobody, bezpečnosti a práva medzi tzv. európske trestné činy.[47] V rámci Európskej únie následne došlo k vytvoreniu európskeho centra boja proti počítačovej kriminalite. Európska únia chápe počítačovú kriminalitu ako trestnú činnosť, ktorá bola spáchaná online prostredníctvom počítačov a komunikačných sietí (napr. cez internet).[48]

Internetovú kriminalitu môžeme zaradiť ako jednu z foriem počítačovej kriminality. Pokiaľ vychádzame z definície od Smejkala, jedná sa o protiprávne konanie, ktoré je páchane prostredníctvom počítačov, konkrétne pomocou ich softvérového vybavenia - internetu. Šírenie

[45] Porov. napr. Článok na portále Artic Wolf s názvom *A Brief History of Cybercrime*, In Arcticwolf.com [online]. [cit. 2023-05-24]. Dostupné z https://arcticwolf.com/resources/blog/decade-of-cybercrime/.
[46] KLIMEK, L.; ZÁHORA, J. a HOLCR, K. 2016, op. cit., s. 18 - 19.
[47] Porov. čl. 83 zmluvy o fungovaní Európskej únie (Konsolidované znenie).
[48] Porov. dokument *Európske centrum boja proti počítačovej kriminalite na úrade Europol*. In Europa.eu [online]. [cit. 2023-05-24]. Dostupné z https://publications.europa.eu/resource/cellar/6d16d2d0-7561-4492-beef-048e64bed66a.0022.02/DOC_1.

protiprávneho obsahu v jeho prostredí, tak predstavuje jednu z foriem počítačovej kriminality, konkrétne ako podmnožina internetovej kriminality.

1.6. Počítačové trestné činy a kybernetické trestné činy

Internet nie len rozšíril spôsoby páchania bežnej trestnej činnosti do kybernetického priestoru, ale zároveň so sebou priniesol aj nové hrozby, ktoré môžeme označiť ako počítačové alebo kybernetické trestné činy. Počítačové trestné činy predstavujú súbor trestných činov, ktoré sa týkajú počítačov alebo počítačových sietí. Ako už bolo uvedené, do podmnožiny počítačovej kriminality môžeme zaradiť aj protiprávne šírenie obsahu. V rámci šírenia obsahu dochádza k rozširovaniu dátových súborov, elektronických správ alebo iného obsahu, ktorý samotný nemusí byť protiprávny, ale jeho úpravou zo strany páchateľa, alebo spôsobom šírenia sa protiprávnym stáva. Medzi spôsoby páchania počítačovej kriminality patria napríklad phishing, ransomvér, útoky na webové stránky a sociálne siete, krádeže identity a úniky dát. Trestný zákonník neupravuje osobitne trestnosť takýchto konaní, ale zodpovednosť za nich je možné dovodiť na základe iných skutkových podstát. Uvedené konania by tak mohli naplniť znaky skutkovej podstaty trestného činu podvodu podľa § 209 trestného zákonníka, vydierania v zmysle § 175 trestného zákonníka alebo trestný čin neoprávneného prístupu do počítačového systému a neoprávnený zásah do počítačového systému alebo nosiča informácií podľa § 230 trestného zákonníku.

Phishing predstavuje formu kybernetického útoku, pri ktorom útočník použije podvodné praktiky na to, aby presvedčil potenciálne obete, aby poskytli svoje citlivé informácie, akými sú napríklad prihlasovacie údaje alebo údaje o bankových účtoch či kreditných kartách. Tento druh útoku v sebe spojuje sociálne inžinierstvo a podvodné praktiky. Phishingový útok je častokrát páchaný prostredníctvom šírenia nevyžiadanej elektronickej pošty, prístupom na škodlivé webové stránky, ktoré sa tvária, že sú prevádzkované legitímnym správcom, ako je banka alebo sociálna sieť. Útočníci pri phishingových útokoch častokrát využívajú rôzne zastrašovacie a nátlakové taktiky, aby prinútili príjemcov k čo najrýchlejšej odpovedi, a tým zároveň obmedzili čas na adekvátnu reakciu a obozretnosť. V rámci phishingu rozlišujeme podskupinu *spear phishing*, ktorá predstavuje sofistikovanejšiu formu phishingu. Útočníci sa zameriavajú na konkrétne organizácie alebo jednotlivcov s cieľom získať prístup k dôverným informáciám. Podobne ako pri štandardnom phishingu sa aj obsah spear phishingu tvári ako dôveryhodný. Rozdiel predstavuje

predovšetkým to, že škodlivý obsah je prispôsobený konkrétnej obeti, napríklad tým, že sa útočník predstaví pod falošnou identitou ako osoba pracujúca v rovnakej spoločnosti.[49]

Ransomware je formou malvéru, škodlivého softvéru, ktorý infikuje počítačové systémy, obmedzuje prístup k nim a požaduje výkupné na obnovenie úplného prístupu. Útočníci pri ransomwarevých útokoch využívajú rôzne praktiky, kedy po napadnutí systému jeho obsah zašifrujú alebo zablokujú prístup k celému systému. Po infikácii ransomwarom obvykle používateľ, ktorý sa stal obeťou útoku, dostane požiadavku na zaplatenie výkupného (pozn. z angl. *ransom* čo znamená výkupné). Ransomware sa šíri podobnými cestami ako iný malvér, vrátane phishingových e-mailov, a častokrát v praxi dochádza ku kombinácii oboch útokov, kedy útočník najprv získa prístup k obsahu alebo systému, a následne tento obsah zneprístupní.

Prevencia pred malvérom, škodlivým softvérom, zahŕňa dodržiavanie bežných postupov bezpečnosti na internete[50] a pravidlá tzv. netikety.[51] Netiketa predstavuje spojenie slov „net“ a „etiketa“, ktoré označuje súbor pravidiel pre správanie používateľov v online prostredí. Ide o etický kódex, ktorý upravuje používanie, spôsoby komunikácie a interakcie na internete. Netiketa zahŕňa pravidlá týkajúce sa sebaprezentácie, správania v online diskusiách, rešpektovania súkromia iných používateľov a všeobecného etického správania sa na sociálnych médiách, fórach, e-mailoch a iných online platformách.[52]

Sociálne inžinierstvo zahŕňa súhrn metód, ktoré si kladú za cieľ nelegitímne presvedčiť inú osobu, aby odhalila špecifické informácie alebo vykonala určitý úkon. V oblasti IT sa tieto techniky rozvinuli s rozvojom informačných a komunikačných technológií. Sociálne inžinierstvo môžeme pozorovať v dvoch hlavných formách, a to buď prostredníctvom psychologickej manipulácie s cieľom získať prístup k IT systému, alebo využitím IT technológií ako podpory pre manipuláciu mimo IT sféry. Táto forma kybernetickej hrozby stále narastá, pričom väčšina kybernetických útokov v sebe dnes zahŕňa taktiež nejakú formu sociálneho inžinierstva. Medzi najčastejšie techniky patrí *pretexting*, *baiting*, *quid pro quo* a *tailgating*, a tvorí kľúčovú súčasť phishingových útokov. Aby sme odvrátili tieto útoky, je dôležité mať účinné procesy identifikácie a autentifikácie, politiky a školenia.

---

[49] Definícia pojmov phishing a spare phishing od Európskej agentúry pre bezpečnosť sietí a informácií (ENISA). In Enisa.europa.eu [online]. [cit. 2023-12-10]. Dostupné z: https://www.enisa.europa.eu/topics/incident-response/glossary/phishing-spear-phishing.

[50] Pravidlá bezpečnosti na internete od VÚB Banky. In Vub.sk [online]. [cit. 2023-12-10]. Dostupné z: https://vub.sk/ludia/jednovubky/12-tipov-ako-zvysit-bezpecnost-na-internete.html.

[51] Definícia pojmu ransomvér od Európskej agentúry pre bezpečnosť sietí a informácií (ENISA), In Enisa.europa.eu [online]. [cit. 2023-12-10]. Dostupné z: https://www.enisa.europa.eu/topics/incident-response/glossary/ransomware.

[52] Pravidlá netikety od technologickej spoločnosti Avast. In Avast.com [online]. [cit. 2023-12-10]. Dostupné z: https://www.avast.com/c-netiquette.

Pretexting predstavuje metódu sociálneho inžinierstva, pri ktorej útočník využije falošnú zámienku s cieľom získať dôveru obete, a tým od nej získa citlivé informácie. Príkladom pretextingu môže byť pre predstavu situácia, v ktorej útočník predstiera, že je IT podpora a tým získa prístupové údaje obete. *Baiting* je taktikou sociálneho inžinierstva, pri ktorej sa útočník snaží zlákať obeť na konanie určitej činnosti, ktorá slúži jeho nelegitímnym zámerom, napríklad otváraním škodlivého odkazu si obeť do počítača stiahne škodlivý malvér. *Quid pro quo* je technika sociálneho inžinierstva, kde útočník ponúka obeti nejaký prospech alebo výhodu výmenou za získanie želaných informácií alebo úkonov. Typickým príkladom techniky quid pro quo je činnosť falošných výskumných dotazníkov, ktoré za odmenu obeť vyplní a tým poskytne útočníkovy citlivé údaje. *Tailgating* (prisunutie) spočíva v neoprávnenom vstupovaní do priestranstiev, ktorú chráni bezpečnostné opatrenie, napríklad prechodom cez dvere za legitímne vstupujúcim, s cieľom dostať sa do vnútra a získať prístup. [53] V prípade internetu by sa o tailgating mohlo jednať v prípade, ak by útočník využil prístup z odomknutého počítača tretej osoby.

Vďaka rozvoju internetu a mobilnej komunikácie sa nepretržite spracováva veľké množstvo dát a informácií, vrátane osobných údajov, ktorých neoprávnené šírenie by mohlo predstavovať zásah do súkromnej sféry dotknutých osôb.[54] Za neoprávnené zverejnenie osobných údajov považujeme nezákonné sprístupnenie osobných údajov skupine vopred individuálne neidentifikovaných osôb. Podľa prieskumu krádeží identít od americkej rankingovej spoločnosti US News & World Report sa každý tretí respondent stal obeťou porušenia údajov (angl. *data breach*).[55] Jedná sa napríklad o situáciu, v ktorej páchateľ zverejní osobné údaje dotknutej osoby na webovej stránke, sociálnej sieti alebo inde na internete. K porušeniu zabezpečenia osobných údajov môže dôjsť na základe hackerského útoku, nedbalostným konaním alebo úmyselným konaním páchateľa. Obeťou takýchto útokov sa častokrát stávajú verejné inštitúcie, ktoré nemajú vždy najlepšie technologické zabezpečenie a spracúvajú obrovské množstvo osobných údajov.[56]

Krádež identity alebo podvod s identitou označuje konanie útočníka, ktorý neoprávnene zneužije osobné údaje obete v online prostredí, s úmyslom získať pre seba isté finančné alebo iné

[53] Definícia pojmov vychádza z definície od Európskej agentúry pre bezpečnosť sietí a informácií (ENISA), *What is "Social Engineering"*? In Enisa.europa.eu [online]. [cit. 2023-12-10]. Dostupné z: https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering.
[54] Nález Ústavného súdu z 22. marca 2011, sp. zn. Pl. ÚS 24/10.
[55] Prieskum americkej rankingovej agentúry U.S. News & World *Report Identity Theft Survey 2023*, In Usnews.com [online]. [cit. 2023-12-09]. Dostupné z: https://www.usnews.com/360-reviews/privacy/identity-theft-protection/identity-theft-fraud-survey.
[56] Tlačová správa k rozhodnutiu Úradu na ochranu osobných údajov sp. zn. UOOU-01752/21. In Uoou.gov.cz [online]. [cit. 2023-12-09]. Dostupné: https://uoou.gov.cz/cinnost/ochrana-osobnich-udaju/ukoncene-kontroly/kontroly-za-rok-2022/kontrolni-cinnost-v-oblasti-ochrany-osobnich-udaju-2022/soukrome-zdravotnicke-zarizeni.

výhody. Podľa výročnej bezpečnostnej správy Európskej agentúry pre bezpečnosť sietí a informácií bolo len v roku 2019 preukázateľne zistených viac ako 900 medzinárodných prípadov krádeže identity alebo súvisiacich zločinov.[57] Medzi najvýznamnejšie incidenty za uplynulé roky patrili:

- v júli 2023 HCA Healthcare oznámila, že došlo ku krádeži osobných údajov približne 11 miliónov pacientov;[58]
- v auguste 2023 došlo k porušeniu údajov v spoločnosti Tesla, pri ktorom došlo k zverejneniu údajov približne 75 000 zamestnancov, a to aj vrátane čísel sociálneho poistenia;[59]
- zverejnenie osobných údajov takmer 106 miliónov amerických a kanadských zákazníkov bánk Capital One po incidente v marci 2019;
- zverejnenie 170 miliónov používateľských mien a hesiel používaných digitálnym herným vývojárom Zynga v septembri 2019;
- odcudzenie 20 miliónov účtov z britskej audio streamovacej služby Mixcloud;
- odcudzenie údajov 600 000 vodičov a 57 miliónov používateľov aplikácie Uber v novembri 2019; a
- krádež 9 miliónov osobných údajov od zákazníkov aerolinky EasyJet vrátane občianskych preukazov a kreditných kariet.[60]

Kybernetická kriminalita sa s rozvojom informačných technológii a zvyšovaním ich dostupnosti stala dokonca aj predmetom protiprávnej podnikateľskej činnosti. Tento fenomén označujeme termínom **kybernetická kriminalita ako služba** (angl. *cybercrime as a service*), ktorá predstavuje model organizovanej kriminality, v ktorom páchatelia ponúkajú protiprávne služby iným používateľom. Používateľ si tak na internete za finančné prostriedky vie zabezpečiť vykonanie istého kybernetického útoku. Typicky sa bude jednať o útoky malvérom, distribuované odmietnutie služby (tzv. DDoS útok),[61] útok pomocou ransomwaru, phishingový útok a sociálne

[57] Informácie vychádzajú z výročnej správy *Identity theft report* od Európskej agentúry pre bezpečnosť sietí a informácií (ENISA), 2020, In Enisa.europa.eu [online]. [cit. 2023-12-09]. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-identity-theft/@@download/fullReport.
[58] Porov. napr. článok *HCA Healthcare says hackers stole data on 11 million patients - CBS News*, dostupný na: https://www.cbsnews.com/news/hca-healthcare-data-breach-hack-11-million-patients-affected/.
[59] Porov. článok CONSOLE, R. *Tesla Notifies Over 75k Current and Former Employees of Recent Data Breach*, In Jduspra.com [online]. [cit. 2023-06-04]. Dostupné z: https://www.jdsupra.com/legalnews/tesla-notifies-over-75k-current-and-4275111/.
[60] *Identity theft report.* 2020, op. cit.
[61] Distribuovaným odmietnutím služby (DDoS) sa označuje kybernetický útok, pri ktorom užívatelia systému alebo služby k nej nemôžu získať prístup. Tento stav môže byť dosiahnutý vyčerpaním služby alebo preťažením časti infraštruktúry siete. Porov. napr. správu ENISA *Distributed denial of service,* IN Enisa.europa.eu [online]. [cit. 2023-

inžinierstvo.[62] Tento spôsob kriminality je častokrát páchaný prostredníctvom prepojených sietí počítačov, ktoré pracujú ako jeden. Takúto sieť označujeme ako botnet. Termín botnet vznikol ako skratka z anglického výrazu robot network.[63]

2. Trestnoprávna zodpovednosť šíriteľa protiprávneho obsahu

Po vyjasnení otázky pôsobnosti právnych noriem v prostredí internetu a objasnení jednotlivých aspektov počítačovej kriminality, prechádzame k samotnej podstate problematiky trestnoprávnej zodpovednosti za publikovanie a šírenie protiprávneho obsahu na internete. Na základe subjektov, ktoré participujú na šírení protiprávneho obsahu môžeme rozlišovať tri kategórie. V prvom rade rozlišujeme zodpovednosť samotného pôvodcu obsahu, ktorý vlastným konaním šíri protiprávny obsah, v druhom rade rozlišujeme zodpovednosť za publikovanie a šírenie cudzieho protiprávneho obsahu v rámci poskytovania digitálnych služieb, kedy hovoríme o zodpovednosti poskytovateľov služieb informačných spoločností. V neposlednom rade môžeme v súčasnosti vidieť nástup nových technológii generatívnej umelej inteligencie, ktoré dokáže protiprávny obsah vytvárať a šíriť ho ďalej v prostredí internetu.

Diplomová práca najprv stručne vo všeobecnej rovine rozoberá úpravu trestnoprávnej zodpovednosti v právnom poriadku Českej republiky. Táto analýza čitateľovi poskytuje pohľad do širších legislatívnych súvislostí a rámca, v ktorom sa pohybuje trestnoprávna zodpovednosť za konanie na internete. V prvom rade je nevyhnutné pochopiť, akým spôsobom je právny poriadok nastavený pri vyvodzovaní trestnoprávnej zodpovednosti v digitálnom prostredí, a aké nástroje a mechanizmy sú orgánom činným v trestnom konaní k dispozícii pri postihovaní tých, ktorí porušujú právne normy prostredníctvom svojej online činnosti.

Cieľom tejto časti diplomovej práce je poskytnúť čitateľovi komplexný pohľad na právne aspekty trestnoprávnej zodpovednosti v prostredí internetu s dôrazom na trestnosť konania v súvislosti s protiprávnym šírením pornografie a sexualizovaného obsahu, ktorú autor diplomovej práce považuje za najlepší prostriedok pre modelové poukázanie na problematiku vynútiteľnosti trestnoprávnej zodpovednosti na internete.

12-09]. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service/at_download/fullReport.

[62] CHEBAC, A. *What Is Cybercrime-as-a-Service (CaaS)?*, In: Heimdal portal [online]. [cit. 2023-12-09]. Dostupné z: https://heimdalsecurity.com/blog/what-is-cybercrime-as-a-service-caas/.

[63] Porov. informačné stránky EUROPOLU k problematike kybernetickej kriminality. *Cybercrime*. In Europol.europa.eu [online]. [cit. 2023-12-21]. Dostupné z: https://www.europol.europa.eu/crime-areas/cybercrime.

2.1. Vymedzenie trestnoprávnej zodpovednosti

Trestné právo je odvetvím práva verejného. Jeho primárnym cieľom je ochrana ústavne garantovaných základných práv a slobôd, ústavného zriadenia a bezpečnosti Českej republiky. V týchto súvislostiach je nutné dodať, že trestné právo si nekladie za cieľ absolútnu ochranu všetkých ústavne zakotvených práv a slobôd, ale len tých, na ktorých ochranu nepostačuje ochrana zaručená prostriedkami iných právnych odvetví, predovšetkým práva občianskeho, správneho, rodinného a pod. Trestnoprávna ochrana býva z tohto dôvodu označovaná ako prostriedok poslednej inštancie (lat. *ultima ratio*). Trestné právo vymedzuje okruh spoločensky škodlivého správania sa, ktoré označuje za trestné, upravuje podmienky trestnej zodpovednosti a stanovuje zvláštne trestné sankcie za ňu.[64]

Pojem trestnoprávnej zodpovednosti zaradzujeme do širšieho kontextu právnej zodpovednosti, ktorá predstavuje zvláštnu formu právneho vzťahu, pri ktorom dochádza na základe porušenia primárnej právnej povinnosti ku vzniku novej (sekundárnej) právnej povinnosti – sankcie. Právna teória rozlišuje právnu zodpovednosť v súkromnoprávnej oblasti a právnu zodpovednosť v oblasti práva verejného. V súkromnoprávnej oblasti vzniká právna zodpovednosť medzi delikventom a poškodeným na základe porušenia noriem súkromného práva. V prípade verejnoprávnej zodpovednosti hovoríme tradične o zodpovednosti trestnej, správnej a disciplinárnej.[65] Trestnoprávna zodpovednosť býva v právnej teórii chápaná, ako zodpovednosť za spáchaný trestný čin, respektíve previnenie.[66] Inými slovami zodpovednosť páchateľa trestného činu niesť nepriaznivé dôsledky svojho spoločensky škodlivého konania, v súvislosti s porušením noriem trestného práva.[67]

Páchateľom trestného činu je aj ten, kto k spáchaniu trestného činu použil inú osobu ktorá nie je trestnoprávne zodpovedná za splnenia podmienok v § 22 ods. 2 trestného zákonníka, teda osobu ktorá z ohľadom na nedostatočný vek, nepríčetnosť, omyl alebo preto že konala pod vplyvom okolností, ktoré vylučujú jej trestnoprávnu zodpovednosť.[68] Rovnako sa trestnoprávna zodpovednosť uplatní aj na osoby, ktoré sa na spáchaní trestného činu zúčastnili, teda konkrétne spáchanie trestného činu zosnovali alebo riadili (organizátor), vzbudili v inom pohnútku k spáchaniu trestného činu (návodca) alebo umožnili a uľahčili inému spáchanie trestného činu

[64] ŠÁMAL, P; NOVOTNÝ, O; GŘIVNA, T; HERCZEG, J; VANDUCHOVÁ, M et al., 2022, op. cit., 35 a 36 s.
[65] GERLOCH, A. *Teorie práva. 7. aktualizované vydanie*. Plzeň: Aleš Čeněk, 2017, 175 s. ISBN 978-80-7380-652-1.
[66] PROVAZNÍK, J. § 12 [Zásada zákonnosti a zásada subsidiarity trestní represe]. In: ŠČERBA, F. a kol., 2022, op. cit., marg. č. 89.
[67] JELÍNEK, J. Pojem trestního práva, jeho funkce, zásady trestního práva. In: JELÍNEK, Jiří a kolektiv. Trestní právo hmotné: obecná část, zvláštní část. 6. aktualizované a doplnené vydanie. Praha: Leges, 2017, 20 s. ISBN 978-80-7502-236-3.
[68] Porov. § 22 ods. 2 trestného zákonníka.

(pomocník). K trestnoprávnej zodpovednosti účastníkov sa obdobne uplatní právna úprava trestnoprávnej zodpovednosti páchateľa.[69]

V tomto kontexte je potrebné dodať že zásada zodpovednosti za spáchaný trestný čin býva spájaná so zásadou individuálnej trestnej zodpovednosti a zásadou zodpovednosti za zavinenie (lat. *nullum crimen sine culpa*). Individualita trestnej zodpovednosti spočíva v premise, že každá fyzická a právnická osoba nesie zodpovednosť za svoje protiprávne konanie, a preto by mal byť trest, ktorý za daný trestný čin obdrží, osobnou ujmou daného páchateľa. Trestom a ujmou s ním spojenou by nemali byť postihnuté osoby, ktoré sa na danej trestnej činnosti nepodieľali. Zásada zodpovednosti za zavinenie je vyjadrením princípu tzv. subjektívnej zodpovednosti.

Podľa českého trestného práva sa pre určenie zodpovednosti páchateľa vyžaduje zavinenie vo forme úmyslu alebo nedbanlivosti. Všeobecne je možné konštatovať, že páchateľovi trestného činu nie je možné pričítať takú skutočnosť, na ktorú by sa nevzťahovalo jeho zavinenie, a to ani vo forme nedbanlivosti. Zavinenie právnických osôb sa posudzuje v závislosti od zavinenia fyzickej osoby, ktorej konanie je právnickej osobe z titulu funkcie alebo postavenia v nej pričítateľné.[70]

Trestnoprávnou zodpovednosťou chápeme povinnosť páchateľa trestného činu niesť nepriaznivé dôsledky svojho konania vo forme trestnoprávnej sankcie. Toto pojatie trestnej zodpovednosti býva označované ako sankčné. Trestnoprávna zodpovednosť páchateľovi vzniká konaním, ktorým porušil alebo ohrozil záujmy chránené trestným zákonom. Obsahom samotnej trestnoprávnej zodpovednosti páchateľa je povinnosť voči štátu, podrobiť sa právnym dôsledkom svojho protiprávneho konania.[71]

Samotným základom trestnoprávnej zodpovednosti podľa českého práva je teda spáchaný trestný čin. Trestný čin je definovaný v § 13 ods. 1 trestného zákonníka ako čin, ktorý je trestný podľa trestného zákona a ktorý vykazuje znaky uvedené v tomto zákone. Trestné činy spáchané mladistvými označuje trestný zákon ako previnenie (česky *provinění*). Trestný zákonník definíciu trestného činu ešte ďalej rozširuje o formy konania páchateľa, ktoré spočívajú v príprave trestného činu (§ 20 trestného zákonníku), pokusu (§ 21 trestného zákonníku) a organizátorstva, návodu a pomoci (§ 24 ods. 1 trestného zákonníku). Trestné činy sa podľa stupňa spoločenskej škodlivosti a formy zavinenia páchateľa ďalej vnútorne delia na zločiny a prečiny. Prečinom sú označované trestné činy spáchané z nedbanlivosti a úmyselné trestné činy, pre ktoré trestný zákonník stanovuje

[69] Porov. § 24 trestného zákonníka.
[70] ŠÁMAL, P; NOVOTNÝ, O; GŘIVNA, T; HERCZEG, J; VANDUCHOVÁ, M et al. 2022, op. cit., 49 a 50 s.
[71] JELÍNEK, J.; HASCH, K.; HERANOVÁ, S.; TEJNSKÁ, K.; KOPEČNÝ, Z. et al. *Trestní právo hmotné: obecná část, zvláštní část. 8. aktualizované a doplnené vydanie*. Praha: Leges, 2022. ISBN 978-80-7502-576-0.

trest odňatia slobody s maximálnou sadzbou do piatich rokov. Ako zločiny označujeme všetky trestné činy, ktoré nie sú považované za prečiny podľa trestného zákona. Trestný zákonník navyše doplňuje pojem zvlášť závažné zločiny, ktorými označuje spoločensky najškodlivejšie trestné činy, ktoré boli spáchané úmyselne a zároveň za ktoré trestný zákonník stanovuje trest minimálne desaťročného odňatia slobody.[72]

Ústavný súd v svojej judikatúre k problematike zodpovednosti za zavinenie navyše dospel k záveru, že pravidlá liberálneho demokratického právneho štátu si vyžadujú, aby bolo zavinenie páchateľa vyhodnotené len v súvislosti s takým konkrétnym konaním, ktoré mohol páchateľ v čase jeho vykonávania oprávnene považovať za trestné, prihliadajúc na obsah vtedy platného trestného zákona.[73] Tento záver Ústavného súdu je obzvlášť dôležitý v kontexte trestnoprávnej zodpovednosti za šírenie obsahu v prostredí internetu, v ktorom pre jeho špecifickosť a pocit anonymity častokrát chýba konkrétne uvedomenie si trestnosti konania páchateľa.[74] V tomto ohľade hovoríme o zásade zákonnosti a subsidiarity trestnej represie, ktoré predstavujú základné princípy trestnoprávnej zodpovednosti. Zásada zákonnosti vyjadruje predpoklad v demokratickej spoločnosti, že iba trestný zákon môže určiť okruh spoločensky škodlivých konaní, ktoré je možné sankcionovať podľa trestného práva. Zásada subsidiarity trestnej represie zase zavádza záruku, že konanie, ktoré je síce označené ako trestné, je naozaj spoločensky škodlivé a nie je možné vyvodiť zodpovednosť za neho prostredníctvom iných právnych inštitútov.

2.2. Zásada zákonnosti a zásada subsidiarity trestnej represie

Koncepčne sú zásady zákonnosti a subsidiarity trestnej represie upravené v článku 39 Listiny[75] a § 12 trestného zákonníka. Zásady zákonnosti a subsidiarity tvoria základné piliere trestného práva, ktoré stanovujú, za akých podmienok je možné pristúpiť k jeho aplikácii. Prvá z týchto zásad, a to zásada zákonnosti, je jednou z kľúčových zásad trestného práva v demokratickom a právnom štáte.[76]

Zásada zákonnosti vyjadruje predpoklad, že iba samotný trestní zákon vymedzuje ktoré konanie je možné označiť za trestný čin a určuje sankcie, ktoré možno udeliť za jeho spáchanie, a to buď v podobe trestu alebo ochranného opatrenia (§ 12 ods. 1 trestného zákonníka). Trestný

[72] Porov. § 14 trestného zákonníka.
[73] Záver vychádza z nálezu Ústavné súdu - senát zo dňa 25.11.2003, sp. zn. I. ÚS 558/01.
[74] Predmetom tejto diplomovej práce je zhodnotiť mieru, v akej sa dá súčasná právna úprava aplikovať na nastupujúce trendy v počítačovej kriminalite, predovšetkým zo zameraním na šírenie protiprávneho obsahu. Diplomová práca sa tejto otázke venuje v ďalších častiach kde sa zoberá trestnou zodpovednosťou za jednotlivé trestné činy.
[75] Ústavný zákon č. 295/2021 Sb., ktorým sa mení a dopĺňa Listina základných práv a slobôd v znení ústavného zákona č. 162/1998 Sb. V texte diplomovej práce ďalej ako Listina.
[76] ŠÁMAL, P. § 12 [Zásada zákonnosti a zásada subsidiarity trestní represe]. 2023, op. cit., s. 187, marg. č. 1.

zákonník nepozná autonómny výklad nezákonnosti osobitne na účely trestného práva. Preto sa nezákonnosť v zmysle § 13 ods. 1 trestného zákonníka musí posudzovať vo svetle celého právneho poriadku.[77] Protiprávnosť nie je teda možné posudzovať len ako rozpor s normami trestného práva ale pri posúdení je nutné brať do úvahy aj hľadiská iných právnych odvetví, vrátane práva súkromného.

Zásada subsidiarity trestnej represie vyjadruje myšlienku, že trestné právo predstavuje najprísnejší prostriedok ochrany spoločnosti, ktorý má štátna moc k dispozícii. Všeobecne platí, že každý protiprávny čin, ktorý spĺňa všetky znaky uvedené v trestnom zákonníku, je považovaný za trestný čin. Avšak tento záver je v prípade menej závažných trestných činov korigovaný práve použitím zásady subsidiarity trestnej represie (§ 12 ods. 2 trestného zákonníka). Táto zásada stanovuje, že trestná zodpovednosť páchateľa a trestnoprávne dôsledky s ňou spojené možno uplatňovať len v prípadoch, ktoré majú spoločensky škodlivé dôsledky, a v ktorých nie je postačujúce uplatnenie zodpovednosti podľa iného právneho predpisu. To znamená, že kvalifikáciu určitého jednania ako trestného činu je potrebné zvažovať až ako prostriedok *ultima ratio*, teda prostriedok ktorého využitie by malo nastať len v krajných prípadoch, ktorých ochrana má význam predovšetkým pre ochranu celej spoločnosti aj jej základných hodnôt. Trestné právo nemá nahrádzať prostriedky práva súkromného ani nemá poskytovať ochranu súkromnoprávnym vzťahom, ktorých ochrana závisí na individuálnej aktivite jednotlivca. Ústavný súd k uvedenému zdôraznil, že v rámci fungovania právneho štátu je neprijateľné, aby prostriedky trestného práva slúžili na zabezpečenie subjektívnych práv súkromnoprávnej povahy, ak nebudú splnené všetky podmienky pre vznik trestnoprávnej zodpovednosti, alebo ak tieto podmienky nie sú plne a nepopierateľne preukázané.[78]

Je dôležité poznamenať, že použitie tohto materiálneho korektívu spočívajúceho v aplikácii zásady subsidiarity trestnej represie vyplýva z faktu, že ide o zásadu a nie konkrétnu právnu normu. Preto ju súdy musia uplatňovať nepriamo, prostredníctvom konkrétnych právnych inštitútov alebo jednotlivých noriem trestného práva.[79] Trestní zákonník týmto spôsobom rieši napríklad problém tzv. bagateľných priestupkov, ktoré nepredstavujú dostatočnú spoločenskú škodlivosť a preto by nemali byť ich páchatelia sankcionovaný normami trestného práva. Použitie zásady subsidiarity trestnej represie, teda bráni tomu, aby spoločensky nedostatočne škodlivé konanie, ktoré síce

[77] PROVAZNÍK, Jan. § 13 [Trestný čin]. In: ŠČERBA, F. a kol. 2022 , op. cit., marg. č. 15.
[78] Porov. napríklad nález Ústavný súdu - senát zo dňa 23.03.2004, sp. zn. I. ÚS 4/04.
[79] Stanovisko Najvyššieho súdu zo dňa 30. januára 2013, sp. zn. Tpjn 301/2012.

naplňuje formálne zákonné znaky niektorej zo skutkových podstát trestného činu bolo považované za trestný čin.[80]

Nie každé šírenie protiprávneho obsahu nevyvoláva automaticky trestnoprávnu zodpovednosť páchateľa. Orgány činné v trestnom konaní tak budú musieť v rámci trestného konania posúdiť každý jednotlivý prípad zvlášť, a to s ohľadom na naplnenie skutkovej podstaty daného trestného činu a zvážiť, či konanie páchateľa je dostatočne spoločensky škodlivé, aby nepostačovalo vyvodenie zodpovednosti podľa iného právneho predpisu. Orgány činné v trestnom konaní a v poslednej inštancii príslušné súdy by mali konkrétne v každej fáze trestného konania starostlivo posúdiť, či je v danom prípade potrebné pristupovať k vyvodeniu trestnoprávnej zodpovednosti. Zváženie potreby postihnutia určitého protiprávneho konania ako trestného je pritom kľúčové. Toto posúdenie by malo byť v prípade súdneho konania dôsledne zahrnuté do odôvodnenia rozhodnutia týkajúceho sa viny za trestný čin. V opačnom prípade hrozí porušenie práva na spravodlivý proces podľa článku 36 ods. 1 Listiny, a to z dôvodu nedostatočnej kvality rozhodnutia, ktorým je daná osoba označená za vinnú za trestný čin. Táto požiadavka platí predovšetkým v prípadoch, v ktorých je v trestnom konaní stíhané konanie páchateľa, ktoré má základ v súkromnom práve.[81]

V tejto súvislosti judikatúra Ústavného súdu konštante zdôrazňuje, že cieľom trestného práva nie je nahradiť ochranu práv a záujmov jednotlivca v oblasti súkromnoprávnych vzťahov ale je na aktivite jednotlivca, aby bránil svoje práva, a nie je prijateľné, aby orgány činné v trestom konaní aktívne prevzali túto úlohu. Hlavným cieľom trestného konania je najmä ochrana hodnôt celej spoločnosti, a nie priamo konkrétnych subjektívnych práv jednotlivca v rámci súkromnoprávnej oblasti. Nie je preto akceptovateľné, aby prostriedky trestného konania slúžili na zabezpečenie subjektívnych práv súkromnoprávnej povahy, pokiaľ nebudú splnené všetky predpoklady naplnenia trestnoprávnej zodpovednosti.[82]

2.3. Protiprávny obsah v prostredí internetu

Pre ďalšiu analýzu trestnoprávnej zodpovednosti za šírenie protiprávneho obsahu je nevyhnutné definovať samotný pojem protiprávny obsah. Platná a účinná právna úprava v súčasnosti nedefinuje pojem protiprávny obsah. Protiprávny obsah môžeme definovať ako obsah, ktorý nie je v súlade s právnym poriadkom ako celkom. Nemusí sa teda jednať len o obsah, ktorý porušuje normy trestného práva.

[80] ŠÁMAL, P. § 13 [Trestný čin]. In: ŠÁMAL, P. a kol. 2023, op. cit., s. 235, marg. č. 7.
[81] Porov. uznesenie Najvyššieho súdu zo dňa 13.12.2016, sp. zn. 6 Tdo 1638/2016.
[82] Napr. nález Ústavného súdu - senát zo dňa 23.03.2004, sp. zn. I. ÚS 4/04.

Protiprávny obsah môžeme ďalej rozčleniť na (i) **obsah, ktorý je protiprávny sám osebe**, napríklad fotografia zobrazujúca sexuálny styk s dieťaťom, nezákonné nenávistné prejavy alebo teroristický obsah alebo (ii.) **obsah, ktorý je vo svojej podstate v súlade s právom ale vo spojitosti s konaním páchateľa, je možné ho označiť za protiprávny**, ako príklad môžeme uviesť protiprávne rozširovanie diela chráneného autorským právom, šírenie súkromných snímok bez súhlasu oprávnenej osoby alebo prípady online prenasledovania.

Uvedená kategorizácia vychádza z prijatého nariadenia Európskej únie o digitálnych službách, ktoré termín nezákonný obsah definuje ako „*akúkoľvek informáciu, ktorá sama osebe alebo tým, že odkazuje na nejakú činnosť vrátane predaja výrobkov alebo poskytovania služieb, nie je v súlade s právnymi predpismi Únie alebo niektorého členského štátu, a to bez ohľadu na presný predmet alebo povahu týchto právnych predpisov*“.[83] Diplomová práca tento pojem bližšie rozoberá v časti 3.3.1. *s názvom* ***Nezákonný obsah***.

2.4. Vznik trestnoprávnej zodpovednosti za šírenie protiprávneho obsahu na internete

Základom trestnoprávnej zodpovednosti je konanie páchateľa, ktoré napĺňa znaky konkrétneho trestného činu. V tomto ohľade pre uplatnenie trestnoprávnej zodpovednosti na internete nie sú žiadne špecifiká, a pri jej uplatnení vychádzame zo všeobecných princípov uplatnenia trestnoprávnej zodpovednosti. Pri posudzovaní otázky, či je možné za šírenie protiprávneho obsahu prostredníctvom internetu vyvodiť trestnoprávnu zodpovednosť a teda či je toto konanie trestným činom, musia orgány činné v trestnom konaní v prvom rade učiniť potrebné zistenia o rozhodujúcich skutkových okolnostiach. Na základe zistených skutočnosti môžu konštatovať, či zistené skutkové okolnosti napĺňajú formálne znaky konkrétneho trestného činu.

V druhom kroku je potrebné posúdiť okolnosti daného prípadu, ktoré by mohli naznačovať, že uvedené šírenie protiprávneho obsahu nedosahuje potrebnú mieru spoločenskej škodlivosti z hľadiska dolnej hranice trestnej zodpovednosti. Následne by mali orgány činné v trestnom konaní zvážiť či je možné uplatniť zásadu subsidiarity trestnej represie a z nej vyplývajúci princíp *ultima ratio* trestnoprávnej zodpovednosti páchateľa (§ 12 ods. 2 trestného zákonníka).

V praxi sa totiž častokrát vyskytujú prípady protiprávnych konaní, ktoré síce napĺňajú všetky formálne znaky trestného činu, ale vzhľadom na špecifické okolnosti, za ktorých k nim došlo, sú buď spoločensky úplne neškodné, alebo majú len zanedbateľnú spoločenskú škodlivosť. Pre takéto prípady je vylúčené uplatnenie trestnoprávnej zodpovednosti, pretože platí vyššie uvedené, že ak určité protiprávne konanie nedosahuje potrebný stupeň spoločenskej škodlivosti,

[83] Článok 3 písm. h) DSA.

nie je ani možné uvažovať o vyvodení trestnoprávnej zodpovednosti. Nemusí pritom byť naplnená podmienka uplatnenia iného druhu právnej zodpovednosti (napr. čin neplnoletého páchateľa, ktorý šíri obsah chránený autorským právom, nemusí byť kvôli malej intenzite takého zneužitia s prihliadnutím k ostatným okolnostiam prípadu posudzovaný ako priestupok).[84]

Ďalšie odlišnosti v spôsobe vyvodzovania trestnoprávnej zodpovednosti v prostredí internetu predstavuje spôsob identifikácie konkrétneho páchateľa, ktorý šírením protiprávneho obsahu naplnil niektorú zo skutkových podstát trestných činov.

2.5. Identifikovateľnosť páchateľov trestných činov v prostredí internetu

Počítače a ďalšia výpočtová technika sa postupom času stali cenovo dostupnejšou pre značnú časť spoločnosti. Zároveň došlo k zjednodušeniu užívateľského rozhrania počítačov a k rozširovaniu prístupu k internetu, a tým sa internet sprístupnil širokému okruhu používateľov. Zvyšujúci sa počet používateľov vytvoril nový spoločenský fenomén, pocit používateľov, že internet je akýmsi anonymným priestorom, ktorý stojí mimo zavedené spoločenské rámce, a tým aj mimo pôsobnosti trestného práva. Tento pocit anonymity je samozrejme len zdanlivý. Používatelia internetu, prípadne aj páchatelia trestnej činnosti v prostredí internetu, zanechávajú v rámci svojej činnosti digitálnu stopu v podobe online identifikátorov, akými sú napríklad IP adresa, MAC adresy počítača alebo súbory cookies. Tieto identifikátory môžu buď samé o sebe alebo v spojitosti s inými informáciami slúžiť na prípadné identifikovanie páchateľov internetovej trestnej činnosti.

IP adresa (skratka pre angl. výraz *Internet Protocol* adresa) je číselný identifikátor, ktorý je pridelený každému zariadeniu pripojenému k počítačovej sieti, ktorá používa internetový protokol (IP) na odosielanie dát. IP adresy sú základným stavebným kameňom internetu a umožňujú smerovanie dát medzi rôznymi zariadeniami v sieti. IP adresa môže byť buď dynamická (pridelená zariadeniu dočasne pri každom pripojení k sieti) alebo statická (trvalo priradená konkrétnemu zariadeniu). Tieto adresy sú pre smerovanie dát na internete kľúčové, tým že umožňujú identifikovať zariadenia v rámci siete, čím umožňujú šírenie obsahu ako takého.

V súčasnosti rozlišujeme dve verzie IP protokolov, konkrétne IPv4 (angl. *Internet Protocol version 4*) a IPv6 (angl. *Internet Protocol version 6*).[85] IPv6 adresy, ktoré sú novším štandardom

[84] ŠÁMAL, Pavel. § 13 [Trestný čin]. In: ŠÁMAL, Pavel a kol. 2023, s. 235, marg. č. 2.
[85] IPv4 používa 32-bitové adresy, čo umožňuje približne 4,3 miliardy unikátnych adries, čo pri dnešnom počte používateľov nie je dostatočné preto bol vyvinutý protokol IPv4, ktorý je postavený na 128-botovej architektúre, čím zabezpečuje dostatočný priestor pre budúce pripojené zariadenia. IPv6 zahŕňa taktiež integrovanú bezpečnosť prostredníctvom IPsec, čo zjednodušuje zabezpečenie komunikácie medzi zariadeniami.

majú väčší rozsah adries, vznikli kvôli nedostatku adries v systéme IPv4. Hlavným účelom IP adresy je jednoznačne identifikovať zariadenie pripojené k sieti a umožniť smerovanie dát medzi týmito zariadeniami v rámci siete.[86]

MAC adresa (angl. *Media Access Control* adresa) je unikátny číselný identifikátor ktorý je priradený každej sieťovej karte, sieťovému rozhraniu v počítači alebo inom zariadení. MAC adresa je zvyčajne vyjadrená vo forme 16 miestneho čísla oddeleného dvojbodkou. MAC adresa je zariadeniu priradená buď samotným výrobcom hardvéru alebo softvéru v prípade virtuálnych MAC adries. Na rozdiel od IP adresy, ktorá môže byť pridelená a následne zmenená, MAC adresa ostáva nezmenená pre konkrétne sieťové rozhranie po celú dobu jeho existencie.[87] V súčasnosti u modernejších zariadení je však možné MAC adresu meniť.

Súbory **cookies** sú textové súbory, ktoré slúžia k ukladaniu a prijímaniu identifikátorov a ďalších informácií o počítačoch a iných zariadeniach, z ktorých používateľ pristupuje na konkrétne webové stránky. Dokážu zaznamenať návštevu konkrétneho používateľa na danej webovej stránke a upraviť jej funkcionalitu na základe jeho zvolených preferencií.[88]

Samotné spojenie páchateľa s konkrétnym identifikátorom nemusí byť ešte samo o sebe dostačujúce pre jeho identifikáciu a následné vyvodenie trestnoprávnej zodpovednosti za spáchaný trestný čin. Príkladom môže byť rozhodnutie špecializovaného trestného súdu Slovenskej republiky, ktorý vo veci trestného stíhania toho času poslanca Národnej rady Slovenskej republiky Stanislava Mizíka za extrémistické statusy na sociálnej sieti Facebook rozhodol, že aj keď boli statusy písané z Facebookového profilu poslanca, nie je za toto konanie zodpovedný, pretože sa obhajobe podarilo preukázať, že nevie pracovať s počítačom.[89]

Toto rozhodnutie stelesňuje základný problém vyvodzovania trestnoprávnej zodpovednosti v prostredí internetu, ktorý spočíva v schopnosti preukázať, že konkrétny páchateľ spáchal určitý trestný čin. Zákonodarca má za úlohu vytvoriť adekvátny legislatívny rámec, ktorý by poskytoval orgánom činným v trestnom konaní dostatočné mechanizmy na zabezpečenie potrebných dôkazov na usvedčenie páchateľa. V demokratických a právnych štátoch predstavuje táto úloha zložitú problematiku s ohľadom na súčasný zásah do súkromia jednotlivcov. Zákonodarcovia sú tak

[86] YASAR, Y. *IP address (Internet Protocol address)*. In Techtarget.com [online]. [cit. 2023-06-14]. Dostupné z: https://www.techtarget.com/whatis/definition/IP-address-Internet-Protocol-Address.
[87] YASAR, Y. *MAC address (media access control address)*. In Techtarget.com [online]. [cit. 2023-06-14]. Dostupné z: https://www.techtarget.com/searchnetworking/definition/MAC-address.
[88] Používanie súborov cookies je regulované zákonom o elektronických komunikáciách.
[89] Porov. napr. článok HUTKO, D. a FILOVÁ, K. *Písal Mizík hanlivý status? Súd to nepotvrdil*. In Pravda.sk [online]. [cit. 2023-06-20]. Dostupné z: https://spravy.pravda.sk/domace/clanok/518484-zacal-sa-proces-s-poslancom-stanislavom-mizikom-obzalovanym-z-extremizmu/.

nútení starostlivo vyvažovať medzi záujmami spoločnosti na vyšetrovaní trestnej činnosti na jednej strane a minimalizovaním úrovne zásahu na zachovanie dostatočnej ochrany súkromia používateľov internetu na strane druhej.

Nariadenie o digitálnych službách (DSA)[90] prinesie isté významné zmeny v oblasti trestného konania. Na základe článku 9 DSA získajú orgány činné v trestnom konaní právomoc identifikovať pôvodcu obsahu prostredníctvom tzv. príkazu na poskytnutie informácii. Tento príkaz umožní orgánom žiadať od poskytovateľa služieb informačných spoločností relevantné dôkazy, údaje a informácie potrebné na identifikáciu príjemcov dotknutej služby.

Súčasne s tým budú mať orgány činné v trestnom konaní na základe článku 10 DSA možnosť príkazom uložiť poskytovateľovi služieb informačných spoločností povinnosť konať proti nezákonnému obsahu, ktorý je šírený prostredníctvom poskytovanej služby. Tieto nové právomoci by mohli predstavovať signifikantný krok v prešetrovaní trestnej činnosti spojenej so šírením protiprávneho obsahu na veľkých sociálnych sieťach. Poskytovatelia služieb sa budú musieť pod hrozbou vysokých sankcií zaoberať týmito príkazmi a konať v snahe eliminovať nezákonný obsah. Je však otázne, do akej miery bude DSA efektívne v praxi. Tento aspekt bude vyžadovať ďalšie hodnotenie a sledovanie.

2.6. Trestné činy v súvislosti so šírením protiprávneho obsahu

Už dávno nie je možné považovať internet len za miesto, v ktorom sa šíria informácie, ale je potrebné na neho nahliadať v právnej teórii komplexnejšie ako na fenomén, ktorý so sebou prináša isté špecifiká právnych vzťahov, ktoré v jeho prostredí vznikajú. V súčasnosti predstavuje internet jedno z najvplyvnejších médií a hlavný kanál komunikácie medzi ľuďmi na celom svete. Trestná zodpovednosť páchateľov v súvislosti so šírením protiprávneho obsahu môže byť najčastejšie páchaná v súvislosti za trestné činy:

- proti právam na ochranu osobnosti, súkromia a listového tajomstva (§ 180 - 184 trestného zákonníka)
- šírenie pornografie (§ 191 trestného zákonníka),
- výroba a iné nakladanie s detskou pornografiou (§ 192 trestného zákonníka),
- nadväzovanie nezákonných kontaktov s dieťaťom (§ 193b trestného zákonníka),
- porušovanie autorského práva, práv súvisiacich s autorským právom a práv k databáze (§ 270 trestného zákonníka);

[90] Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách).

- hanobenie národa, rasy, etnickej alebo inej skupiny osôb (§ 355 trestného zákonníka);
- neoprávneného prístupu do počítačového systému a neoprávnený zásah do počítačového systému alebo nosiča informácií (§ 230 trestného zákonníku);
- podnecovanie k nenávisti voči skupine osôb alebo k obmedzovaniu ich práv a slobôd (§ 356 trestného zákonníka);
- šírenie poplašnej správy (§ 357 trestného zákonníka);
- ohováranie (§ 184 trestného zákonníka); a
- vydieranie (§ 175 trestného zákonníka).

Diplomová práca si v ďalšej časti kladie za cieľ definovať trestnoprávnu zodpovednosť za protiprávne šírenie pornografického obsahu a ďalšie konanie páchateľov v súvislosti s porušovaním súkromia jednotlivca v sexuálnej oblasti a posúdiť, aktuálnosť platnej právnej úpravy pri postihovaní trestnej činnosti v tejto oblasti. Cieľom tejto časti diplomovej práce je oboznámiť čitateľa s tým, ako častokrát právna úprav nedokáže odrážať špecifiká konkrétnych konaní, ktoré so sebou zákonite prináša nástup nových technológii.

2.7. Trestnoprávna zodpovednosť za protiprávne šírenie pornografického obsahu

2.7.1. Protiprávne šírenie pornografického obsahu

Systematicky trestný zákonník upravuje trestné činy v súvislosti s protiprávnym šírením pornografického obsahu v tretej hlave zvláštnej časti trestného zákonníka - trestné činy proti ľudskej dôstojnosti v sexuálnej oblasti, a to konkrétne v ustanoveniach § 185 až § 193b. Obsahom tejto hlavy trestného zákonníka sú sexuálne motivované protiprávne konania páchateľov, ktoré sú v svojej podstate v rozpore s morálnym konsenzom spoločnosti v oblasti sexuálnych vzťahov.

Cieľom tejto časti trestného zákonníka, rešpektujúc zásadu subsidiarity trestnej represie, nie je postihovať všetky trestné činy v súvislosti so šírením pornografického obsahu, ale len také protiprávne konanie páchateľa, ktoré predstavuje porušenia morálnych zásad reflektovaných v trestnej politike Českej republiky. Predovšetkým konania páchateľov v prípadoch, v ktorých ich sexuálne motivované správanie ohrozuje iné hodnoty chránené trestným právom, akými sú napríklad ľudská dôstojnosť, právo na súkromie v sexuálnej oblasti, mravný a telesný vývoj detí a pod.[91]

[91] ŠÁMAL, P; NOVOTNÝ, O; GŘIVNA, T; HERCZEG, J; VANDUCHOVÁ, M et al. 2022, op. cit., 707 s.

V tejto súvislosti je potrebné opätovne zdôrazniť, že nie každé šírenie pornografických materiálov je automaticky považované za protiprávne. Naopak, trestné právo postihuje len také šírenie pornografických diel, ktoré vyobrazujú násilné konanie, neúctu k človeku, sexuálny styk so zvieraťom, alebo ktoré akýmkoľvek spôsobom zachytávajú sexuálny styk s dieťaťom. Česká republika v tomto prípade nešla cestou úplného zákazu pornografie ako takej, ako napríklad v niektorých krajinách, predovšetkým na blízkom východe a v Číne, kde je už samotné šírenie pornografie a sexuálne explicitného materiálu protizákonné.[92] Nepovažujeme to ani za vhodné, vzhľadom na súčasnú úroveň technologického pokroku a dostupnosti internetu, pretože akékoľvek pokusy o zásah do šírenia pornografického obsahu by boli v podstate nekontrolovateľné a ich bezmedzné vymáhanie by predstavovalo neprijateľný zásah do slobôd a súkromia jednotlivcov.

Trestný zákonník v súvislosti so šírením pornografie upravuje v tretej hlave zvláštnej časti tri skutkové podstaty, konkrétne sa jedná o trestný čin šírenia pornografie (§ 193 trestného zákonníka), výrobu a iné nakladanie s detskou pornografiou (§ 194 trestného zákonníka) a zneužitie dieťaťa k výrobe detskej pornografie (§ 195 trestného zákonníka).

2.7.2. Definícia pornografického diela

Názory na to, čo je spoločensky prijateľné v sexuálnej oblasti sa menia v čase, priestore a s dosiahnutým stupňom rozvoja spoločnosti. Tieto názory sa líšia v jednotlivých geografických regiónoch a medzi jednotlivými skupinami obyvateľstva. Pri posúdení či je možné dané autorské dielo označiť za pornografické je možné využiť tzv. *test pornografickej povahy diela*, ktorý je založený na posúdení toho, či celkový dojem z diela vyvoláva morálne pohoršenie u osoby s bežnou citlivosťou.[93]

Česká právna úprava neobsahuje legálnu definíciu pojmu pornografické dielo, ale stanovuje len jeho jednotlivé formy, ktorými sú pornografické diela fotografické, filmové, počítačové, elektronické alebo iné pornografické diela, a vo vzťahu k osobám mladším ako osemnásť rokov rozlišuje aj písomné pornografické dielo. Pre porovnanie slovenský trestný zákon[94] definuje v § 132 ods. 3 pornografické dielo ako „*zobrazenie súlože, iného spôsobu pohlavného styku alebo iného obdobného sexuálneho styku alebo zobrazenie obnažených pohlavných orgánov určené na sexuálne účely*“.

[92] Informácie vychádzajú z portálu *World Population Review* z článku *Countries Where Porn Is Illegal 2023*, In Worldpopulace.com [online]. [cit. 2023-06-17]. Dostupné z: https://worldpopulace.com/countries-where-porn-is-illegal/.
[93] ŠÁMAL, P; NOVOTNÝ, O; GŘIVNA, T; HERCZEG, J; VANDUCHOVÁ, M et al. 2022, op. cit., 718 s.
[94] Zákon č. 300/2005 Z. z. Trestný zákon.

Pornografické dielo je možné podľa právnej teórie definovať ako také dielo, ktorého jediným alebo primárnym účelom je vyvolať alebo zvýšiť sexuálne vzrušenie osoby, ktorá je takému dielu vystavená. Spravidla to pornografické dielo dosahuje opisom, vyobrazením či iným znázornením pohlavného styku, masturbácie alebo čiastočným alebo úplným obnažením pohlavných orgánov.[95] Pornografické dielo býva tiež definované ako dielo, ktoré vtieravým spôsobom podnecuje sexuálny pud, prekračuje hranice sexuálnej slušnosti akceptované prevládajúcimi názormi v spoločnosti, uráža zmysel pre sexuálnu slušnosť neprijateľným spôsobom a vyvoláva pocit hanby.[96] Za pornografické dielo ale nie je považované každé vyobrazenie nahého ľudského tela, a to predovšetkým s ohľadom na zasadenie do prirodzenej situácie, v ktorej sa nahé ľudské telo bežne nachádza (napríklad kúpeľ), alebo vyobrazenie nahého ľudského tela pre účely reklamy, a to aj v prípade, ak by toto vyobrazenie mohlo svojím prevedením u pozorovateľa vzbudiť sexuálne vzrušenie.

Pre úplnosť výkladu je potrebné dodať, že dielom sa v tomto kontexte chápe dielo autorské, vo zmysle § 2 autorského zákona. Teda konkrétne dielo literárne, vedecké alebo iné umelecké dielo, ktoré predstavuje jedinečný výsledok individuálnej tvorivej činnosti autora, ktoré je vyjadrené vo forme, ktorá je objektívne vnímateľná, vrátane elektronickej formy, bez ohľadu na rozsah, účel alebo význam diela, a to buď trvale alebo dočasne.[97]

Pre účely tejto diplomovej práce je podstatné definovať predovšetkým pojmy elektronické pornografické dielo a počítačové pornografické dielo. Za elektronické pornografické dielo je potrebné považovať také pornografické dielo, ktoré je dostupné v strojovo čitateľnej podobe. Pričom za počítačové pornografické dielo sa považuje aj pornografické dielo, ktoré bolo vytvorené za pomoci počítačového softvéru, akými sú grafické programy alebo systémy umelej inteligencie na automatickú generáciu obsahu.[98]

2.8. Šírenie pornografie (§ 191 trestného zákonníka)

Prvým z trestných činov, ktorých predmetom je ochrana spoločnosti pred nakladaním s protiprávnym pornografickým obsahom je trestný čin šírenia pornografie, ktorý v sebe zahŕňa dve základné skutkové podstaty. Objektom prvej z nich (§ 193 ods. 1 trestného zákonníka), je záujem spoločnosti na ochrane mravnosti dospelých pred osobitným druhom útokov, ktoré predstavuje

[95] ŠČERBA, F. § 191 [Šíření pornografie]. In: ŠČERBA, F. a kol. 2022. op. cit., marg. 3.
[96] ŠÁMAL, P; NOVOTNÝ, O; GŘIVNA, T; HERCZEG, J; VANDUCHOVÁ, M et al. 2022, op. cit., 718 s.
[97] Porov. § 2 zákona č. 121/ 2000 Sb., autorský zákon vo znení neskorších predpisov.
[98] GŘIVNA, T. *Trestné činy proti lidské důstojnosti v sexuální oblasti v novém trestním zákoníku*. In Bulletin advokacie, č. 10, s. 70 [online]. [cit. 2023-06-16]. Dostupné z: https://www.cak.cz/assets/files/2678/BA_10_2009_web.pdf.

sexuálne obťažovanie tzv. tvrdou pornografiou, alebo niekedy tiež v právnej teórii označovanou zvrátenou pornografiou. Táto skutková podstata postihuje výrobu a nakladanie s pornografiou, ktorá vyobrazuje násilie alebo neúctu k človeku, a taktiež pornografiu, ktorá opisuje, zobrazuje alebo inak znázorňuje pohlavný styk človeka so zvieraťom.[99]

Objektom druhej skutkovej podstaty trestného činu šírenia pornografie je ochrana osôb mladších ako 18 rokov pred tzv. obyčajnou pornografiou (§ 193 ods. 2 trestného zákonníka). V tomto prípade trestný zákonník postihuje správanie páchateľa, v ktorom priamo ponúka, odovzdáva alebo sprístupňuje pornografické dielo osobe mladšej ako 18 rokov (tzn. dieťaťu), alebo prípadne v ktorom páchateľ takto sprístupňuje pornografické dielo na mieste, ktoré je prístupné osobám mladším ako osemnásť rokov.[100] Teda aj konanie páchateľa, pri ktorom akýmkoľvek spôsobom šíri pornografické dielo so zameraním na dieťa v prostredí internetu.

2.8.1. Šírenie tvrdej pornografie

Tvrdou (zvrátenou) pornografiou chápeme pornografické dielo, ktoré vyobrazuje násilie, neúctu k človeku alebo ktoré znázorňuje pohlavný styk so zvieraťom. Násilím sa v tomto kontexte chápe len násilie voči človeku v súvislosti so sexuálnym správaním páchateľa. Predmetné pornografické dielo musí zároveň zahŕňať násilie vyššej intenzity, a nie napríklad len isté formy násilia, ktoré sú všeobecne akceptované ako napríklad „plieskanie“ alebo spútavanie pri sexuálnych aktivitách. Neúctou k ľudskej osobe v kontexte trestného činu šírenia pornografie chápeme zobrazovanie rôznych foriem ponižovania, sexuálneho zotročovania, znásilňovania atď. Aj v tomto prípade platí vyššie spomenuté, že toto neúctivé správanie musí byť vykonávané v súvislosti so sexuálne motivovaným správaním, a zároveň musí byť páchateľom vykonávané s vyššou mierou intenzity. Za pohlavný styk so zvieraťom sa považuje konanie páchateľa, ktoré je smerované na účely uspokojenia sexuálneho pudu človeka, ktorého sa v akejkoľvek forme zúčastňuje zviera.[101]

Páchateľom trestného činu šírenia pornografie môže byť ktokoľvek, teda fyzická alebo právnická osoba, ktorá je trestnoprávne zodpovedná, a to vrátane mladistvých. Páchateľom trestného činu šírenia pornografie môže byť teda aj osoba, ktorá je mladšia ako osemnásť rokov a je sama dieťaťom. Ochrana detí podľa tohto ustanovenia smeruje k deťom, ktoré sú ohrozené

[99] ŠČERBA, F. § 191 [Šíření pornografie]. In: ŠČERBA, F. a kol. 2022. op. cit., marg. 1.
[100] ŠČERBA, F. § 191 [Šíření pornografie]. In: ŠČERBA, F. a kol. 2022. op. cit., marg. 3.
[101] ŠČERBA, F. § 191 [Šíření pornografie]. In: ŠČERBA F. a kol. 2022. op. cit., marg. 11.

šírením pornografie, nie na tie, ktoré takéto ohrozenie samé svojím protiprávnym konaním vyvolávajú.[102]

2.8.2. Spôsoby šírenia pornografie v prostredí internetu

V prostredí internetu je možné spáchanie trestného činu šírenia pornografie šírením prostredníctvom verejne prístupnej počítačovej siete. Páchateľ sa trestného činu dopustí, najmä ak sprístupní pornografické dielo na internetovej stránke alebo toto dielo iným spôsobom sprístupňuje či šíri v prostredí internetu. V tomto kontexte je potrebné dodať, že pojem verejne prístupná počítačová sieť nezahŕňa každé šírenie v prostredí internetu. V prípade uzavretých počítačových sieti, ktoré sú používané napríklad v rámci podnikov, v školách alebo na úradoch (tzv. intranety) nebude možné hovoriť o šírení verejne prístupnej počítačovej siete. Rovnako za šírenie pornografických diel prostredníctvom verejne prístupnej počítačovej siete nie je možné považovať ani šírenie prostredníctvom elektronickej pošty medzi tzv. e-mailovými schránkami chránenými individuálnymi prístupovými heslami. V prípade zasielania pornografických diel na veľký počet e-mailových adries, ak je význam tohto činu pre šírenie diela porovnateľný so spáchaním trestného činu prostredníctvom tlače, filmu, rozhlasu, televízie alebo verejne prístupnej počítačovej siete, napĺňa znak „iného obdobne účinného prostriedku“ v zmysle § 191 ods. 3 písm. b) a § 192 ods. 3 písm. b) trestného zákonníka. Túto podmienku spĺňa napríklad šírenie pornografických diel 163 príjemcom.[103] Problematikou pojmu verejne prístupná počítačová sieť sa práca podrobnejšie zaoberá v tretej kapitole.

2.9. Pojem detská pornografia

Ochrana detí predstavuje jeden zo základných biologických a sociálnych úloh spoločnosti. Sexuálne zneužívanie a sexuálne vykorisťovanie detí, spolu s vytváraním detskej pornografie, predstavujú závažné narušenie ich základných práv a slobôd. Toto konanie sa dotýka najmä práv detí na ochranu a starostlivosť. Výskyt diel, ktoré vyobrazujú detskú pornografiu, ktorá pozostáva z obrázkov zobrazujúcich sexuálne zneužívanie detí alebo iné obzvlášť závažné formy sexuálneho zneužívania a sexuálneho vykorisťovania detí, sa zvyšuje a narastá spolu s rozširovaním používania nových informačných technológií a internetu.[104] Česká republika sa spolu s ďalšími štátmi v súlade s článkom 34 Dohovoru Organizácie Spojených národov o právach dieťaťa[105]

[102] Uznesenie Najvyššieho súdu zo dňa 20.07.2022, sp. zn. 8 Tdo 514/2022.
[103] Stanovisko Najvyššieho súdu zo dňa 30.01.2013, sp. zn. Tpjn 300/2012.
[104] Porov. recitál č. 2 Smernice Európskeho parlamentu a Rady 2011/93/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorou sa nahrádza rámcové rozhodnutie Rady 2004/68/SVV. V ďalšej časti len ako smernice 2011/93/EÚ.
[105] Dohovor o právach dieťaťa prijatý a otvorený na podpis, ratifikáciu a pristúpenie rezolúciou Valného zhromaždenia z 20. novembra 1989. Ďalej ako Dohovor o právach dieťaťa.

zaviazala, že príjme opatrenia pre ochranu detí pred všetkými formami sexuálneho vykorisťovania a sexuálneho zneužívania.

Trestný zákonník definuje detskú pornografiu v § 192 odseku 1 a 3 ako fotografie, filmy, počítačové, elektronické alebo iné pornografické dielo, ktoré zobrazuje alebo inak využíva dieťa alebo osobu, ktorá sa javí byť dieťaťom.[106] Za detskú pornografiu sa teda považuje vyobrazenie detí zapojených do sexuálneho konania alebo samotné vyobrazenie ich pohlavných orgánov, ktoré slúžia na sexuálne účely bez ohľadu na to, či boli vyhotovené s vedomím dieťaťa alebo bez jeho vedomia. Táto právna úprava vychádza zo smernice Európskej únie č. 2011/93/EÚ,[107] ktorá v článku 2 písm. c) definíciu detskej pornografie ďalej rozširuje na akýkoľvek materiál, ktorý zobrazuje dieťa, ktoré sa zúčastňuje skutočného alebo predstieraného sexuálneho konania, akékoľvek zobrazenie pohlavných orgánov dieťaťa primárne určené na sexuálne účely, realistické vyobrazenie dieťaťa, ktoré sa zúčastňuje jednoznačného sexuálneho konania, alebo realistické vyobrazenie pohlavných orgánov dieťaťa primárne určené na sexuálne účely.[108]

Dieťaťom sa pre účely trestného práva v zmysle § 126 trestného zákonníka rozumie osoba mladšia ako 18 rokov, pokiaľ osobitné ustanovenia trestného práva neurčia inak. Toto chápanie pojmu „dieťa“ obsahovo vychádza z článku 1 Dohovoru o právach dieťaťa, ktorý definuje dieťa ako ľudskú bytosť mladšiu ako osemnásť rokov.

Pre úplnosť výkladu je nutné podotknúť, že spomínaná právna úprava nepredstavuje všeobecný zákaz sexuálneho styku alebo iného sexuálne motivovaného správania smerovaného voči osobe mladšej ako osemnásť rokov. V tejto súvislosti si ani smernica 2011/93/EÚ nekladie za cieľ zosúladiť vek spôsobilosti osôb dať súhlas na sexuálne aktivity. Vek, do ktorého je zakázané zapájať sa do sexuálnych aktivít s dieťaťom smernica ponecháva na úpravu vnútroštátneho práva jednotlivých členských štátov.[109] Vek, od ktorého je povolený sexuálny styk s dieťaťom je v jednotlivých členských štátoch v rozmedzí 13 – 17 rokov. Najnižšiu hranicu trinásť rokov zaviedlo napríklad Španielsko a hranicu sedemnásť rokov veku nájdeme napríklad v Írsku. Česká republika, podobne ako Slovensko, ustanovila hranicu veku, od ktorého je povolený pohlavný styk na pätnásť rokov.[110]

[106] § 192 ods. 1, 3 trestného zákonníka.
[107] Smernica Európskeho parlamentu a Rady 2011/93/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorou sa nahrádza rámcové rozhodnutie Rady 2004/68/SVV.
[108] Článok 2 c smernice 2011/93/EÚ.
[109] Článok 2 b smernice 2011/93/EÚ.
[110] KLIMEK, L.; ZÁHORA, J. a HOLCR, K. 2016, op. cit., s. 202.

Trestný zákonník považuje za detskú pornografiu aj pornografické dielo, v ktorom nie je zobrazené, alebo ani inak použité skutočné dieťa, t. j. reálna fyzická osoba mladšia ako 18 rokov ale postačuje, ak sa osoba v pornografickom diele javí byť dieťaťom. Komentovaná literatúra k § 192 trestného zákonníka za osobu, ktorá sa javí byť dieťaťom považuje taktiež osobu, ktorá v skutočnosti nie je dieťaťom, ale ktorej vzhľad, správanie, oblečenie, hlas alebo celkový kontext diela v ktorom je dané dieťa vyobrazené, môžu u priemerného diváka jednoznačne vyvolať dojem, že ide o dieťa mladšie ako osemnásť rokov. Za detskú pornografiu bude považované aj pornografické dielo, v ktorom vystupuje postava vytvorená napr. pomocou počítačovej animácie alebo generatívneho softvéru umelej inteligencie, ak vyobrazuje dieťa realisticky alebo sa toto vyobrazenie javí ako dieťa.

Aj v kontexte detskej pornografie platí vyššie spomenuté, že samotný záver o pornografickom charaktere diela nemôže byť jednoznačne vyvodený len z faktu, že je v diele vyobrazené dieťa, a toto dielo je vo svojej podstate schopné uspokojiť sexuálne pudy inej osoby trpiacej istou formou sexuálnej deviácie (pedofíliou, hebefíliou alebo efebofíliou), teda osoby, pre ktoré sú sexuálne príťažlivé neplnoleté osoby, na miestach alebo v médiách, ktoré tieto osoby vyhľadávajú. Podľa rozhodnutia Najvyššieho súdu, je možné za detskú pornografiu jednoznačne označiť také dielo, ktoré obsahuje snímky nahých detských modelov v pózach, ktoré vyzývavo prezentujú pohlavie alebo simulujú sexuálny styk s nimi.[111]

2.10. Trestná zodpovednosť za výrobu a iné nakladanie s detskou pornografiou (§ 192 trestného zákonníka)

Páchateľom trestného činu výroby a iného nakladania s detskou pornografiou v zmysle § 192 trestného zákonníka môže byť akákoľvek osoba, fyzická alebo právnická, vrátane mladistvých. Predmetom tejto diplomovej práce je predovšetkým trestná zodpovednosť páchateľa za šírenie protiprávneho obsahu v prostredí internetu, preto sa diplomová práca vo svojej ďalšej časti zaoberá predovšetkým trestnoprávnou zodpovednosťou za šírenie detskej pornografie, jej prechovávanie a prehliadanie webových stránok s obsahom detskej pornografie.[112]

2.10.1. Prechovávanie detskej pornografie

Dielo s obsahom detskej pornografie predstavuje vyššiu mieru ohrozenia záujmov spoločnosti, ako nakladanie s takzvanou pornografiou prostou. Ochrana detí pred ich zapájaním sa do výroby sexualizovaného obsahu vychádza z medzinárodných záväzkov Českej republiky a z práva Európskej únie. Podľa judikatúry Najvyššieho súdu sa prechovávaním detskej

[111] Uznesenie Najvyššieho súdu zo dňa 28. 12. 2004, sp. zn. 7 Tdo 1077/2004.
[112] Porov. § 192 trestného zákonníka.

pornografie rozumie akýkoľvek spôsob uchovávania pornografických materiálov, ktoré obsahujú vyobrazenie nahých detí v polohách, ktoré predstavujú alebo naznačujú pohlavný styk, alebo v polohách, ktoré podnecujú predstavu pohlavného styku s nimi. Dĺžka doby prechovávania pornografického diela nie je v tomto ohľade podstatná. Postačuje teda, ak páchateľ pornografický obsah s detskou pornografiou prechováva len po určitú dobu, teoreticky aj niekoľko sekúnd. Nie je ani nevyhnutné, aby páchateľ mal detskú pornografiu priamo vo svojej držbe (napríklad v taške, v šuplíku, doma, v práci, vo svojom počítači), podľa rozhodnutia Najvyššieho súdu postačuje, ak ju má vo svojej moci (napríklad uloženú v e-mailovej schránke prípadne na cloude alebo na serveri poskytovateľa internetových služieb).[113]

Pre naplnenie subjektívnej stránky trestného činu výroby a iného nakladania s detskou pornografiou v zmysle v § 192 ods. 1 trestného zákonníka sa vyžaduje úmyselná forma zavinenia, pričom trestný zákonník predpokladá úmysel eventuálny. Páchateľ musí vedieť alebo byť prinajmenšom uzrozumený s možnosťou, že vo svojej držbe prechováva pornografické dielo, ktoré vyobrazuje dieťa alebo osobu ktorá sa javí byť dieťaťom v sexuálnom styku alebo v inej forme sexuálne motivovaného konania.

Isté špecifikum predstavuje situácia, v ktorej existuje istá forma citového vzťahu medzi páchateľom trestného činu a dieťaťom, v ktorej napríklad osemnásťročný páchateľ prechováva pornografické dielo, ktoré obsahuje snímky jeho sedemnásťročnej družky, ktorá s vyhotovením pornografického diela vyslovila dobrovoľný súhlas alebo páchateľovi sama takýto obsah poskytla. V takom prípade by bolo možné uvažovať o tom, že týmto skutkom nebola naplnená subjektívna stránka trestného činu, pretože páchateľ nemal úmysel nakladať s detskou pornografiou. Prípade by pripadalo v úvahu, vzhľadom k tomu, že páchateľ prechováva pornografické dielo čisto pre vlastnú potrebu a nižšiu (alebo skoro žiadnu) mieru spoločenskej škodlivosti využitie zásady subsidiarity trestnej represie.[114] V tomto prípade by pravdepodobne nedošlo ani k ohrozeniu objektu trestného činu, ktorým je mravná ochrana spoločnosti pred protiprávnym nakladaním s detskou pornografiou a ochrana dotknutých detí.

Najvyšší súd sa vo svojom stanovisku zo dňa 30. januára 2013 vyjadril kladne k možnosti súbehu trestných činov šírenia pornografie a výroby a iného nakladania s detskou pornografiou.[115]

---

[113] Uznesenie Najvyššieho súdu zo dňa 28.05.2014, sp. zn. 6 Tdo 551/2014.

[114] ŠČERBA, F. *Posuzování případů zneužívání dětí prostřednictvím internetu k pornografickým účelům*. In Trestněprávní revue, 2020, č. 3, s. 125-129. In Beck [online]. [cit. 2023-06-20]. Dostupné z: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=nrptembsgbpxi4s7gnpxgxzrgi2q&groupIndex=1&rowIndex=0&refSource=search.

[115] Stanovisko Najvyššieho súdu zo dňa 30.1.2013, sp. zn. Tpjn 300/2012.

2.10.2. Získanie prístupu k detskej pornografii

Trestný zákonník okrem vyššie spomenutého prechovávania detskej pornografie postihuje nie len konanie páchateľa, pri ktorom dochádza ku ukladaniu pornografického diela na úložisko páchateľa, ale aj také konanie, s úmyslom získať prostredníctvom informačných alebo komunikačných technológii prístup k detskej pornografii. Komunikačnými a informačnými technológiami sa v tomto kontexte chápu systémy, ktoré umožňujú výmenu dát a informácii medzi počítačovými systémami prepojenými v sieti, pričom na túto komunikáciu využívajú technické (hardvérové) a programové (softvérové) prostriedky.[116]

Takým konaním chápeme napríklad prosté prehliadanie webových stránok s úmyslom získať prístup k detskej pornografii. Páchateľom trestného činu získania prístupu k detskej pornografii môže byť akákoľvek fyzická a právnická osoba, vrátane mladistvých. Subjektívna stránka spočíva v úmysle páchateľa vstúpiť na webové stránky, pričom si je vedomí že na nich môže detskú pornografiu nájsť.[117] Rovnako ako v prípade prechovávania detskej pornografie aj pri získavaní prístupu postačuje úmysel eventuálny.[118] Smernica o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii[119] uvádza, že trestne zodpovednou by nemala byť osoba, ktorá sa na stránky s detskou pornografiou dostane neúmyselne pri prehliadaní internetu. Úmyselnosť konania páchateľa by bolo možné vyvodiť zo skutočnosti, že na predmetné stránky pristupuje opakovane, teda s vedomím toho, že webové stránky obsahujú detskú pornografiu. Zároveň je možné trestnosť konania vyvodiť v prípade, že páchateľ pre prístup k detskej pornografii využíva istú formu služby za odplatu. Za získavanie prístupu k detskej pornografii hrozí v prípade odsúdenia páchateľovi trest odňatia slobody až do výšky dvoch rokov.[120]

2.10.3. Šírenie detskej pornografie

Treťou skutkovou podstatou v rámci trestného činu výroby a nakladania s detskou pornografiou predstavuje konanie páchateľa, ktorý vyrába, dováža, preváža, ponúka, učiní verejne dostupným, uvedie do obehu, predá alebo iným spôsobom poskytne inej osobe fotografické, filmové, počítačové, elektronické alebo iné pornografické dielo, ktoré zobrazuje alebo inak zneužíva dieťa alebo osobu, ktorá vyzerá ako dieťa (§ 192 ods. 3 trestného zákonníka). Rovnako

[116] GŘIVNA, T. § 192 [Výroba a jiné nakládání s dětskou pornografií]. In: ŠÁMAL. 2023, op. cit., s. 2404, marg. č. 10.
[117] Porov. recitál 18 smernice Európskeho parlamentu a Rady 2011/93/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorou sa nahrádza rámcové rozhodnutie Rady 2004/68/SVV. Ďalej len Smernica 2011/93/EU.
[118] In: ŠÁMAL, P a kol. 2023, op. cit., s. 2404, marg. č. 11.
[119] Smernica 2011/93/EU.
[120] Porov. § 192 ods. 2 trestného zákonníka.

aj v tomto prípade môže byť páchateľom ktokoľvek, vrátane mladistvých. Jedná sa o skutkovú podstatu, ktorá postihuje šírenie detskej pornografie. Podstatná je predovšetkým trestná zodpovednosť páchateľa za šírenie detskej pornografie prostredníctvom verejne prístupnej počítačovej siete, predovšetkým internetu, ktoré je postihované ako zvlášť priťažujúca okolnosť v rámci odstavca 4. zmieneného paragrafu. K uvedenému je potrebné konštatovať, že šírenie detskej pornografie prostredníctvom elektronickej pošty, s prístupom chráneným individuálnymi heslami nenaplní znak verejnej počítačovej siete. Naopak, ak by šlo o značný počet e-mailových adries, znak verejnosti by už mohol byť naplnený.[121] Za zvlášť priťažujúcu okolnosť je rovnako považované aj konanie páchateľa v rámci organizovanej skupiny alebo s úmyslom získať pre seba alebo iného značný prospech.[122]

Ústavný súd pri posúdení naplnenia znaku učinenia verejne prístupným v prípade, v ktorom páchateľ šíril detskú pornografiu prostredníctvom sociálnych sietí dospel k záveru, že súdy musia najprv objasniť, ktorú z funkcií mal páchateľ k dispozícii, ktoré skutočne použil a čo toto použitie znamená z hľadiska rozsahu jeho trestnej činnosti.[123]

2.11. Nadviazanie nedovoleného kontaktu s dieťaťom (§ 193b trestného zákonníka)

Podobne ako v predchádzajúcich časti, je týmto ustanovením chránená bezpečnosť dieťaťa mladšieho ako pätnásť rokov pred skorými sexuálnymi kontaktmi a následne pred sexuálnym zneužívaním, čím sa zabezpečuje jeho morálny a telesný vývoj. Trestný čin nadviazania nedovoleného kontaktu s dieťaťom je trestným činom ohrozovacím, Nemusí teda dôjsť k samotnému narušeniu morálneho a telesného vývoja ale, postačuje, ak by k takýmto situáciám hypoteticky mohlo dôjsť.[124] Trestnosť konania páchateľa spočíva v kontaktovaní dieťaťa s úmyslom návrhu stretnutia, a to za sexuálne motivovaným účelom. Návrh na takéto stretnutie môže byť urobený akýmkoľvek spôsobom, napr. prostredníctvom informačných alebo komunikačných technológií, v listinnej podobe či ústne.[125]

Jedná sa napríklad najčastejšie o situáciu, kedy páchateľ kontaktuje dieťa prostredníctvom sociálnych sietí a to buď písomne cez čet (chat) alebo prostredníctvom videohovoru. V rámci toho páchateľ vyzve dieťa, aby mu zaslalo svoje obnažené fotografie alebo videá, prípadne aby sa mu obnažilo vo videohovore. Pre uplatnenie trestnoprávnej zodpovednosti je podmienkou, aby bol

[121] Stanovisko trestného kolégia Najvyššieho súdu z 30. 1. 2013, vec č. Tpjn 300/2012.
[122] Porov. § 193 ods. 4 trestného zákonníka.
[123] Rozhodnutie Ústavného súdu zo dňa 31. 1. 2017, sp. zn. IV.ÚS 3223/16.
[124] GŘIVNA, T. § 193b [Navazování nedovolených kontaktů s dítětem]. In: ŠÁMAL, Pavel a kol. 2023, op. cit., s. 2417, marg. č. 1.
[125] Porov. uznesenie Najvyššieho súdu zo dňa 25. 11. 2020, sp. zn. 8 Tdo 1041/2020.

páchateľ minimálne uzrozumený s tým, že zaslaný obsah bude mať pornografický charakter, v opačnom prípade by nedošlo k naplneniu subjektívnej stránky uvedeného trestného činu. Napríklad v prípade, kedy by páchateľ žiadal len obyčajnú fotografiu ale dieťa mu zo svojej vôle zašle erotickú fotografiu. V konečnom dôsledku je potrebné predpokladať, že páchateľ pozná skutočný vek dieťaťa, to znamená že v tomto ohľade nedochádza k omylu.[126]

V prípade trestného činu nadviazania nedovoleného kontaktu s dieťaťom je predmetom ochrany len dieťa mladšie ako pätnásť rokov, na rozdiel od trestného činu výroby a iného nakladania s detskou pornografiou (§ 182 trestného zákonníku). Trestný čin nadviazania nedovoleného kontaktu nepostihuje kontaktovanie osoby, ktorá sa javí byť dieťaťom. Túto textáciu zákona možno považovať za nešťastnú a malo by dôjsť k rozšíreniu jeho aplikovateľnosti aj na konanie páchateľa, ktorý za účelom stretnutia osloví aj osobu staršiu, ktorá sa javí byť dieťaťom mladším ako pätnásť rokov.[127] V praxi tak môže nastať situácia, kedy bude konanie páchateľa, ktorý kontaktuje pätnásť ročnú osobu, za účelom výroby detskej pornografie považované za beztrestné. Kontaktovanie dieťaťa by totiž nemuselo byť považované za dostatočné, aby naplnilo pokus trestného činu výroby alebo iného nakladania s detskou pornografiou. V tomto ohľade nie je v súčasnosti k dispozícii žiadna judikatúra, ktorá by dané konanie posúdila.

Pre vyvodenie trestnoprávnej zodpovednosti páchateľa je nevyhnutné, aby bolo v rámci trestného konania objasnené, akého sexuálne motivovaného trestného činu sa páchateľ v čase učinenia návrhu stretnutia zamýšľal dopustiť.[128]

Dané ustanovenie popisuje fenomén tzv. **kybergroomingu**, ktorý označuje konanie páchateľa, pri ktorom sa, častokrát s nekalými úmyslami, systematicky snaží budovať dôveru s dieťaťom na internete s cieľom získať jeho citlivé informácie alebo ho zaťahovať do sexuálne explicitných situácií. Táto forma kybernetickej manipulácie môže byť využitá na sexuálne vykorisťovanie alebo zneužívanie detí online.[129] Podľa stránok polície je kybergrooming úzko spojený s trestným činom zvádzania k pohlavnému styku (§ 202 trestného zákonníku). Páchatelia

---

[126] ŠČERBA, F. *Posuzování případů zneužívání dětí prostřednictvím internetu k pornografickým účelům*. In Trestněprávní revue, 2020, č. 3, s. 125-129 [online]. [cit. 2023-06-22]. Dostupné z: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=nrptembsgbpxi4s7gnpxgxzrgi2q&groupIndex=1&rowIndex=0&refSource=search.

[127] Toto obmedzenie rozsahu pôsobnosti daného ustanovenia vychádza z článku 6 2011/92/EÚ z 13. decembra 2011, ktoré nedosiahlo vek, v ktorom je spôsobilé dať súhlas na pohlavný styk.

[128] Uznesenie Najvyššieho súdu zo dňa 25. 11. 2020, sp. zn. 8 Tdo 1041/2020.

[129] Definícia pojmov vychádza zo správy *Cyber-Bullying and online Grooming: helping to protect against the risks* od Európskej agentúry pre bezpečnosť sietí a informácií (ENISA), ktorá je dostupná na: https://www.enisa.europa.eu/publications/Cyber-Bullying%20and%20Online%20Grooming/@@download/fullReport

oslovujú obete na sociálnych sieťach a v rámci komunikačných programov, snažiac sa ich presvedčiť k obnažovaniu pred webkamerou, erotickému samoukájaniu a nakoniec im ponúkajú odmenu za pohlavný styk.[130]

2.12. Ďalšie spôsoby páchania trestných činov v súvislosti so šírením pornografie

Technologický pokrok a rozvoj sociálnych sieti zmenil a rozšíril možnosti páchania rôznych foriem zákonom zakázaného sexuálne motivovaného konania. S rozvojom internetu sa postupne objavujú nové hrozby voči sexuálnemu súkromiu obete. Pojem sexuálne súkromie predstavuje podľa Daniella Keatsa Citrona právo jednotlivca slobodne rozhodovať o svojom intímnom živote. Právo na sexuálne súkromie v sebe zahŕňa možnosť jednotlivca rozhodnúť sa o tom, či zverejní alebo nezverejní obsah, ktorý vyobrazuje napríklad častí jeho obnaženého tela a intímnych činností, vrátane pohlavného styku jednotlivca, v prostredí internetu. S ohľadom na vývoj spoločnosti v tejto oblasti a zvyšujúcej sa informovanosti obetí sa sexuálne súkromie čoraz viac dostáva do hľadáčiku právnej vedy a tvorcov legislatívy v rozvinutejších častiach sveta.

K rozvoju verejnej diskusie v tejto oblasti prispelo hnutie #MeToo, ktoré vzniklo v roku 2017 ako reakcie žien po prevalení obvinení amerického filmového producenta Harveyho Weinsteina zo sexuálneho zneužívania. Hnutie #MeToo začalo ako spontánne virálne šírenie hashtagu #MeToo na sociálnych sieťach, ktoré predstavovalo verejné priznanie prevažne žien, ktoré sa vo svojom živote stretli s istou formou sexuálneho zneužívania.[131] Za nové formy sexuálne motivovaného konania môžeme označiť nekonsenzuálnu pornografiu, ktorá býva v odbornej právnej literatúre označovaná ako zneužívanie založené na obrázkoch s sexuálnym obsahom (angl. *image based sexual abuse*), niekedy tiež ako pornografia z pomsty (angl. *revange porn*“), sexting alebo virtuálny sexuálny styk.[132]

2.12.1. Nekonsenzuálna pornografia

Šírenie nekonsenzuálnej pornografie, predstavuje šírenie pornografického diela, ktorého obsahom je intímne vyobrazenie inej osoby, bez jej slobodného a dobrovoľného súhlasu.[133] Už zo samotného názvu je zrejmé, že sa bude jednať o prípady, kedy osoba dobrovoľne zašle svoje

[130] Porov. príspevok Polície Českej republiky ohľadom zneužívania detí na internete, dostupný na: https://www.policie.cz/clanek/zneuzivani-deti-na-internetu.aspx.
[131] Porov. napr. článok na portále Forbes s názvom *Sexual Harassment In The Workplace.* In A #MeToo World Forbes, dostupný na: https://www.forbes.com/sites/forbeshumanresourcescouncil/2017/12/20/sexual-harassment-in-the-workplace-in-a-metoo-world/?sh=18b083135a42
[132] Porov. MCGLYNN, C., RACKLEY, E. *Image-based sexual abuse. Oxford Journal of Legal Studies*, 37 (3). pp. 534-561. ISSN 0143-6503. Dostupné také online z: https://kar.kent.ac.uk/76541/1/20260.pdf.
[133] CITRON, D. K. *Sexual Privacy. The Yale Law Journal*. 2018-2019, roč. 128, 7 s. (1924). In Yale Journal [online]. [cit. 2023-06-23]. Dostupné z: https://www.yalelawjournal.org/article /sexual-privacy.

intímne fotografie alebo videa a tieto sa dostanú do dispozičnej sféry inej osoby, ktorá sa rozhodne z akéhokoľvek motívu prípadne nejakého pomstychtivého dôvodu tieto fotografie alebo videa zdieľať, bez súhlasu s inými osobami, ktorým neboli prvotne určené.

Zneužívanie založené na obrázkoch so sexuálnym obsahom (angl. *image based sexual abuse*) je podmnožinou nekonsenzuálnej pornografie, ktoré označuje vytváranie, distribúciu alebo hrozbu distribúcie nahých alebo sexuálne motivovaných obrázkov bez súhlasu vyobrazenej osoby. Zneužívanie založené na obrázkoch s sexuálnym obsahom, zahŕňa tri hlavné formy správania. Prvou je nekonsenzuálne vytváranie nahého alebo inak sexuálne motivovaného obsahu, vrátane digitálne upraveného alebo manipulovaného obsahu, kde sa tvár osoby pridáva k existujúcemu nahému alebo sexuálnemu obsahu. Druhou formou je nekonzistentné šírenie tohto obsahu bez súhlasu vyobrazenej osoby, a treťou je hrozba distribúcie takéhoto obsahu.[134] Rozvoj v oblasti zneužívania založeného na obrázkoch so sexuálnym obsahom nastal s rozširovaním funkcionalít komunikačných zariadení, ktoré postupom času umožnili odosielanie obrázkov a videí, a tým došlo ku vzniku fenoménu sextingu, teda posielania sexuálne motivovaných správ.

Sexting je termín, ktorý označuje spôsob komunikácie, pri ktorom dochádza k odosielaniu sexuálne explicitných správ, fotografií alebo videí prostredníctvom mobilných telefónov alebo iných elektronických zariadení, obvykle medzi partnermi alebo známymi. Jeho história súvisí s rozvojom mobilných technológií a populárnym využívaním smartfónov a sociálnych médií.[135] Trend sextingu začal naberať na sile v priebehu poslednej dekády, kedy sa technológie stali bežným prostriedkom komunikácie. Tento jav bol často spojovaný s rôznymi aspektami, vrátane zmien v správaní a vzorcoch medziľudských vzťahov v digitálnom veku. Vedecké štúdie a výskumy sa začali zameriavať na sexting, skúmajú jeho dopady na jednotlivcov a spoločnosť, a riešia právne a etické otázky s tým spojené.[136]

---

[134] Definícia vychádza z výročnej správy Austrálskeho inštitútu pro kriminológii s názvom *Trends & issuesin crime and criminal justice*, ISSN 0817-8542, ktorá bola publikovaná v marci 2019 austrálskou vládou. In AIC [online]. [cit. 2023-06-23]. Dostupné z: https://www.aic.gov.au/sites/default/files/2020-05/imagebased_sexual_abuse_victims_and_perpetrators.pdf.

[135] Porov. napr. BARRENSE-DIAS, Y., BERCHTOLD, A., SURÍS J. C., AKRE C. *Sexting and the Definition Issue*. In J Adolesc Health [online]. [cit. 2023-06-23]. Dostupné z: https://pubmed.ncbi.nlm.nih.gov/28734631/.

[136] Napríklad vo výskume španielskych dospelých, ktorý uskutočnili Gámez-Guadix a kolegovia (2015), jedno percento respondentov uviedlo, že niekto šíril alebo nahral na internet fotografie alebo videá s erotickým alebo sexuálnym obsahom bez ich súhlasu, pričom sa pre mužov a ženy vykazovali pomerne podobné percentá.. Dostupná na: GÁMEZ-GUADIX M., SANTISTEBAN P., RESETT S. *Sexting among Spanish adolescents: Prevalence and personality profiles*. In Psicothema [online]. [cit. 2023-06-24]. Dostupné z: https://pubmed.ncbi.nlm.nih.gov/28126055/. V národne reprezentatívnom prieskume obyvateľov Spojených štátov vo veku 15 rokov a starších Lenhart, Ybarra a Price-Feeney (2016) zistili, že tri percentá žien a dva percentá mužov uviedlo, že niekto zverejnil ich fotografiu online bez ich súhlasu. Analýza je dostupná na: https://datasociety.net/wp-content/uploads/2016/11/Online_Harassment_2016.pdf.

Za posledné roky sa celosvetovo zvýšilo povedomie verejnosti venované zneužívaniu založenému na obrázkoch, ako dokazujú verejné konzultácie, reformy trestného práva, pozornosť médií a aj iné navrhované alebo prijaté právne a neprávne opatrenia v rôznych právnych oblastiach. Podľa výskumu vykonaného v Španielsku jedno percento respondentov uviedlo, že niekto šíril alebo nahral na internet fotografie alebo videá s erotickým alebo sexuálnym obsahom bez ich súhlasu.[137] V roku 2014 bolo na webovej stránke so sídlom v USA zverejnených stovky súkromných a intímnych snímok verejne známych osôb. Snímky boli odcudzené prostredníctvom prelomenia bezpečnosti cloudového úložiska iCloud od spoločnosti Apple (online platformy na zálohovanie fotografií z Mac a iPhone zariadení). Tieto obrázky boli následne šírené prostredníctvom sociálnych sieti, vrátane Twitteru (dnešný X), Tumblr a Reddit.[138] Podobne v júni 2015 bolo v Spojených štátoch zverejnených viac ako 400 obnažených snímok žien a dievčat z Južnej Austrálie na webovej stránke so sídlom bez súhlasu týchto osôb. Snímky boli nahrané partnermi, bývalými partnermi alebo hackermi a boli k dispozícii na stiahnutie pre ostatných používateľov.[139]

Aktuálne znenie trestného zákonníka neobsahuje explicitnú skutkovú podstatu, ktorá by postihovala konanie páchateľa v súvislosti so šírením nekonsenzuálnej pornografie alebo s tzv. *image based sexual abuse*, pokiaľ by šírené obrázky nevyobrazovali dieťa, osobu ktorá svojím vzhľadom pripomína dieťa alebo by pornografické dielo vyobrazovalo násilie, neúctu k ľuďom alebo ktoré by opisovalo, zobrazovalo alebo inak znázorňovalo pohlavný styk so zvieraťom.

Toto konanie páchateľa nie je možné považovať za beztrestné. Konanie, pri ktorom osoba rozširuje bez súhlasu dotknutej osoby jej intímne fotografie, mohlo naplniť niekoľko skutkových podstát trestných činov, a to v závislosti na určitých špecifikách konania páchateľa. Za najvhodnejšie považujeme uvažovanie o naplnení skutkovej podstaty trestného činu poškodzovania cudzích práv (§ 181 trestného zákonníka).

---

[137] GÁMEZ-GUADIX M., SANTISTEBAN P., RESETT S. *Sexting among Spanish adolescents: Prevalence and personality profiles*. In Psicothema [online]. [cit. 2023-06-24]. Dostupné z: https://pubmed.ncbi.nlm.nih.gov/28126055/.

[138] Porov. napr. článok *Apple confirms accounts compromised but denies security breach* z roku 2014. In Bbc.com [online]. [cit. 2023-06-24]. Dostupné z: https://www.bbc.com/news/technology-29039294.

[139] CLEARY, B. 'It's outrageous we can't identify them': Lack of action over illegal posting of 400 nude photos of women online angers victims. In Dailymail.co.uk [online]. [cit. 2023-11-16]. Dostupné z: https://www.dailymail.co.uk/news/article-3601202/Lack-action-posting-400-nude-photos-South-Australian-women-leaked-online-angers-victims.html.

2.12.2. Trestný čin poškodzovania cudzích práv v kontexte šírenia nekonsenzuálnej pornografie (§ 181 trestného zákonníka)

Skutková podstata trestného činu poškodzovania cudzích práv je upravená v § 181 trestného zákonníka. Jej trestnosť spočíva v protiprávnom konaní páchateľa, ktorý uvedie niekoho do omylu alebo takýto omyl využije, a tým spôsobí vážnu ujmu na právach obete trestného činu.[140] Predmet ochrany tohoto ustanovenia spočíva v ochrane iných než majetkových práv jednotlivca.[141] Okruh chránených práv nie je zákonom bližšie špecifikovaný. Judikatúrou bolo dovodené, že sa môže jednať o práva v oblasti rodinných vzťahov, pracovných vzťahov, osobnostných práv a tak pod. Rozdelenie majetkových a nemajetkových práv je pritom rozhodujúce pre správne rozlíšenie tohto trestného činu od trestného činu podvodu, ktorý cieli na ochranu majetkových práv osôb.

Z textácie zákona vyplýva že je ochrana poskytovaná len v prípade ich závažnejších porušení. To či dané konanie páchateľa môžeme posúdiť ako trestný čin poškodenia cudzích práv je nutné posúdiť so zreteľom k okolnostiam konkrétneho prípadu. Súd by mal posúdiť to, aké právo obete trestného činu bolo poškodené, v akej oblasti spoločenských vzťahov a predovšetkým to, akú intenzitu dosahoval škodový následok konania páchateľa.[142] Samotný priebeh konania spáchaného páchateľom musí mať povahu podvodného konania. To znamená, že páchateľ zámerne používa klamlivé informácie, či už verbálne alebo neverbálne, s cieľom manipulovať s inými osobami, a tým uviesť tieto osoby do omylu. Páchateľ týmto spôsobom vytvára falošný dojem alebo mylné povedomie u iných osôb, s cieľom ovplyvniť ich rozhodnutia alebo konanie.[143]

V prostredí internetu je možné trestný čin poškodzovania cudzích práv spáchať prostredníctvom šírenia protiprávneho obsahu, ktorý vo svojej podstate poškodzuje práva tretej osoby takým spôsobom, že toto šírenie spôsobuje závažnú ujmu na nemajetkových právach osoby poškodeného alebo tretej osoby. Za vážnu ujmu na právach jednotlivca považujeme porušenie práv na intimitu, súkromie, zachovanie cti, ľudskej dôstojnosti a dobrej povesti.

V súvislosti so šírením pornografie môžeme podľa autora diplomovej práce o tejto skutkovej podstate uvažovať v dvoch prípadoch. Jednak k v prípade kedy osoba zneužije omyl tretej osoby a bez jej vedomia vyhotoví alebo iným spôsobom získa prístup k sexuálne explicitnému obsahu alebo takýto obsah získa priamo od tretej osoby s jej vedomím, ale použije ho k iným, ako treťou osobou stanoveným účelom.

[140] Porov. § 181 trestného zákonníka.
[141] ŠÁMAL, P, ŠKVAIN, Petr. § 181 [Poškození cizích práv]. In: ŠÁMAL. 2023, op. cit., s. 2277, marg. č. 1.
[142] Uznesenie Najvyššieho súdu zo dňa 14. 7. 2015, sp. zn. 4 Tdo 843/2015.
[143] Porov. § 181 trestného zákonníka.

Prvé konanie teda predstavuje situáciu, kedy sa páchateľ k „pornografickému“ materiálu dostal bez vedomia vyobrazenej osoby. Jednak v situácii, kedy sa neoprávnene dostane k záznamom, ktoré vyhotovila obeť alebo záznam sám vytvorí. Obdobným prípadom sa zaoberal Najvyšší súd, ktorý vo svojom rozhodnutí posudzoval konanie páchateľa, ktorý v rokoch 2007 až 2013 bez vedomia a súhlasu jeho nájomcov nainštaloval skryté kamery v ich kúpeľni za zrkadlom, sledujúc ich v intímnych situáciách, za účelom vlastného sexuálneho uspokojenia. Súd hodnotil toto konanie ako prečin poškodenia cudzích práv podľa § 181 ods. 1 písm. a) trestného zákonníka, pričom páchateľ podľa rozsudku využil alebo uviedol do omylu poškodených pri neoprávnenom získavaní záznamu, čím zásadne zasiahol do práva na ochranu súkromia.[144]

Ďalším príkladom konaní, ktoré by mohli naplniť skutkovú podstatu uvedeného trestného činu je situácia, pri ktorej páchateľ využije lesť k získaniu prístupu do zariadenia, v ktorom sú uložené súkromné záznamy. Pre predstavu sa môže jednať o situáciu, kedy si páchateľ od poškodenej vyžiada telefón, s úmyslom zavolať si a bez jej vedomia si z galérie odošle nahé fotografie. Druhým príkladom môže byť konanie páchateľa, ktorý si po pohlavnom styku vyfotí nahú družku počas sprchovania. Tieto konania, predstavujú zásah do práva na súkromie vyobrazenej osoby a to, či toto konanie dosahuje zákonom požadovanej intenzity bude závisieť na okolnostiach konkrétneho prípadu, a to s ohľadom na motiváciu páchateľa a jeho ďalšie nakladanie s takýmto obsahom.

Druhou situáciou je situácia, kedy páchateľ získal pornografické dielo s vedomím vyobrazenej osoby, ktorá mu dielo sprístupnila napríklad v rámci vyššie zmieneného sextingu. Poškodenie práva na súkromie a jeho novo definovanou podmnožinou práva na sexuálne súkromie predstavuje konanie páchateľa, ktorý uvedie poškodenú osobu do omylu, ktorá explicitné záznamy zdieľa s vedomím toho, že zostanú v dispozičnej sfére adresáta. Podľa rozhodnutia Najvyššieho súdu bude trestným činom poškodzovania cudzích práv predstavovať situácia, pri ktorej páchateľ zdieľa intímne fotografie, vyhotovené so súhlasom vyobrazenej osoby bez jej vedomia na sociálnej sieti. V predmetnom prípade odsúdený neoprávnene vytvoril pod menom a priezviskom poškodenej J. T. profil na sociálnej sieti Facebook. Tento profil obsahoval intímne fotografie poškodenej, ktoré vyhotovil s jej súhlasom, a tie boli sprístupnené vybraným používateľom v režime „priatelia“ bez vedomia poškodenej.[145]

Isté špecifiká pri konaní páchateľa môžu nad rámec porušovania cudzích práv v jednočinnom alebo viacčinnom súbehu naplniť skutkovú podstatu trestného činu porušenia

[144] Uznesenie Najvyššieho súdu zo dňa 14. 7. 2015, sp. zn. 4 Tdo 843/2015.
[145] Uznesenie Najvyššieho súdu zo dňa 14. 5. 2015, sp. zn. 4 Tdo 815/2014-37.

tajomstva dopravovaných správ (§ 182 trestného zákonníka), porušenie tajomstva dokumentov a iných dokumentov uchovávaných v súkromí (§ 183 trestného zákonníka) a pri istých špecifických situáciách aj trestných činov vydierania (§ 175 trestného zákonníka) a sexuálneho nátlaku (§ 186 trestného zákonníka). Problematické je aj stanovenie mieri zodpovednosti poskytovateľov digitálnych služieb, prostredníctvom ktorých sa protizákonný obsah šíri.

3. Trestnoprávna zodpovednosť poskytovateľov služieb informačných spoločností za šírenie protiprávneho obsahu

V otázkach zodpovednosti za šírenie protiprávneho obsahu sa naskytá otázka, akým spôsobom je zodpovedná osoba, ktorá prostredníctvom svojej činnosti umožňuje rozširovať protiprávny obsah, bez toho aby to činila priamo. V tomto prípade hovoríme o zodpovednosti poskytovateľov služieb informačných spoločností.

Jedným z prvých zaznamenaných porušení poskytovateľov služieb informačných spoločností je spor o technológiu Betamax americkej spoločnosti Sony Corp. Betamax predstavoval systém určený pre ukladanie záznamu obrazu a zvuku, ktorý bol dostupný pre spotrebiteľov a je považovaný za predchodcu technológie VHS. Jeho uvedeniu na trh sa snažili zabrániť veľké filmové štúdia, ktoré v technológii videli potenciálne ohrozenie ich autorských práv, vzhľadom k tomu, že technológia umožnila nahrávanie televízneho záznamu a jeho následné rozširovanie. V uvedenom prípade súd dospel k záveru, že nie je možné vyvodzovať zodpovednosť dodávateľa technológie len z toho hľadiska, že daná technológia môže byť teoreticky zneužitá na protiprávne účely.[146] Rozhodnutie vo veci Sony sa stalo precedentným rozhodnutím pre komerčné využívanie technológii. Základný princíp rozhodnutia Sony sa však postupne začal uplatňovať aj v prípadoch nekomerčných technológií a dokonca v situáciách, kde nešlo o výrobu a dodávky konkrétnej technológie, ale o poskytovanie technologických služieb. Argumentácia z tohto prípadu sa dodnes analogicky uplatňuje vo sporoch, týkajúcich sa porušovania práv používateľov voči poskytovateľom služieb informačnej spoločnosti.[147]

V ďalšej časti vymedzujeme (trestnoprávnu) zodpovednosť poskytovateľov služieb informačných spoločností[148] ako osôb, ktoré sami protiprávny obsah nerozširujú ale prevádzkujú

[146] Porov. rozhodnutie Najvyššieho súdu Spojených štátov vo veci *Sony Corp. of America v. Universal City Studios*, Inc., 464 U.S. 417 (1984). In Supreme.justia.com [online]. [cit. 2017-11-30]. Dostupné z: https://supreme.justia.com/cases/federal/us/464/417/

[147] JOSTAŠ, P., KASL, F., KYSELOVSKÁ, T., LECHNER, T., LOUTOCKÝ, P., MÍŠEK, J., MYŠKA, M., POLČÁK, R., STUPKA, V., TOMÍŠEK, J., UŘIČAŘ, M. *Právo informačních technologií*. [Systém ASPI]. Wolters Kluwer (dříve ASPI). ASPI_ID MN328CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

[148] Definícia je obsiahnutá v ďalšej časti diplomovej práce.

službu, ktorá umožňuje prostredníctvom nej užívateľom obsah šíriť. Regulácia služieb informačných spoločností prechádza v čase písania tejto diplomovej práce novelizáciou, ktorá do značnej miery ovplyvní poňatie zodpovednosti poskytovateľov. Diplomová práca preto v úvode tejto kapitoly popisuje aktuálnu právnu úpravu, hodnotí jej nedostatky a v širšej miere rozoberá zodpovednosť poskytovateľov služieb informačných spoločností podľa novo schválenej právnej úpravy.

3.1. Vymedzenie základných pojmov

Službou informačných spoločností je akákoľvek služba, ktorá je poskytovaná prevažne úplatne, a to prostredníctvom elektronických prostriedkov na základe individuálnej žiadosti používateľa. Služba je poskytnutá elektronickými prostriedkami, ak je odoslaná cez elektronickú komunikačnú sieť a používateľ k nej môže získať prístup zo svojho elektronického zariadenia. V tomto kontexte výraz „*elektronickými prostriedkami*" predovšetkým zahŕňa sieť elektronických komunikácií, elektronické komunikačné zariadenia, systémy na automatické volanie a komunikáciu, telekomunikačné koncové zariadenia a elektronickú poštu. Tieto prostriedky slúžia na prenos elektronických informácií a umožňujú interakciu a komunikáciu medzi používateľmi. Vzhľadom na zameranie tejto diplomovej práce sa jej text ďalej zameriava na šírenie predovšetkým prostredníctvom sietí elektronických komunikácii, elektronických komunikačných zariadení a elektronickú poštu.[149]

Siete elektronických komunikácii sú definované v samostatnom právnom predpise, v zákone o elektronických komunikáciách. Jedná sa o pomerne komplexný pojem, ktorý zahŕňa široké spektrum prenosových systémov, bez ohľadu na to, či sú založené na trvalých infraštruktúrach alebo sú centralizovane riadené kapacitou, a to vrátane fyzickej siete, ktorá umožňuje prenos signálov pomocou vedení, rádiových, optických alebo iných elektromagnetických prostriedkov. Do tohto širokého pojmu patria aj družicové siete, pevné okruhové alebo paketové siete vrátane internetu, mobilné siete, siete využívané na prenos signálov elektrickej energie (ak sa používajú na tieto účely), siete pre rozhlasové a televízne vysielanie a káblová televízia.

Poskytovateľom služby informačných spoločností[150] je definovaná každá fyzická alebo právnická osoba, ktorá poskytuje niektorú zo služieb informačnej spoločnosti, vrátane služieb

[149] Porov. § 2 ods. 1 písm. a) ZSIS.
[150] Pre zjednodušenie je tento pojem ďalej v diplomovej práci zovšeobecnený ako poskytovatelia internetových služieb alebo poskytovatelia digitálnych služieb.

sprostredkovateľských.[151] **Užívateľom služieb informačných spoločností** je každá fyzická alebo právnická osoba, ktorá využíva službu informačnej spoločnosti, najmä za účelom šírenia a ukladania informácií.[152]

3.2. Relevantná právna úprava

Pokiaľ ide o práva a povinnosti poskytovateľov služieb informačných spoločností, je základným právnym predpisom zákon č. 480/2004 Sb., o niektorých službách informačnej spoločnosti a o zmene a doplnení niektorých zákonov (ďalej tiež ako „**ZSIS**“). Tento zákon bol prijatý z dôvodu potreby transpozície právnych predpisov Európskej únie do právneho poriadku Českej republiky. Išlo predovšetkým o transpozíciu smernice o elektronickom obchode a smernice o súkromí a elektronických komunikáciách.[153] ZSIS postupom času obsiahol aj implementáciu ďalších právnych predpisov predovšetkým z oblasti online sprostredkovateľských služieb.

Smernica o elektronickom obchode[154] predstavuje základný právny rámec pre online služby v Európskej únii. Jej primárnym cieľom je snaha odstrániť prekážky, ktoré by bránili cezhraničnému poskytovaniu služieb informačných spoločností. Práva a povinnosti poskytovateľov služieb informačných spoločností sú upravené podľa tzv. princípu krajiny pôvodu, na základe ktorého podliehajú regulácii toho členského štátu, na ktorého území majú svoje sídlo.[155] Okrem otázok zodpovednosti poskytovateľov služieb informačných spoločností reguluje smernica aj oblasť nevyžiadaných obchodných oznámení (tzv. spam), informačnú povinnosť poskytovateľov, uzatváranie zmlúv elektronickou cestou a tak ďalej.

V oblasti zodpovednosti poskytovateľov služieb informačných spoločností a sprostredkovateľských služieb smernica stanovuje konkrétne pravidlá, na základe ktorých zodpovedajú poskytovatelia internetových služieb za obsah tretích osôb (užívateľov), ktorý je šírený prostredníctvom nimi poskytovaných služieb. Poskytovatelia internetových služieb, ktorí pôsobia v oblasti poskytovania služieb jednoduchého prenosu (tzv. *mere conduit*), ukladania do vyrovnávacej pamäte - kešing (angl. *caching*) alebo zhromažďovania informácií - hosting (angl. *hosting*), nenesú zodpovednosť za informácie, ktoré prenášajú alebo zhromažďujú, v prípade ak splnia podmienky podľa čl. 12, 13 a 14 smernice. Táto časť smernice bola do ZSIS transponovaná

[151] Porov. § 2 ods. 1 písm. d) ZSIS.
[152] Porov. § 2 ods. 1 písm. e) ZSIS.
[153] Konkrétne zákon transponoval články 3, 7, 8, 11, 12, 13, 14, 15 a niektoré časti článkov 5, 6, 10 a 19 smernice.
[154] Smernica 2000/31/ES Európskeho parlamentu a Rady z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode. V ďalších častiach diplomovej práce len smernica o elektronickom obchode.
[155] Porov. čl. 3 smernice o elektronickom obchode.

v paragrafoch 3 až 6.[156] Cieľom daných ustanovení nie je v žiadnom prípade stanoviť poskytovateľom internetových služieb všeobecnú monitorovaciu povinnosť nimi prenášaných alebo ukladaných informácií. Poskytovatelia internetových služieb nemusia prijímať aktívne opatrenia s cieľom vyhľadávať protiprávny obsah, ktorý je šírený prostredníctvom nimi poskytovaných služieb.[157] Aj keď zákon v tomto prípade nehovorí priamo o zodpovednosti trestnej ale vymedzuje ju len všeobecne, môžeme dovodiť na základe zásady subsidiarity trestnej represie, že pokiaľ nenesie poskytovateľ zodpovednosť podľa ZSIS, nie je možné ju vyvodiť ani z predpisov v oblasti trestného práva.

Poskytovatelia služieb jednoduchého prenosu (*mere conduit*), ktoré umožňujú šírenie informácií prostredníctvom sieti elektronických komunikácií (internetu) zodpovedajú za ich obsah v prípade ak dané šírenie sami iniciujú, určia jeho adresáta alebo obsah prenášanej informácie zmenia.[158] Z uvedeného môžeme konštatovať, že súčasná právna úprava vylučuje akúkoľvek zodpovednosť poskytovateľov služieb jednoduchého prenosu za konanie tretích osôb, pokiaľ svojou činnosťou nezasahujú do činnosti používateľov, ale poskytujú len infraštruktúru na prenos dát.[159]

Dané ustanovenie je implementáciou článku 12 smernice o elektronickom obchode. Súdny dvor sa k výkladu rozsahu článku 12, najmä s dôrazom na základné práva, zaoberal v prípade *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH*, v ktorom rieši mimo iného otázku, za akých okolností, a do akej miery môžu byť prevádzkovatelia verejne prístupných Wi-Fi sietí zodpovední za porušenia autorských práv, a aké opatrenia môžu byť proti nim uložené. Tobias Mc Fadden poskytol svoju Wi-Fi sieť verejnosti, a jej prostredníctvom došlo k protiprávnemu stiahnutiu hudby chránenej autorským právom spoločnosti Sony. Prípad sa prostredníctvom Krajinského súdu v Mníchove, položením predbežných otázok, dostal k súdnemu dvoru EÚ. K otázke rozsahu zodpovednosti sprostredkovateľa služieb sa súd vyjadruje v štvrtej a piatej predbežnej otázke. V rozsudku súd rozhodol, že poskytovateľ verejnej prístupnej Wi-Fi siete je poskytovateľom služieb informačnej spoločnosti, a teda na neho dopadajú všetky zákonom stanovené povinnosti v oblasti zodpovednosti za protiprávny obsah, ktorý je prostredníctvom jeho

[156] Vzhľadom na to, že od 17. februára 2024 nadobudne účinnosť priamo použiteľné nariadenie o digitálnych službách (pozri ďalej) práca tieto pojmy definuje na základe novoprijatých právnych predpisov. V tejto časti sa vymedzuje len na základný popis aktuálne platného právneho stavu v oblasti zodpovednosti poskytovateľov internetových služieb, pričom sa snaží poukázať na zásadné rozdiely ktoré prinesie nová právna úprava oproti stávajúcej.
[157] Porov. § 6 ZSIS.
[158] Porov. § 3 ods. 1 ZSIS.
[159] JOSTAŠ, P., KASL, F., KYSELOVSKÁ, T., LECHNER, T., LOUTOCKÝ, P., MÍŠEK, J., MYŠKA, M., POLČÁK, R., STUPKA, V., TOMÍŠEK, J., UŘIČAŘ, M. *Právo informačních technologií*. [Systém ASPI]. Wolters Kluwer (dříve ASPI) [cit. 2023-11-4]. ASPI_ID MN328CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

siete šírený. Súd konštatoval, že článok 12 smernice o elektronickom obchode treba vykladať v tom zmysle, že „*bráni tomu, aby osoba, ktorej práva k dielu boli porušené, mohla od poskytovateľa prístupu požadovať náhradu škody z dôvodu, že jeden z týchto prístupov bol použitý treťou osobou na porušenie jej práv. Naopak, toto ustanovenie treba vykladať v tom zmysle, že nebráni tomu, aby táto osoba požadovala uloženie povinnosti zdržať sa konania s ohľadom na toto porušenie, ako aj náhrady nákladov na výzvu a trov konania voči poskytovateľovi prístupu do komunikačnej siete, ktorého služby boli použité na dopustenie sa tohto porušenia, ak sa tieto návrhy týkajú alebo nasledovali po vydaní príkazu orgánom alebo vnútroštátnym súdom, ktorým sa zakazuje tomuto poskytovateľovi umožňovať dané porušovanie*“.[160] Z uvedeného vyplýva, že aj keď poskytovateľ služby obyčajného prenosu nezodpovedá za ním prenášaný obsah, stále môže byť zo strany súdu požiadaný o obmedzenie poskytovania služby, ktorá porušuje práva tretej osoby. Toto rozšírenie pojmu poskytovateľ služieb obyčajného prenosu na poskytovateľov verejnej Wi-Fi siete vyvolalo značnú diskusiu.[161]

Poskytovatelia služieb kešingu, ktorí umožňujú prenos informácií a ich dočasné medziukladanie zodpovedajú za tento obsah len v prípade, ak akýmkoľvek spôsobom obsah informácie zmenia, alebo v prípade, ak ani na základe uloženého opatrenia nepristúpia k znemožneniu prístupu k nemu.[162] Zodpovednosť poskytovateľov služieb kešingu v rámci práva informačných a komunikačných technológií zatiaľ nepredstavuje široko diskutovaný problém, a to prevažne z praktického hľadiska, kedy sa jedná len o dočasné medziuloženie.

Poskytovatelia služieb hostingu, ktoré spočívajú vo ukladaní obsahu užívateľov zodpovedajú za jeho obsah len v prípade, ak mohli vzhľadom k predmetu svojej činnosti a okolnostiach daného prípadu vedieť, že je obsah protiprávny, alebo v prípade, ak sa preukázateľne o protiprávnosti dozvedeli v právnom konaní v súvislosti s uloženými informáciami, ale ani vzhľadom k tomu, nepodnikli všetky kroky, ktoré bolo možné od nich požadovať k odstráneniu alebo zneprístupneniu daného obsahu.[163] Dané ustanovenie implementuje čl. 14 ods. 1 smernice o elektronickom obchode, podľa ktorého informačné spoločnosti, ktoré poskytujú služby ukladania obsahu nezodpovedajú za obsah uložený užívateľmi v prípade, ak si neboli vedomí protiprávnosťou činnosti, a hneď ako sa o tomto dozvedeli, jednali s cieľom odstrániť tento obsah,

[160]Rozsudok Súdneho dvora EU zo dňa 16.9.2016, vec C-484/14. Dostupné na: https://curia.europa.eu/juris/document/document.jsf?text=&docid=183363&pageIndex=0&doclang=SK&mode=lst&dir=&occ=first&part=1&cid=2510084.
[161] Porov. napr. blog JÜTTE J., *Limited liability for free Wi-Fi access (Case C-484/14, Mc Fadden v Sony Music)*. In Europeanlawblog.eu [online]. [cit. 2023-07-10]. Dostupné z: https://europeanlawblog.eu/2016/03/31/limited-liability-for-free-wi-fi-access-case-c-48414-mc-fadden-v-sony-music/.
[162] Porov. § 4 ods. 1 ZSIS.
[163] Porov. § 5 ods. 1 ZSIS.

alebo znemožniť k nemu prístup. Jedná sa o uplatnenie princípu bezpečného prístavu (*angl. safe harbour),* na základe ktorého poskytovatelia pri uplatnení vymedzených povinností nezodpovedajú za obsah používateľov.[164]

Vzhľadom k tomu, že súčasná právna úprava zodpovednosti poskytovateľov internetových služieb za obsah užívateľov vychádza zo smernice o elektronickom obchode, ktorá bola transponovaná do právneho poriadku Českej republiky pri vstupe do Európskej únie v roku 2004, je už do značnej miery neaktuálna a vyžadovala si potrebu novelizácie. To predovšetkým z dôvodu značného technologického pokroku a vzniku nových technológii, ku ktorým v medzičase došlo.

Jedná sa predovšetkým o vzostup digitálnej ekonomiky, online trhovísk a predovšetkým sociálnych sietí. Tieto nové digitálne technológie sa stali zdrojom doteraz neregulovaných výziev a rizík a potreby lepšej ochrany používateľov. Z tohto dôvodu prijala Európska únia nariadenie o jednotnom trhu s digitálnymi službami, ktoré býva označované ako akt o digitálnych službách alebo anglicky *Digital Service Act*[165] (ďalej tiež ako „**DSA**"). Prijatím DSA došlo k zrušeniu ustanovení smernice o elektronickom obchode, ktoré upravujú zodpovednosť poskytovateľov internetových služieb. Vzhľadom k tomu, že DSA má priamu účinnosť, bude musieť zákonodarca pristúpiť ku zmene ustanovení ZSIS, ktoré vychádzajú zo smernice o elektronickom obchode. V dobe písania tejto diplomovej práce je v legislatívnom procese zákon o digitálnej ekonomike, ktorý by mal mimo iného, zrušiť ZSIS a v otázke zodpovednosti poskytovateľov internetových služieb plne vychádzať z úpravy nariadení DSA. Diplomová práca v ďalšej časti popisuje novo prijatú reguláciu poskytovateľov internetových služieb a to predovšetkým oblasti regulácie obsahu a zodpovednosti.

3.3. Zodpovednosť poskytovateľov internetových služieb podľa aktu o digitálnych službách (DSA)

Rozvoj digitálnej ekonomiky so sebou zákonite priniesol nové výzvy s ním spojené. Jednotlivé členské štáty Európskej únie na tieto výzvy reagovali prijímaním vnútroštátnych právnych predpisov, ktoré subjektom poskytujúcim digitálne služby ukladali povinnosti pre ochranu ich používateľov. Vzhľadom na cezhraničný charakter internetu a jeho vplyv na vnútorný trh Európskej únie by tieto rozdielne vnútroštátne právne predpisy mohli negatívne ovplyvniť

[164] Porov. rozsudky Súdneho dvora z 23. marca 2010 v spojených veciach C-236/08, C-237/08 a C-238/08 Google France SARL a Google Inc. proti Louis Vuitton Malletier SA, Google France SARL proti Viaticum SA a Luteciel SARL a Google France SARL proti Centre national de recherche en relations humaines (CNRRH) SARL a z 12. júla 2011 vo veci C-324/09 L'Oréal SA a i. proti eBay International AG a i.

[165] Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách). V ďalšej časti diplomovej práce len ako DSA.

fungovanie vnútorného trhu v oblasti poskytovania digitálnych služieb. V opačnom extréme by sa bez dostatočnej regulácie poskytovatelia internetových služieb stali *de facto* samoregulátormi. Verejný dozor nad poskytovateľmi internetových služieb je v súčasnosti rozdelený medzi rôznych sektorových regulátorov, akými sú orgány pre dohľad nad spracúvaním osobných údajov, orgány pre ochranu hospodárskej súťaže, elektronických komunikačných služieb a orgány pre ochranu spotrebiteľa.[166] DSA reaguje na tieto výzvy s cieľom zabezpečiť správne fungovanie jednotného trhu v oblasti digitálnych služieb, udržiavania bezpečného online prostredia a ochrany základných práv užívateľov pred negatívnymi dopadmi nezákonného obsahu.[167]

DSA zavádza pre poskytovateľov internetových služieb súbor povinnosti nad rámec smernice o elektronickom obchode. Tieto povinnosti sú stanovené asymetrický podľa charakteru poskytovanej služby a veľkosti jej poskytovateľa. Poskytovatelia, ktorí dosahujú veľkosť mikro a malých podnikov sú z väčšiny povinnosti vyňatí. Naopak poskytovatelia, ktorými sú veľkými podnikmi (predovšetkým veľmi veľké online platformy a veľmi veľké online vyhľadávače) s priemerným počtom mesačných aktívnych používateľov vyšším než 45 miliónov, čo predstavuje 10 percent obyvateľov Európskej únie, majú ďalšie dodatočné povinnosti.

Ako už bolo spomenuté vyššie, smernica o elektronickom obchode si nevyžadovala, aby poskytovatelia internetových služieb aktívne vyhľadávali nezákonný obsah. Nariadenie DSA však už túto povinnosť stanovuje. Konkrétne zavádza povinnosť náležitej starostlivosti, vrátane nutnosti zavedenia postupov pre nahlasovanie a odstraňovanie nezákonného obsahu, a možnosť užívateľov sa proti tomuto rozhodnutiu odvolať. *De facto* týmto ustanovením došlo k zavedeniu povinnosti moderácii obsahu.

3.3.1. Nezákonný obsah

DSA za nezákonný obsah považuje také informácie, ktoré buď samé osebe alebo s odkazom na určitú činnosť, vrátane predaja produktov alebo poskytovania služieb, nie sú v súlade s právnymi predpismi EÚ alebo s právnymi predpismi niektorého členského štátu. To všetko bez ohľadu na predmet alebo povahu týchto právnych predpisov.[168] Podľa ustanovení v recitáli DSA by mal tento pojem plne reflektovať existujúce pravidlá platné pre off-line prostredie.

[166] HOFFMANN, A. a GASPAROTTI, A., *Liability for illegal content online: Weaknesses of the EU legal framework and possible plans of the EU Commission to address them in a 'Digital Services Act.* Marec 2020. In Cep.eu [online]. [cit. 2023-07-12]. Dostupné z: https://www.cep.eu/fileadmin/user_upload/hayek-stiftung.de/cepStudy_Liability_for_illegal_content_online.pdf.
[167] Informácie vychádzajú z recitálu a dôvodovej správy k DSA.
[168] Porov. čl. 2 písm. f) DSA.

Predovšetkým je potrebné tento pojem podľa výkladového ustanovenia v recitáli DSA vykladať tak, že za nezákonné považuje informácie, ktoré sú buď samy osebe nezákonné alebo nezákonné v spojitosti s kontextom v ktorom sa šíria. Táto definícia teda v prvom rade za nezákonný obsah nepovažuje len obsah, ktorý je v rozpore s normami trestného práva, ale ochranu rozširuje aj na obsah, ktorý porušuje právo súkromné, ako napríklad predpisy na ochranu spotrebiteľa alebo ochranu autorských práv. Pre predmet tejto diplomovej práce sa za nezákonný obsah budú považovať napríklad nezákonne vyhotovené snímky so sexuálnym kontextom.

Druhú kategóriou tvorí obsah, ktorý je nezákonný vzhľadom na jeho spojenie s inou nezákonnou činnosťou. Vzhľadom na obsah tejto diplomovej práce sa bude jednať predovšetkým o zdieľanie obrázkov sexuálneho zneužívania detí, nezákonné zdieľanie súkromných snímok bez súhlasu, alebo nepovolené používanie materiálu chráneného autorským právom. Pokiaľ by ale šírený obsah obsahoval videozáznam vytvorený očitým svedkom trestného činu, nemal by byť sám osebe považovaný za nezákonný obsah, len pretože vyobrazuje páchanie trestného činu, to znamená, že na takýto obsah sa nariadenie DSA vzťahovať nebude ak samozrejme, nie je jeho vytvorenie a šírenie v rozpore s právnym poriadkom Českej republiky alebo relevantnými predpismi Európskej únie.[169]

3.3.2. Rozsah pôsobnosti aktu o digitálnych službách (DSA)

Pojem digitálnych služieb nie je v DSA definovaný. Jeho obsah v sebe zahŕňa širokú škálu služieb poskytovaných prostredníctvom internetu, od prevádzkovania jednoduchých webových sídiel po komplexné služby internetovej infraštruktúry a online platformy.[170] Poskytovateľov digitálnych služieb preto môžeme v rozsahu DSA chápať ako poskytovateľov určitých služieb informačnej spoločnosti, t. j. všetky služby, ktoré sa bežne poskytujú za úplatu, na diaľku, elektronicky a na individuálnu žiadosť príjemcu týchto služieb. DSA vo svojom rozsahu nedopadne na všetkých poskytovateľov služieb informačnej spoločnosti ale len na tzv. poskytovateľov sprostredkovateľských služieb. Jedná sa o okruh subjektov, ktoré v rámci svojej činnosti poskytujú fyzickým alebo právnickým osobám možnosť využívať tzv. sprostredkovateľské služby.

Sprostredkovateľským službami ostávajú služby definované v smernici o elektronickom obchode, pričom došlo k rozšíreniu okruhu o poskytovateľov nový digitálnych služieb, ktoré

[169] Porov. recitál 12 DSA.
[170] Dostupné z online informácií ohľadom politiky Európskej únie s názvom balík týkajúci sa aktu o digitálnych službách v rámci stratégie *Shaping Europe's digital future* dostupná online na odkaze: https://digital-strategy.ec.europa.eu/sk/policies/digital-services-act-package.

v čase prijatia smernice ešte neboli tak rozšírené a nepredstavovali potrebu regulácie. Sprostredkovateľskými službami sa v kontexte DSA rozumie služba „*obyčajného prenosu*“, *kešing*“ a služba „*hosting*“,[171] Toto rozdelenie je doležíte z hľadiska uplatnenia zodpovednosti poskytovateľov jednotlivých služieb za obsah.

3.3.3. Zodpovednosť pri poskytovaní služieb obyčajný prenos

Obyčajný prenos predstavuje podľa článku 4 DSA proces, pri ktorom sú údaje, informácie alebo dáta užívateľov[172], ako príjemcov danej služby,[173] presúvané v rámci komunikačnej sieti z jedného miesta siete na druhé, alebo poskytovanie prístupu ku komunikačnej sieti. Môže sa pritom napríklad jednať o prenos dát z jedného počítača na iný, koncového zariadenia užívateľa na koncové zariadenie iného užívateľa, alebo z jedného bodu siete na iný. Obyčajný prenos môže prebiehať prostredníctvom rôznych komunikačných kanálov, ako sú pre predstavu káblové pripojenie, bezdrôtové siete alebo internet. Sprostredkovateľské služby obyčajného prenosu vo svojej definícii zahŕňajú všeobecné kategórie digitálnych služieb, akými sú služby v oblasti poskytovania internetových prepojovacích uzlov, bezdrôtových prístupových bodov, virtuálnych súkromných sietí, služby a prekladače DNS alebo správcovstvo domén.[174]

Vo všeobecnosti platí, že poskytovateľ služby obyčajného prenosu zodpovedá za obsah šírený prostredníctvom ním poskytovaných služieb. DSA ale zavádza súbor podmienok, na základe ktorých sa môžu poskytovatelia služieb obyčajného prenosu zodpovednosti zbaviť. Konkrétne poskytovateľ služieb obyčajného prenosu nezodpovedá za informácie, ktoré sú predmetom prenosu alebo prístupu za splnenia podmienok stanovených v článku 4 ods. 1 DSA. DSA konkrétne zavádza tri výnimky zo zodpovednosti poskytovateľ služieb obyčajného prenosu pokiaľ nie je žiadnym spôsobom zainteresovaný na zdieľaní informácii, ktoré sú predmetom daného prenosu. Predpokladom pre vylúčenie zodpovednosti je teda skutočnosť, že poskytovateľ žiadnym spôsobom neupravuje informácie ktoré prenáša, alebo informácie ku ktorým má z titulu poskytovania služieb prístup. DSA ale ďalej uvádza, že podmienka neupravovania informácii príjemcov služieb neplatí bezvýhradne, ale ponecháva poskytovateľovi služby z praktických dôvodov možnosť manipulácie s informáciami technickej povahy za podmienok, že táto

[171] Porov. recitál 5 DSA.
[172] DSA označuje všetky údaje, informácie alebo dáta užívateľov jednotným pojmom informácie, tento pojem následne používa diplomová práca aj v ďalšej časti tejto kapitoly.
[173] Príjemcom služby sa v zmysle článku 3 DSA rozumie fyzická alebo právnická osoba, ktorá využíva sprostredkovateľskú službu, najmä na účely vyhľadávania alebo sprístupňovania informácií.
[174] Výpočet poskytovaných služieb vychádza z recitálu 29 DSA.

manipulácia nemení integritu informácií, ktoré sú predmetom prenosu, alebo ku ktorým sa poskytuje prístup.

3.3.4. Zodpovednosť pri poskytovaní služieb kešingu

Druhou regulovanou službou je tzv. *kešing* z anglického výrazu *caching*. Kešing predstavuje proces pri ktorom sa dáta alebo informácie príjemcov služby ukladajú do dočasnej pamäte (tzv. kešovacej pamäte) s cieľom zvýšiť rýchlosť a efektivitu prístupu k nim. To znamená, že dáta, ktoré sa často používajú, sú predbežne uložené na mieste, kde sú rýchlo dostupné, čím sa zníži časová náročnosť na načítanie týchto dát z pôvodného miesta. Kešing sa často používa na rôznych úrovniach IT systémov, vrátane webových stránok a databáz.[175] Podľa recitálu k DSA sa bude jednať predovšetkým o digitálne služby, ktoré zahŕňajú výhradné poskytovanie sietí sprístupňovania obsahu, reverzných proxy serverov alebo proxy serverov na úpravu obsahu, jedná sa o súbor služieb, ktorých primárnym účelom je zabezpečenie efektívneho prenosu informácii na internete.[176]

Podobne ako v prípade služieb online prenosu, ani poskytovateľ kešingovej služby nezodpovedá za automatické, dočasné a prechodné uchovávanie informácií používateľov v prípade, ak splní podmienky v článku 5 ods. 1 DSA. Poskytovateľ konkrétne nesmie žiadnym spôsobom zasahovať do obsahu uložených informácii (s výnimkou technického zásahu pre zaistenie splnenia účelu uložených informácii). Zároveň musí poskytovateľ dodržiavať podmienky prístupu k uloženým informáciám. Predovšetkým musí zaistiť výmaz informácii, ak daná informácia bola odstránená z pôvodného zdroja, alebo ak jej odstránenie nariadil k tomu oprávnený štátny orgán.[177]

3.3.5. Zodpovednosť poskytovateľa pri poskytovaní služieb hostingu

Treťou, a zároveň poslednou službou regulovanou v rámci nariadenia DSA sú tzv. služby hostingu. Hosting je služba, pri ktorej poskytovateľ internetovej služby ako tretia strana (hostiteľ) poskytuje serverové zdroje a infraštruktúru na uloženie a sprístupnenie webových stránok, aplikácií alebo informácii. Tieto servery sú spravované a udržiavané poskytovateľom hostingových služieb, čo umožňuje majiteľom webových stránok alebo aplikácií zverejňovať ich online a zabezpečiť ich prístupnosť pre používateľov na celom svete. Hosting môže byť zdieľaný (viacero webstránok zdieľa jeden server), virtuálny (virtuálny server na fyzickom serveri) alebo

[175] Definícia kešingu z portálu TechTarget. In Techtarget.com [online]. [cit. 2023-07-11]. Dostupné z: https://www.techtarget.com/whatis/definition/caching.
[176] Výpočet poskytovaných služieb vychádza z recitálu 29 DSA.
[177] Pre detailnejšie podmienky ohľadom povinností poskytovateľa kešingovej služby porov. čl. 5 DSA.

dedikovaný (celý server pre jednu webovú stránku alebo aplikáciu).[178] Príkladom hostingových služieb je okruh digitálnych služieb, ktorý v sebe zahŕňa služby, akými sú služby *cloud computingu*, *webový hosting*, služby platených odkazov alebo služby umožňujúce výmenu informácií a obsahu online, vrátane ukladania a zdieľania súborov.[179] Vzhľadom na široký okruh vymedzených poskytovateľov hostingových služieb zavádza v rámci tohto pojmu DSA podkategóriu poskytovateľov online platforiem. Keďže sa jedná o relevantnú kategóriu digitálnych služieb, ktorá v sebe zahŕňa sociálne siete, ktoré sú častým miestom šírenia nezákonného obsahu vymedzuje zodpovednosť za nich diplomová práca v samostatnej časti 3.5.

Ak poskytovateľ služieb hostingu uchováva informácie poskytované príjemcom služby, nie je zodpovedný za tieto informácie pod podmienkou, že nemá skutočnú vedomosť o nezákonnej činnosti alebo nezákonnom obsahu. V prípade, ak získa vedomosť o nezákonnosti obsahu, musí rýchlo konať, aby tento nezákonný obsah odstránil, alebo aby k nemu zablokoval prístup. Odstránenie alebo zneprístupnenie nezákonného obsahu by sa však malo uskutočniť v súlade so základnými právami používateľov na slobodu prejavu a práva na informácie. Informáciu o nezákonnosti obsahu môže poskytovateľ hostingových služieb nadobudnúť buď z vlastnej iniciatívy, alebo prostredníctvom tretích osôb. V tomto prípade by sa malo jednať o konkrétne porušenie, konkrétneho práva, na základe konkrétneho nezákonného obsahu, nestačí pritom, len všeobecné povedomie, že je služba využívaná na šírenie nezákonného obsahu.

Na záver je potrebné dodať, že poskytovatelia všetkých vyššie spomenutých digitálnych služieb, musia pre naplnenie výnimky zo zodpovednosti splniť taktiež povinnosti v článku 7 DSA. Konkrétne musia poskytovatelia v dobrej viere a svedomite vykonávať dobrovoľné vyšetrovania nezákonného obsahu, a to z vlastnej iniciatívy alebo musia v tomto ohľade prijímať dobrovoľné opatrenia, ktoré sú zamerané na odhaľovanie, identifikáciu a odstraňovanie šíreného nezákonného obsahu v rámci poskytovaných digitálnych služieb. To však neznamená, že by DSA ukladalo poskytovateľom digitálnych služieb povinnosť neustáleho monitorovania šíreného obsahu (informácii) užívateľov, ktorý tento obsah (informácie) prenášajú alebo uchovávajú, a neznamená ani povinnosť poskytovateľov, aby aktívne preskúmavali obsah alebo zisťovali skutočnosti, ktoré poukazujú na nelegálnu činnosť.[180]

[178] Pre podrobnejšie informácie porov. definíciu pojmu hosting v slovníku TechDirectory. In Techopedia.com [online]. [cit. 2023-07-12]. Dostupné z: https://www.techopedia.com/definition/29023/web-hosting.
[179] Výpočet poskytovaných služieb vychádza z recitálu 29 DSA.
[180] Porov. čl. 8 DSA.

3.3.6. Zodpovednosť poskytovateľov online platforiem

DSA zavádza v rámci kategórie poskytovateľov hostingových služieb podkategóriu poskytovateľov online platforiem.[181] Online platformy, akými sú napríklad sociálne siete, umožňujú svojím používateľom nie len užívateľský obsah (informácie) ukladať na serverovú infraštruktúru, ale zároveň im umožňujú tento obsah (informácie) na ich žiadosť ďalej verejne rozširovať.

Nariadenie DSA nepovažuje za online platformy všetky hostingové služby, ktoré umožňujú zdieľanie informácii medzi používateľmi, ale zavádza korekciu, aby s tým spojené prísnejšie povinnosti regulácie nedopadli na široký obsah poskytovateľov hostingových služieb. Predovšetkým na tých, ktorí umožňujú zdieľanie informácií len ako okrajovú funkcionalitu poskytovanej služby, ak túto funkcionalitu nie je možné používať bez používania služby hlavnej.

V tomto ohľade DSA zavádza súbor povinností pre poskytovateľov online platforiem. DSA za online platformu považuje činnosť poskytovateľa hostingovej služby, ktorý na žiadosť príjemcu tejto služby uchováva a verejne šíri informácie ako svoju primárnu činnosť.[182] Za online platformy sú považované sociálne siete alebo online trhoviská.

Za online platformy teda môžeme označiť webové stránky alebo aplikácie, ktoré umožňujú používateľom medzi sebou komunikovať, zdieľať informácie, vytvárať obsah a šíriť ho. Tieto platformy sú dôležitým nástrojom pre internetovú komunikáciu a umožňujú rýchle a efektívne šírenie informácií a názorov po celom svete. Pojem online platforma vo svojom obsahu zastrešuje digitálne služby rôzneho druhu akými sú napríklad sociálne siete, videoplatformy, blogy, fóra a mnoho ďalších. V súčasnej dobe sú online platformy kľúčovým mediálnym kanálom, ktorý je využívaný pre účely marketingu, politickú propagandu alebo na šírenie informácií a zábavy. Vzhľadom na ich obrovskú popularitu a vplyv, majú online platformy zásadný význam pre internetovú komunikáciu a spoločnosť ako celok.

Činnosť online platforiem bola do zahájenia iniciatívy Európskej únie v tejto oblasti[183] do značnej miery neregulovaná, alebo regulovaná len čiastočne na základe pravidiel, z ktorých mnohé pochádzali ešte z obdobia pred rozvojom digitálneho hospodárstva.[184] Rozvoj používania týchto

[181] Porov. v čl. 2 písm. f) DSA.
[182] Porov. čl. 2 písm. i) DSA.
[183] Pre podrobnejšie informácie porov. webové stránky Európskej komisie ohľadom stratégia Formovanie digitálnej budúcnosti Európy. Dostupné z: https://digital-strategy.ec.europa.eu/sk.
[184] Smernica o elektronickom obchode, upravovala činnosť niektorých aspektov vnútorného trhu týkajúceho sa poskytovania služieb informačnej spoločnosti. Konkrétne sa týkala zodpovednosti poskytovateľov služieb informačnej spoločnosti za obsah, ktorý prenášajú alebo ukladajú na požiadanie svojich zákazníkov, a stanovuje obmedzenia zodpovednosti poskytovateľov služieb informačnej spoločnosti za takýto obsah.

služieb zároveň prináša nové riziká a výzvy pre spoločnosť ako celok, tak aj pre jednotlivcov, ktorí ich využívajú. DSA zavádza pre poskytovateľov online platforiem povinnosti nad rámec poskytovateľov hostingových služieb. Tieto povinnosti sú navyše asymetricky rozdelené podľa počtu aktívnych užívateľov online platforiem, pričom z ich aplikácie sú úplne vylúčené mikropodniky, alebo malé podniky podľa vymedzenia v odporúčaní Európskej komisie 2003/361/ES.[185] Naopak veľké online platformy a internetové vyhľadávače môžu podľa DSA predstavovať spoločenské riziká, ktoré vyžadujú vyššiu úroveň povinností vzhľadom na ich významný vplyv na spoločnosť. Tento významný vplyv sa stanovuje na základe počtu aktívnych používateľov, pričom systémové riziká sa považujú za existujúce, ak tento počet presiahne 45 miliónov, teda 10 % obyvateľstva EÚ.[186]

Poskytovatelia veľmi veľkých online platforiem a veľkých internetových vyhľadávačov majú na základe DSA povinnosť systematicky hodnotiť a riadiť riziká, ktoré vyplývajú z prevádzky poskytovanej služby a jej využívania zo strany užívateľov, a zároveň povinnosť zabezpečiť ochranu základných práv a slobôd. Pri tomto procese je dôležité zvážiť závažnosť potenciálnych negatívnych vplyvov a pravdepodobnosť výskytu takýchto systémových rizík, pričom môžu posúdiť ich rozsah, nezvratnosť a možnosti nápravy. Poskytovatelia veľkých online platforiem a internetových vyhľadávačov musia v tomto ohľade dôkladne posudzovať štyri kategórie systémových rizík. Pre obsah tejto diplomovej práce je dôležitá predovšetkým prvá kategória prieskumu, ktorá sa týka povinnosti posúdenia rizík spojených s šírením nezákonného obsahu a nezákonnými aktivitami na ich platformách. Tieto riziká môžu predstavovať vážne hrozby, ak obsah rýchlo a masovo cirkuluje na ich platformách s veľkým dosahom. Je na poskytovateľoch, aby posúdili tieto riziká a prijali opatrenia a zaistili súlad s ich obchodnými podmienkami. Je potrebné dodať, že zavedenie zodpovednosti poskytovateľov digitálnych služieb nijako neznižuje osobnú zodpovednosť príjemcov služby alebo vlastníkov obsahu. Ďalšie kategórie rizík predstavujú riziká pre uplatňovanie základných práv, účinok na demokratické procesy a poslednou účinok na ochranu verejného zdravia a maloletých.[187]

3.3.7. Povinnosti pre poskytovateľov služieb hostingu vrátane online platforiem

Poskytovateľ hostingových služieb je povinný zaviesť pre užívateľov mechanizmy oznamovania a prijímania opatrení, ktoré im umožnia prijímať oznámenia o existencii

[185] Porov. EURÓPSKA KOMISIA. Odporúčanie Komisie zo 6. mája 2003 o definícii mikropodnikov, malých a stredných podnikov. In Europa.eu [online]. [cit. 2023-11-16]. Dostupné z: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=celex:32003H0361.
[186] Porov. recitál 79 a násl DSA.
[187] Porov. recitál 80 DSA.

nezákonného obsahu na nimi poskytovaných službách. Žiadosti o výmaz obsahu by mali byť riadne odôvodnené a oznamovateľ by mal byť riadne identifikovaný, aby nedošlo k zneužívaniu zavedených mechanizmov. Vzhľadom k tomu, že odstránenie obsahu užívateľa predstavuje zásah do jeho základných práv na slobodu prejavu a práva na informácie, vrátane slobody a plurality médií, je v DSA stanovená požiadavka na to, aby poskytovateľ hostingovej služby toto svoje rozhodnutie náležite odôvodnil a umožnil dotknutému požívateľovi možnosť odvolania sa proti rozhodnutiu o odstránení alebo zneprístupnení jeho obsahu.[188] Rozhodnutie o moderácii obsahu, predovšetkým v prostredí sociálnych sietí, je vnímané veľmi citlivo, pretože sloboda prejavu je považovaná za jeden zo základných pilierov demokratickej spoločnosti a jednu zo základných podmienok sebarealizácie každého jednotlivca. Podľa článku 10 ods. 2 Listiny sa vzťahuje nielen na informácie, ktoré sú prijímané priaznivo, ale aj na tie, ktoré môžu urážať, šokovať alebo znepokojovať.[189] Ako jasne uvádza, táto sloboda podlieha určitým výnimkám, ktoré sa však musia vykladať reštriktívne a každé obmedzenie musí byť presvedčivo odôvodnené.

Poskytovateľ hostingových služieb je navyše povinný okamžite informovať orgány presadzovania práva dotknutého členského štátu a poskytnúť mu všetky relevantné informácie ktoré ma k dispozícii, ak sa dozvie o skutočnostiach, ktoré nasvedčujú tomu, že by mohlo prostredníctvom ním prevádzkovanej infraštruktúry dôjsť k spáchaniu trestného činu, ktorý ohrozuje život alebo bezpečnosť osôb. Daná povinnosť teda nedopadá na podozrenia zo spáchania všetkých trestných činov, ale len takých ktoré môžu ohroziť život alebo bezpečnosť používateľov.[190]

Nová právna úprava prináša v súvislosti so sociálnymi sieťami markantné zmeny, ktoré majú zabezpečiť reguláciu obsahu, a zároveň ochranu základných práv používateľov na slobodu prejavu a prístup k informáciám. Významným aspektom vyvažovania týchto práv je požiadavka na riadne odôvodnenie žiadostí o výmaz obsahu a identifikáciu jeho nahlasovateľa. Týmto spôsobom je možné predísť zneužívaniu zavedených oznamovacích mechanizmov, a tým chrániť legitímne práva používateľov. Táto požiadavka zároveň reflektuje citlivosť vnímania rozhodnutí o moderácii obsahu v kontexte sociálnych sietí, kde sú sloboda prejavu a pluralita médií považované za kľúčové pre demokratickú spoločnosť. Z uvedeného môžeme dovodiť, že prijatá právna úprava dostatočne vyvažuje jednotlivé záujmy. Vzhľadom k tomu, že nariadenie DSA

[188] Porov. čl. 17 a násl. DSA.
[189] REHMAN, J. *International Human Rights Law, 2nd edition Harlo*w: Pearson, 2010. 213 s. ISBN-13: 978-0199654574.
[190] Porov. čl. 17 a násl. DSA.

vstúpi v platnosť až začiatkom roka 2024, bude si potrebné pre komplexné závery počkať až na finálne prevedenie danej úpravy do praxe.

4. Trestnoprávna zodpovednosť za šírenie protiprávneho obsahu počítačov alebo umelej inteligencie na internete prostredníctvom posúdenia zodpovednosti botov

Tretím, a zároveň posledným subjektom, ktorý môže v rámci svojej činnosti šíriť protiprávny obsah na internete sú autonómne systémy umelej inteligencie. V súčasnej dobe neexistuje jednotná definícia umelej inteligencie. Európska komisia vo svojom oznámení o umelej inteligencii pre Európu definuje umelú inteligenciu ako systém, ktorý vykazuje inteligentné správanie. Samotný systém umelej inteligencie môže fungovať vo virtuálnom svete (hlasový asistenti, softvér na kontrolu obsahu), alebo ako súčasť hardvérových riešení (autonómne vozidlá, roboti).[191] Technológia umelej inteligencie často využíva metódy strojového učenia na spracovanie veľkého množstva dát. Na základe týchto dát sa umelá inteligencia zdokonaľuje, a to bez toho aby bolo potrebné upravovať jej softvér.

Tak ako každá nová technológia, aj umelá inteligencia prináša spolu s výhodami aj značné množstvo rizík. Medzi hlavnými rizikami, ktoré vidí Európska komisia sú predovšetkým chýbajúci právny rámec, ktorý by zohľadnil potrebu ochrany základných práv, vrátane ochrany osobných údajov, súkromia, otázok bezpečnosti a zodpovednosti za jej protiprávne konanie.[192]

4.1. Úprava trestnej zodpovednosti počítačov a umelej inteligencie v trestnom zákone

Zodpovednosť umelej inteligencie, vzhľadom na veľký počet zúčastnených subjektov a celkovú komplikovanosť systémov, predstavuje podľa Európskeho parlamentu jednu z najaktuálnejších výziev v 21. storočí.[193] V rámci posúdenia umelej inteligencie rozlišujeme niekoľko jej typov. Pre modelovú analýzu vyvodzovania trestnoprávnej zodpovednosti za šírenie protiprávneho obsahu sú najvýznamnejšie systémy označované ako boti.

[191] Porov. oznámenie Európskej komisie *Umelá inteligencia pre Európu*. In Eux-lex.europa.eu [online]. [cit. 2017-04-16]. Dostupné z: https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:52018DC0237.
[192] Porov. streategický dokument Európskej komisie *White paper on artificial intelligence - a European approach to excellence and trust.* In Commissioneuropa.eu. [online]. [cit. 2023-21-12]. Dostupné z: https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.
[193] Porov. správu Európskeho parlamentu *Report with recommendations to the Commission on a civil liability regime for artificial intelligence*. In Europarl.europa.eu [online]. [cit. 2023-12-21]. Dostupné z: https://www.europarl.europa.eu/doceo/document/A-9-2020-0178_EN.html.

Oxfordský slovník definuje pojem bot, ako počítačový program, ktorý vykonáva automatizované úlohy na internete. Často býva tento pojem spájaný aj s falošnými účtami na sociálnych sieťach, ktoré boli vytvorené za účelom komunikácie s ostatnými používateľmi.[194]

V rámci botov ďalej rozlišujeme podskupinu konverzačných botov, tzv. chatbotov. Chatbot je počítačový program, ktorý bol zhotovený na spracúvanie a simuláciu ľudskej konverzácie, čo používateľom týchto programov umožňuje komunikovať s digitálnym zariadením, a to hovoreným alebo písaným spôsobom. Chatboti môžu fungovať ako jednoduché programy, ktoré zodpovedajú základné otázky alebo ako komplexní asistenti, ktorí sa zdokonaľujú na základe strojového učenia.[195]

V súčasnosti teória rozlišuje dva typy chatbotov. Prvým sú tzv. úlohami riadení chatboti (angl. *task-oriented chatbots*), ktorí boli naprogramovaní k tomu, aby plnili jednotlivé požiadavky svojich používateľov. Najčastejšie sa tento druh chatovacích botov využíva na zodpovedanie jednoduchých požiadaviek, akými sú napríklad požiadavky na vytvorenie rezervácie, vykonanie jednoduchej transakcie alebo aj zdieľanie obsahu na internete. Úlohovo riadení chatboti nedokážu vyhodnocovať požiadavky svojich užívateľov a zdokonaľovať svoj kód na základe strojového učenia. Tento typ chatbotov je v súčasnosti najrozšírenejším. Druhým typom chatovacích botov sú tzv. prediktívni chatboti (angl. *predictive chatbots*), ktorí sú často využívaní ako virtuálni asistenti, pretože dokážu vyhodnocovať požiadavky svojich používateľov, a na základe strojového učenia prispôsobujú svoj kód konkrétnemu používateľovi.[196]

Páchateľom trestného činu v zmysle platnej právnej úpravy je osoba, či už fyzická alebo právnická, ktorá svojím jednaním naplnila všetky znaky konkrétneho trestného činu, a zároveň v dobe jeho spáchania bola trestnoprávne zodpovedná.[197] Trestný zákonník v súčasnej dobe neupravuje trestnú zodpovednosť umelej inteligencie a tieto systémy nemôžeme ani zaradiť pod pojem osoba. V prípade tzv. úlohovo riadených chatbotov je otázka vyvodenia zodpovednosti páchateľa v celku jednoduchá. Úlohovo riadený chatbot bude v prípade spáchania trestnej činnosti posudzovaný ako tzv. nástroj trestnej činnosti. Nástrojom trestnej činnosti chápeme vec, ktorá bola určená alebo využitá na spáchanie trestnej činnosti.[198] Páchateľom trestného činu spáchaného pomocou tohto druhu konverzačných botov bude teda osoba, ktorá buď bota vytvorila alebo

[194] Porov. definíciu pojmu Bot zo slovníka Oxford University. In Oxfordlearnersdictionaries.com [online]. [cit. 2023-02-12]. Dostupné z: https://www.oxfordlearnersdictionaries.com/definition/english/bot.
[195] ORACLE. *What is a chatbot?* In Oracle.com [online]. [cit. 2023-02-12]. https://www.oracle.com/middleeast/chatbots/what-is-a-chatbot/.
[196] Oracle.com, op. cit.
[197] ŠÁMAL, P; NOVOTNÝ, O; GŘIVNA, T; HERCZEG, J; VANDUCHOVÁ, M et al. 2022, op. cit., 166 s.
[198] Porov. § 135a trestného zákonníku.

naprogramovala s cieľom páchania trestnej činnosti vo forme šírenia protiprávneho obsahu alebo osoba, ktorá tento program takto využila.

Zložitejší prípad predstavuje posúdenie trestnej zodpovednosti za trestné činy spáchané prostredníctvom prediktívnych chatbotov, ktorí by šírili nezákonný obsah. Pripomíname, že prediktívni chatboti dokážu reagovať na podnety z okolia, a tým vykonávať zmeny v zdrojovom kóde, ktoré nie sú výsledkom činnosti žiadneho programátora. Chatbot sa „učí" na základe podnetov z okolia a prostredníctvom strojového učenia na tieto podnety reaguje. V nasledujúcej časti práca uvádza niekoľko prípadov, v ktorých sa prediktívni chatboti dopustili trestného činu v zmysle českého právneho poriadku.

Spoločnosť Microsoft v roku 2016 predstavila chatbota s názvom Tay, ktorý bol naprogramovaný k tomu, aby sa prostredníctvom strojového učenia naučil verbálne imitovať vyjadrovanie mladého človeka. Chatbot Tay bol umiestnený na sociálnu sieť Twitter, kde mal interagovať s mladými používateľmi tejto sociálnej siete. Tay interagoval s používateľmi tejto sociálnej site tým, že vytváral príspevky a odpovedal na otázky od ostatných používateľov. Tayov Tweeterový účet musel byť ale po niekoľkých hodinách zrušený z dôvodov frekventovaného porušovania pravidiel sociálnej siete Twitter. Chatbot začal vytvárať príspevky s urážlivým, rasistickým, sexsistickým a antisemitickým obsahom. Chatbot napríklad v príspevkoch napísal: „*Hitler was right*" alebo uviedol „*feminists should burn in Hell*", alebo frázu „*Taylor Swift rapes us daily*". Čo v preklade znamená „*Hitler mal pravdu*", „*feministky by mali ... zhorieť v pekle*" a „*Taylor Swift nás denne znásilňuje*".[199] Aj napriek tomu, že konverzačný bot Tay bol vytvorený s dobrým úmyslom, došlo jeho prostredníctvom k šíreniu protiprávneho obsahu.

Podobný prípad zaznamenala aj polícia v Holandsku, kde vtedy 28 ročný programátor Jeffry van der Goot umiestnil na svojom Twitterovom účte @jeffrybooks chatovacieho bota, ktorý vytváral na základe predošlých fragmentov jeho textov náhodné príspevky. V jednom z príspevkov ale chatbot pri konverzácii s iným chatobotom uviedol frázu „*I seriously want to kill people*" čo v preklade znamená „*vážne by som si prial zabíjať ľudí*". Tento príspevok zacielil na používateľský účet spojený s amsterdamskou módnou prehliadkou. Z dôvodov obáv o životy účastníkov začala tento príspevok vyšetrovať holandská polícia, ktorá v rámci vyšetrovania

[199] HUNT, E., *Tay, Microsoft's AI chatbot, gets a crash course in racism from Twitter*. In The Guardian [online]. [cit. 2023-02-13]. Dostupné z: https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter.
METZ, R., *Why Microsoft Accidently Unleashed a Neo-Nazi Sexbot*. In MIT Technology Review [online]. [cit. 2023-02-13]. Dostupné z: https://www.technologyreview.com/2016/03/24/161424/why-microsoft-accidentally-unleashed-a-neo-nazi-sexbot/.

pripisovala zodpovednosť za výroky práve Jeffreymu van der Gootovi, a to z dôvodu, že je to práve on kto chatbota vytvoril a prevádzkoval, a zároveň sú to jeho texty, z ktorých chatbot čerpal obsah pri strojovom učení.[200] Rozsudok v tejto veci by bol nepochybne zaujímavý pre vymedzenie trestnoprávnej zodpovednosti za obsah šírený umelou inteligenciou. Samotný prípad sa však k súdu nedostal, pretože bolo následné trestné stíhanie zastavené.

Otázkou v prípade chatbotov založených na strojovom učení naďalej zostáva, vymedzenie toho, kto nesie zodpovednosť za protiprávny obsah šírený v prostredí internetu. V prvom rade sa nám naskytá možnosť trestnej zodpovednosti samotného programátora alebo spoločnosti, ktorá vytvorila zdrojový kód, na základe ktorého sa umelá inteligencia strojovo učí. V prípade chatbota Tay by v tomto prípade bola trestne zodpovednou spoločnosť Microsoft, ktorá v strojovom kóde nedostatočne zabránila tomu, aby chatbot vytváral a šíril protiprávny obsah. V úvahu by pripadala aj trestná zodpovednosť požívateľov, ktorí pri vedomí toho, že umelá inteligencia vytvára obsah na základe strojového učenia z ich podnetov, zasielali nevhodný obsah s úmyslom šíriť tento nevhodný obsah ďalej prostredníctvom umelej inteligencie. V tomto prípade by mohla umelá inteligencia byť rovnako ako v prípade tzv. úlohovo riadenej umelej inteligencie, považovaná za nástroj trestnej činnosti. Je potom otázkou prípadného dokazovania, do akej miery daný používateľ naplnil znaky konkrétneho trestného činu, a akým spôsobom by sa k podobnému problému postavili české súdy. S nástupom umelej inteligencie je to zdá sa len otázkou času, kedy sa podobný prípad objaví aj v Českej republike.

V súčasnej dobe je úprava zodpovednosti poskytovateľov systémov umelej inteligencie predmetom návrhu nariadenia Európskej komisie, ktorá vytvorila vôbec prvý právny rámec pre umelú inteligenciu. Tento návrh predstavila Európska komisia v apríli 2021 a jej prijatie sa očakáva v prvej polovici roka 2024.

4.2. Pripravovaný právny rámec pre umelú inteligenciu

S nástupom a vývojom umelej inteligencie môžeme aj ruku v ruke vidieť snahu zo strany odbornej verejnosti o identifikáciu a klasifikáciu hrozieb, ktoré by potencionálne vyplývali z trestnej činnosti páchanej s pomocou umelej inteligencie. Jednou z iniciatív bola aj štúdia publikovaná v časopise *Crime Science*, ktorá mimo iného identifikovala dvadsať spôsobov, akými môže byť umelá inteligencia zneužitá na podporu a páchanie kriminality v priebehu nasledujúcich pätnástich rokov. Jednou z hrozieb, ktorú štúdia identifikovala je aj hrozba, ktorá súvisí so

[200] HERN, A. *Randomly generated tweet by bot prompts investigation by Dutch police.* In The Guardian [online]. [cit. 2023-02-13]. Dostupné z: https://www.theguardian.com/technology/2015/feb/12/randomly-generated-tweet-by-bot-investigation-dutch-police.

zdieľaním falošného obsahu.[201] Nástup využívania technológií založených na umelej inteligencii a strojovom učení so sebou zákonite priniesol aj potrebu regulácie, ktorá by mohla nie len ochrániť používateľov systémov umelej inteligencie, ale aj priniesť právny rámec a istotu pre jej poskytovateľov.

Európska komisia predložila začiatkom roka 2021 návrh nariadenia, ktorým sa stanovujú harmonizované pravidlá pre umelú inteligenciu.[202] Toto nariadenie býva tiež označované ako akt o umelej inteligencii. Tento návrh predstavuje vôbec prvý pokus o vytvorenie právneho rámca pre umelú inteligenciu. Jeho cieľom je zaistiť, aby systémy umelej inteligencie používané v Európskej únii boli bezpečné, transparentné, etické, nestranné a čo je dôležité stále pod ľudskou kontrolou.[203]

Nariadenie o umelej inteligencii prináša vlastnú definíciu umelej inteligencie, respektíve systémov umelej inteligencie, ktoré definuje ako softvér, ktorý môže, na základe človekom stanovených cieľov, generovať výstupy ako sú obsah, predikcie, odporúčania alebo rozhodnutia ovplyvnené prostredím s ktorým komunikuje. Samotná definícia sa prikláňa k názoru, že za umelú inteligenciu je považovaný len software a nie hardware. V tejto súvislosti je potrebné dodať, že definícia systémov umelej inteligencie je predmetom debaty na pôde Európskej rady a podlieha neustálym zmenám.[204]

V návrhu nariadenia sa predpokladá, že bude dopadať na viacero subjektov. Konkrétne sú nimi prevádzkovatelia, dovozcovia, distribútori a používatelia systémov umelej inteligencie. Práve tieto subjekty by podľa návrhu čelili viacerým novým povinnostiam. Za užívateľa nie je považovaná fyzická osoba, ktorá používa systémy umelej inteligencie mimo rámca svojej podnikateľskej činnosti.[205]

Nariadenie klasifikuje systémy umelej inteligencie do štyroch kategórii, na základe toho, akú mieru rizika predstavujú pre bezpečnosť občanov EÚ. Najmenej regulovanú kategóriu tvoria systémy umelej inteligencie s minimálnym rizikom, medzi ktoré bude spadať prevažná väčšina všetkých systémov. Jedná sa napríklad o systémy umelej inteligencie využívané v počítačových

[201] Závery vychádzajú zo štúdie *AI-enabled future crime* v časopise Crime Science. In Crimesciencejournal.com [online]. [cit. 2023-02-14]. Dostupné z: https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-020-00123-8.

[202] Návrh nariadenie Európskeho parlamentu a Rady, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie (Akt o umelej inteligencii) a menia niektoré legislatívne akty únie. V ďalšej časti práce ho označujeme ako nariadenie o umelej inteligencii.

[203] Porov. napr. čl. 16 nariadenia o umelej inteligencii.

[204] Porov. čl. 3 ods. 1 nariadenia o umelej inteligencii.

[205] Porov. čl. 3 ods. 4 – 8 nariadenia o umelej inteligencii.

hrách, alebo rôzne filtre proti spamom. Tieto systémy s minimálnym rizikom nie sú regulované nariadením o umelej inteligencii.[206]

Ďalšiu kategóriu tvoria systémy, ktoré predstavujú obmedzené riziko, ktorým nariadenie ukladá povinnosť transparentnosti. V prípade chatbotov nariadenie ukladá používateľom povinnosť upozorniť, že v interakcii s ľuďmi dochádza k použitiu systémov umelej inteligencie. Na základe toho, sa každý kto tento systém s prvkami umelej inteligencie využíva, bude môcť rozhodnúť či chce naďalej v jeho využívaní pokračovať. Najzásadnejšie regulovanou je tretia kategória, ktorú tvoria systémy umelej inteligencie, ktoré predstavujú najvyššiu mieru rizika. Nariadenie sem zaradzuje systémy, ktoré sú využívané ako súčasť kritickej infraštruktúry, súčasťou systémov dopravy, systémov na rozpoznávanie tvárí a pod. Prevádzkovatelia týchto systémov musia splniť celú radu povinnosti. Najzásadnejšími sú povinnosti v oblasti kybernetickej ochrany, transparentnosti a ľudského dohľadu.[207]

Každý systém umelej inteligencie podlieha registrácii Európskej komisii a povinnosti získať certifikačné označenie CE predtým ako vstúpi na trh. Tým ale povinnosti prevádzkovateľov systémov s vysokou mierov rizika nekončia, pretože musia aj naďalej monitorovať softvér a v prípade, že umelá inteligencia zmení jeho funkcionalitu musia opätovne požiadať o registráciu a splniť nanovo všetky stanovené požiadavky. Návrh nariadenia o umelej inteligencii je stále v legislatívnom procese.[208]

Aj napriek tomu, že sa v prípade nariadenia o umelej inteligencii jedná o prvý pokus o reguláciu systémov umelej inteligencie, nie je jeho súčasťou úprava zodpovednosti za jej protiprávne konanie. Nariadenie špecifikuje len zodpovednosť poskytovateľov služieb za nesplnenie stanovených regulačných povinností. V dohľadnej dobe sa ani obdobná právna úprava nepripravuje. Preto je stanovenie a vyvodzovanie prípadnej trestnoprávnej zodpovednosti umelej inteligencie ponechané na výkladovú činnosť súdov. Je však nepochybné, že v dohľadnej dobe bude potrebné podobnú reguláciu prijať. Vzhľadom na komplikovanosť systémov umelej inteligencie by bolo najlepšou alternatívou dosiahnutie medzinárodného alebo minimálne európskeho konsenzu. Zodpovednosť za systémy umelej inteligencie, tak bude aj naďalej možné s určitosťou odvodzovať len v súvislosti so súkromnoprávnou reguláciou bezpečnosti za výrobky.

[206] Porov dôvodovú správu k nariadeniu o umelej inteligencii. In. Europa.eu. [online]. [cit. 2023-12-21]. Dostupné z: https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:52021PC0206.
[207] Porov dôvodovú správu k nariadeniu o umelej inteligencii. In. Europa.eu. [online]. [cit. 2023-12-21]. Dostupné z: https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:52021PC0206.
[208] Porov. recitál 67 nariadenia o umelej inteligencii.

Záver

Problematika trestnoprávnej zodpovednosti za šírenie protiprávneho obsahu v prostredí internetu predstavuje jednu z najaktuálnejších výziev právnej teórie. S rozvojom internetu a nových technológií sa neustále objavujú nové formy trestnej činnosti, ktoré predstavujú doteraz nepoznané hrozby pre spoločnosť. Primárnym cieľom tejto práce bolo posúdiť dostatočnosť právnej úpravy v oblasti vyvodzovania trestnoprávnej zodpovednosti za šírenie protiprávneho obsahu zo strany zainteresovaných subjektov a overiť jej aktuálnosť vzhľadom na nové trendy v tejto oblasti. V tejto súvislosti môžeme konštatovať, že internet nie je možné považovať za akési právne vákuum, na ktoré by nedopadala právna regulácia ako taká.

Právne vzťahy v prostredí internetu ale predstavujú isté špecifikum, ktoré nie je vzhľadom na neustály vývoj technológii, možné ponechať bez špecifickej regulácie. Predovšetkým zvyšujúci sa význam sociálnych sieti na spoločnosť, a s tým spojené v podstate nekontrolovateľné šírenie protiprávneho obsahu prinieslo potrebu prijatia novej právnej regulácie v oblasti poskytovania digitálnych služieb. Technológie autonómnych strojov, akými sú programy s využitím umelej inteligencie, predstavujú pre spoločnosť doteraz nepoznané možnosti, ale aj hrozby, ktoré by bez dodatočnej regulácie predstavovali neúnosné riziko.

Stávajúca právna úprava trestného zákonníka preto nemusí vždy dostatočne reflektovať všetky možnosti páchania trestnej činnosti, ktoré so sebou priniesol internet. Je tak častokrát na súdnej moci, aby dané konanie páchateľa podradila pod konkrétnu skutkovú podstatu, a na zákonodarcoch, aby sa s prípadnými hrozbami vysporiadali v rámci trestnej politiky. Preto sme naznačili potrebu adaptácie sa neustále meniacim výzvam v oblasti technologického pokroku, a to predovšetkým v súvislosti s rozširovaním protiprávneho obsahu na internete.

V prvej kapitole sme poukázali na špecifiká fungovania internetu a na rýchlosť jeho vývoja. Internet predstavuje unikátny fenomén, na ktorom majú používatelia pocit anonymity a beztrestnosti. Tento pocit je, ako sme dospeli, neopodstatnený a používatelia internetu sú za svoje protiprávne konanie zodpovední rovnako, akoby dané konanie spáchali v „reálnom“ svete. Na základe zásady subsidiarity trestnej represie, by ale mali súdy a orgány činné v trestnom konaní v prostredí internetu starostlivo posúdiť závažnosť protiprávneho konania a trestnú zodpovednosť vyvodzovať len v takom prípade, ktorý dosahuje potrebný stupeň spoločenskej škodlivosti, pri ktorom už nepostačuje vyvodenie zodpovednosti podľa inej právnej normy.

V druhej kapitole sme definovali základné aspekty trestnoprávnej zodpovednosti, ktorú sme aplikovali na špecifické právne vzťahy v prostredí internetu. Následne sme poukázali na modelovom prípade protiprávneho šírenia pornografie a pri konaniach, ktoré porušujú právo na súkromie v sexuálnej oblasti na to, že zavedené skutkové podstaty nemusia postihnúť všetky variácie možnosti páchania trestnej činnosti v tejto oblasti. V prípade niektorých, pomerne častých trestných činoch, by bolo na základe vykonanej modelovej analýzy možné vyvodiť trestnoprávnu zodpovednosť, teoreticky len za trestný čin porušenia cudzích práv. Takéto právne vákuum môže predstavovať zásah do zásady *nullum crimen sine lege*. Pri zmienenom modelovom prípade, kedy by páchateľ bez vedomia obete vyhotovil jej nahú fotografiu, si ani nemusí uvedomovať trestnosť svojho konania. Tým by bolo v niektorých prípadoch možno problematické dovodiť jeho úmysel k spáchaniu trestného činu poškodzovania cudzích práv. Vyvodenie jeho zodpovednosti by vzhľadom na mieru spoločenskej škodlivosti mohlo byť považované za zásah do už spomenutej zásady. Tvorba trestnej politiky si preto vyžaduje neustálu revíziu, ktorá by náležite odrážala všetky aspekty, ktoré so sebou prináša internet, a to nie len v súvislosti so šírením protiprávneho obsahu.

V tretej časti diplomovej práce sme v teoretickej rovine porovnali aktuálnu právnu úpravu v oblasti zodpovednosti poskytovateľov služieb informačných spoločností, ktorí v rámci svojej podnikateľskej činnosti umožňujú šírenie obsahu tretím osobám, s prijatou právnou úpravou Európskej únie. V záverečnej časti tejto kapitoly sme sa bližšie zaoberali problematikou sociálnych sietí. Činnosť sociálnych sietí bola do prijatia nariadenia o digitálnych službách do značnej miery neregulovaná, alebo regulovaná len čiastočne na základe pravidiel, z ktorých mnohé pochádzali ešte z obdobia pred rozvojom digitálneho hospodárstva. Nariadenie o digitálnych službách však stanovilo poskytovateľom sociálnych sieti nové povinnosti, akými sú odstránenie alebo zneprístupnenie nezákonného obsahu a poskytovanie súčinností pri vyvodzovaní trestnoprávnej zodpovednosti za jeho šírenie. Sociálne siete by však stanovené opatrenia mali uskutočniť v súlade so základnými právami a starostlivo vyvažovať práva používateľov na slobodu prejavu a práva k prístupu a šíreniu informácii. Rozhodnutie o moderácii obsahu je zo strany používateľov vnímané veľmi citlivo, pretože sloboda prejavu je považovaná za jeden zo základných pilierov demokratickej spoločnosti.

V poslednej časti sme načrtli možné vyvodzovanie zodpovednosti za šírenie protiprávneho obsahu zo strany autonómnych strojov, akými sú systémy umelej inteligencie, na modelovom prípade botov. V súčasnosti nemáme žiadnu právnu úpravu, ktorá by upravovala trestnú zodpovednosť za šírenie protiprávneho obsahu zo strany umelej inteligencie. V rámci vykonanej

analýzy sme došli k záveru, že zodpovednosť za konanie jednoduchých systémov umelej inteligencie, ktoré nedokážu na základe vonkajších podnetov meniť svoj kód je vo väčšine prípadov možné pričítať jej programátorovi alebo používateľovi. Naopak komplexnejšie systémy umelej inteligencie založené na strojovom učení si budú vyžadovať starostlivé posúdenie konania jednotlivých subjektov, ktoré umelú inteligenciu vytvorili alebo používali, teda ako programátorov tak používateľov. Nejasnosti v problematike by vyriešil až zákonodarca, ktorý by mal stanoviť právny rámec v oblasti zodpovednosti za konanie umelej inteligencie. V súčasnosti pripravovaná právna úprava v rámci Európskej únie však danú problematiku nevyrieši, pretože neobsahuje ustanovenia pre vyvodzovanie zodpovednosti za konanie umelej inteligencie.

Vo všeobecnosti je možné prácu uzavrieť zo záverom, že svoje ciele splnila. Je však nepochybné, že je potrebné v danej problematike ďalšie skúmanie, predovšetkým s ohľadom na novoprijatú právnu úpravu, ktorá ešte nevstúpila v účinnosť. Osobitnú pozornosť si nepochybne zaslúži problematika sociálnych sieti a zodpovednosti za konanie umelej inteligencie.

Zoznam použitých zdrojov

1. Zoznam použitej literatúry

GERLOCH, A. *Teorie práva. 4. upravené vydání*. Plzeň: Aleš Čeněk, 2007. ISBN 978-80-7380-023-9.

GERLOCH, A. *Teorie práva. 7. aktualizované vydanie*. Plzeň: Aleš Čeněk, 2017. ISBN 978-80-7380-652-1.

JELÍNEK, Jiří a kolektiv. Trestní právo hmotné: obecná část, zvláštní část. 8. aktualizované a doplnené vydanie. Praha: Leges, 2017. ISBN 978-80-7502-576-0.

JOSTAŠ, P., KASL, F., KYSELOVSKÁ, T., LECHNER, T., LOUTOCKÝ, P., MÍŠEK, J., MYŠKA, M., POLČÁK, R., STUPKA, V., TOMÍŠEK, J., UŘIČAŘ, M. *Právo informačních technologií*. [Systém ASPI]. Wolters Kluwer (dříve ASPI). ASPI_ID MN328CZ. ISSN 2336-517X.

KLIMEK, L.; ZÁHORA, J. a HOLCR, K. *Počítačová kriminalita: v európskych súvislostiach*. Bratislava: Wolters Kluwer, 2016. ISBN 978-80-8168-538-5.

MCGLYNN, C., RACKLEY, E. *Image-based sexual abuse. Oxford Journal of Legal Studies*, 37 (3). pp. 534-561. ISSN 0143-6503.

PARKER, D. B. *Fighting computer crime: A new framework for protecting information*. In John Wiley & Sons, 1998. ISBN 978-0471163787.

RAMEŠOVÁ, K.: *Právní regulace kybernetické bezpečnosti a její meze. 1. vydanie*. Praha: C. H. Beck, 2023. ISBN: 978-80-7400-931-0.

REHMAN, J. *International Human Rights Law, 2nd edition Harlo*w: Pearson, 2010. 213 s. ISBN-13: 978-0199654574.

SMEJKAL, V. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. ISBN 978-80-7380-849-5.

ŠÁMAL, P; NOVOTNÝ, O; GŘIVNA, T; HERCZEG, J; VANDUCHOVÁ, M et al. *Trestní právo hmotné*. 9., prepracované vydanie. Praha: Wolters Kluwer, 2022, 1 ISBN 978-80-7598-764-8.

ŠÁMAL, P. a kol. *Trestní zákoník. 3. vydanie*. Praha: C. H. Beck, 2023. ISBN: 978-80-7400-893-1.

ŠČERBA, F. a kol. *Trestní zákoník. 1. vydanie (2. aktualizácia)*. Praha: C. H. Beck, 2022. ISBN 978-80-7400-807-8.

VAN DER MERWE, D. P. *Computers and the law*. In: Barkley Law, 2000. ISBN 0702150878.

2. Zoznam použitých internetových zdrojov

ARCTIC WOLF, A Brief History of Cybercrime. In Articwolf.com [online]. [cit. 2023-05-24]. Dostupné z: https://arcticwolf.com/resources/blog/decade-of-cybercrime/.

AUSTRALIAN INSTITUTE OF CRIMINOLOGY. *Trends & issuesin crime and criminal justice*. In AIC [online]. [cit. 2023-06-23]. Dostupné z: https://www.aic.gov.au/sites/default/files/2020-05/imagebased_sexual_abuse_victims_and_perpetrators.pdf.

BARLOW, J. P. *A Declaration of the Independence of Cyberspace*. In Eff.org [online]. [cit. 2023-05-22]. Dostupné z: www.eff.org/cyberspace-independence.

BARRENSE-DIAS, Y., BERCHTOLD, A., SURÍS J. C., AKRE C. *Sexting and the Definition Issue*. In J Adolesc Health [online]. [cit. 2023-06-23]. Dostupné z: https://pubmed.ncbi.nlm.nih.gov/28734631/.

BBC. *Apple confirms accounts compromised but denies security breach*. In Bbc.com [online]. [cit. 2023-06-24]. Dostupné z: https://www.bbc.com/news/technology-29039294.

CITRON, D. K. *Sexual Privacy. The Yale Law Journal*. 2018-2019, roč. 128, 7 s. (1924). In Yale Journal [online]. [cit. 2023-06-23]. Dostupné z: https://www.yalelawjournal.org/article/sexual-privacy.

CLEARY, B. 'It's outrageous we can't identify them': Lack of action over illegal posting of 400 nude photos of women online angers victims. In Dailymail.co.uk [online]. [cit. 2023-11-16]. Dostupné z: https://www.dailymail.co.uk/news/article-3601202/Lack-action-posting-400-nude-photos-South-Australian-women-leaked-online-angers-victims.html.

CRIME SCIENCE. *AI-enabled future crime.* In Crimesciencejournal.com [online]. [cit. 2023-02-14]. Dostupné z: https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-020-00123-8.

CONSOLE, R. *Tesla Notifies Over 75k Current and Former Employees of Recent Data Breach*, In Jduspra.com [online]. [cit. 2023-06-04]. Dostupné z: https://www.jdsupra.com/legalnews/tesla-notifies-over-75k-current-and-4275111/.

CHEBAC, A. *What Is Cybercrime-as-a-Service (CaaS)?*, In: Heimdal portal [online]. [cit. 2023-12-09]. Dostupné z: https://heimdalsecurity.com/blog/what-is-cybercrime-as-a-service-caas/.

Definícia pojmu internet v portáli BRITTANICA [online]. [cit. 2023-5-20]. Dostupné z https://www.britannica.com/technology/Internet.

Definícia pojmov phishing a spare phishing od Európskej agentúry pre bezpečnosť sietí a informácií (ENISA). In Enisa.europa.eu [online]. [cit. 2023-12-10]. Dostupné z: https://www.enisa.europa.eu/topics/incident-response/glossary/phishing-spear-phishing.

Definícia pojmu ransomvér od Európskej agentúry pre bezpečnosť sietí a informácií (ENISA), In Enisa.europa.eu [online]. [cit. 2023-12-10]. Dostupné z: https://www.enisa.europa.eu/topics/incident-response/glossary/ransomware.

Definícia pojmov vychádza z definície od Európskej agentúry pre bezpečnosť sietí a informácií (ENISA), *What is "Social Engineering*"? In Enisa.europa.eu [online]. [cit. 2023-12-10]. Dostupné z: https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering.

EUROPOL. *Cybercrime*. In Europol.europa.eu [online]. [cit. 2023-12-21]. Dostupné z: https://www.europol.europa.eu/crime-areas/cybercrime.

EURÓPSKY PARLAMENT. *Report with recommendations to the Commission on a civil liability regime for artificial intelligence*. In Europarl.europa.eu [online]. [cit. 2023-12-21]. Dostupné z: https://www.europarl.europa.eu/doceo/document/A-9-2020-0178_EN.html.

EURÓPSKA AGENTÚRA PRE BEZPEČNOSŤ SIETÍ A INFORMÁCIÍ. *Identity theft report 2020,* In Enisa.europa.eu [online]. [cit. 2023-12-09]. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-identity-theft/@@download/fullReport.

EURÓPSKA AGENTÚRA PRE BEZPEČNOSŤ SIETÍ A INFORMÁCIÍ. *Distributed denial of service*. In Enisa.europa.eu [online]. [cit. 2023-12-09]. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service/at_download/fullReport.

EURÓPSKA AGENTÚRA PRE BEZPEČNOSŤ SIETÍ A INFORMÁCIÍ. *Cyber-Bullying and online Grooming: helping to protect against the risks*. In: Enisa.europa.eu. [online]. [cit. 2023-12-01]. Dostupné z: https://www.enisa.europa.eu/publications/Cyber-Bullying%20and%20Online%20Grooming/@@download/fullReport.

EURÓPSKE CENTRUM BOJA PROTI POČÍTAČOVEJ KRIMINALITE. *Európske centrum boja proti počítačovej kriminalite na úrade Europol*. In Europa.eu [online]. [cit. 2023-05-24]. Dostupné z https://publications.europa.eu/resource/cellar/6d16d2d0-7561-4492-beef-048e64bed66a.0022.02/DOC_1.

EUROPSKÁ KOMISIA. *Politika v oblasti internetu vecí v Európe*. In Europa.eu [online]. [cit. 2023-05-20]. Dostupné z: https://digital-strategy.ec.europa.eu/sk/policies/internet-things-policy.

EUROPSKÁ KOMISIA. *Shaping Europe's digital future*. In Europa.eu [online]. [cit. 2023-06-28]. Dostupné z: https://digital-strategy.ec.europa.eu/sk/policies/digital-services-act-package.

EUROPSKÁ KOMISIA. *Umelá inteligencia pre Európu*. In Eux-lex.europa.eu [online]. [cit. 2017-04-16]. Dostupné z: https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:52018DC0237.

EUROPSKÁ KOMISIA. *White paper on artificial intelligence - a European approach to excellence and trust.* In Commissioneuropa.eu. [online]. [cit. 2023-21-12]. Dostupné z: https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.

GÁMEZ-GUADIX M., SANTISTEBAN P., RESETT S. *Sexting among Spanish adolescents: Prevalence and personality profiles*. In Psicothema [online]. [cit. 2023-06-24]. Dostupné z: https://pubmed.ncbi.nlm.nih.gov/28126055/.

GRIFFITHS, R. T. (n.d.). The History of the Internet. [online]. [cit. 2023-5-20]. Dostupné z http://edu.fmph.uniba.sk/~winczer/SocialneAspekty/GergelInternetHistoria.html.

HARMADA, A. Predchodca internetu sa začal rozrastať presne pred 54 rokmi. In Živé.sk [online]. [cit. 2023-5-20] Dostupnú z https://zive.aktuality.sk/clanok/149753/predchodca-internetu-sa-zacal-rozrastat-presne-pred-54-rokmi/.

HERN, A. *Randomly generated tweet by bot prompts investigation by Dutch police.* In The Guardian [online]. [cit. 2023-02-13]. Dostupné z: https://www.theguardian.com/technology/2015/feb/12/randomly-generated-tweet-by-bot-investigation-dutch-police.

HOFFMANN, A. a GASPAROTTI, A., *Liability for illegal content online: Weaknesses of the EU legal framework and possible plans of the EU Commission to address them in a 'Digital Services Act.* Marec 2020. In Cep.eu [online]. [cit. 2023-07-12]. Dostupné z: https://www.cep.eu/fileadmin/user_upload/hayek-stiftung.de/cepStudy_Liability_for_illegal_content_online.pdf.

HUNT, E., *Tay, Microsoft's AI chatbot, gets a crash course in racism from Twitter*. In The Guardian [online]. [cit. 2023-02-13]. Dostupné z:

https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter.

HUTKO, D. a FILOVÁ, K. *Písal Mizík hanlivý status? Súd to nepotvrdil*. In Pravda.sk [online]. [cit. 2023-06-20]. Dostupné z: https://spravy.pravda.sk/domace/clanok/518484-zacal-sa-proces-s-poslancom-stanislavom-mizikom-obzalovanym-z-extremizmu/.

JÜTTE J., *Limited liability for free Wi-Fi access (Case C-484/14, Mc Fadden v Sony Music)*. In Europeanlawblog.eu [online]. [cit. 2023-07-10]. Dostupné z: https://europeanlawblog.eu/2016/03/31/limited-liability-for-free-wi-fi-access-case-c-48414-mc-fadden-v-sony-music/.

MAJID, J. (2916): *Online Crime*. In Oxford Research Encyclopedia of Criminology. [online]. [cit. 2023-05-24]. Dostupné z: https://www.academia.edu/33173425/Online_Crime_In_Oxford_Research_Encyclopedia_of_Criminology_2016_DOI_10_1093_acrefore_9780190264079_013_112.

METZ, R., *Why Microsoft Accidently Unleashed a Neo-Nazi Sexbot*. In MIT Technology Review [online]. [cit. 2023-02-13]. Dostupné z: https://www.technologyreview.com/2016/03/24/161424/why-microsoft-accidentally-unleashed-a-neo-nazi-sexbot/.

ORACLE. *What is a chatbot?*. In Oracle.com [online]. [cit. 2023-02-12]. Dostupné z: https://www.oracle.com/in/chatbots/what-is-a-chatbot/.

OXFORD UNIVERSITY. *Bot*. In Oxfordlearnersdictionaries.com [online]. [cit. 2023-02-12]. Dostupné z: https://www.oxfordlearnersdictionaries.com/definition/english/bot.

POLICIE ČESKÉ REPUBLIKY. *Zneužívání dětí na internetu*. In Policie.cz [online]. [cit. 2023-12-01]. Dostupné z: https://www.policie.cz/clanek/zneuzivani-deti-na-internetu.aspx.

Pravidlá netikety od technologickej spoločnosti Avast. In Avast.com [online]. [cit. 2023-12-10]. Dostupné z: https://www.avast.com/c-netiquette.

SALIFU, A. (2012): *The impact of internet crime on development*, Journal of Financial Crime. In Emerald.com, [online]. [cit. 2023-05-24]. Dostupné z: https://www.emerald.com/insight/content/doi/10.1108/13590790810907254/full/html.

SARANGHAM, A. (2021): *Cyber Space: A Comprehensive Guide in 2021*. In UNext Learning Pvt. Ltd. 2020. online]. [cit. 2023-05-20]. Dostupné z: https://u-next.com/blogs/cyber-security/cyber-space/.

SMARTT, N., Sexual Harassment In The Workplace In A #MeToo World. In Forbes.com [online]. [cit. 2023-12-02]. Dostupné z:https://www.forbes.com/sites/forbeshumanresourcescouncil/2017/12/20/sexual-harassment-in-the-workplace-in-a-metoo-world/?sh=18b083135a42.

STATISTA, *Number of internet and social media users worldwide as of October 2023*. In Statista.com [online]. [cit. 2023-05-23]. Dostupné z: https://www.statista.com/statistics/617136/digital-population-worldwide/.

ŠČERBA, F. *Posuzování případů zneužívání dětí prostřednictvím internetu k pornografickým účelům*. In Trestněprávní revue, 2020, č. 3, s. 125-129. In Beck [online]. [cit. 2023-06-20]. Dostupné z: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=nrptembsgbpxi4s7gnpxgxzrgi2q&groupIndex=1&rowIndex=0&refSource=search.

TECHTARGET. *Caching*. In Techtarget.com [online]. [cit. 2023-07-11]. Dostupné z: https://www.techtarget.com/whatis/definition/caching.

TECHDIRECTORY. *Hosting*. In Techopedia.com [online]. [cit. 2023-07-12]. Dostupné z: https://www.techopedia.com/definition/29023/web-hosting.

URAM, J. *Čo je to internet, ako funguje a aká je jeho história?* In Visibility.sk [online]. [cit. 2022-5-20]. Dostupné z: https://visibility.sk/blog/internet-existuje-uz-viac-ako-50-rokov-co-by-ste-mali-o-nom-vediet/.

U.S. NEWS & WORLD. *Report Identity Theft Survey 2023*. In Usnews.com [online]. [cit. 2023-12-09]. Dostupné z: https://www.usnews.com/360-reviews/privacy/identity-theft-protection/identity-theft-fraud-survey.

YASAR, Y. *IP address (Internet Protocol address)*. In Techtarget.com [online]. [cit. 2023-06-14]. Dostupné z: https://www.techtarget.com/whatis/definition/IP-address-Internet-Protocol-Address.

YASAR, Y. *MAC address (media access control address)*. In Techtarget.com [online]. [cit. 2023-06-14]. Dostupné z: https://www.techtarget.com/searchnetworking/definition/MAC-address.

WORLD POPULATION REVIEW. *Countries Where Porn Is Illegal 2023*, In Worldpopulace.com [online]. [cit. 2023-06-17]. Dostupné z: https://worldpopulace.com/countries-where-porn-is-illegal/.

3. Zoznam použitých právnych predpisov

Dohovor o právach dieťaťa prijatý a otvorený na podpis, ratifikáciu a pristúpenie rezolúciou Valného zhromaždenia z 20. novembra 1989.

Smernica Európskeho parlamentu a Rady 2011/93/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorou sa nahrádza rámcové rozhodnutie Rady 2004/68/SVV.

Smernica 2000/31/ES Európskeho parlamentu a Rady z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode.

Návrh nariadenie Európskeho parlamentu a Rady, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie (Akt o umelej inteligencii) a menia niektoré legislatívne akty únie. V ďalšej časti práce ho označujeme ako nariadenie o umelej inteligencii.

Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách).

Ústavný zákon č. 1/1993 Sb., Ústava Českej republiky.

Ústavný zákon č. 295/2021 Sb., ktorým sa mení a dopĺňa Listina základných práv a slobôd v znení ústavného zákona č. 162/1998 Sb.

Zákon č. 40/2009 Sb., trestní zákonník.

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

Zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o súdnictve vo veciach mládeže).

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetickej bezpečnosti).

Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o niektorých službách informačnej spoločnosti).

Zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikáciach).

Zákon o telekomunikáciách Spojených štátov amerických (*H.R.2977 - Public Telecommunications Act of 1992*).

Zmluva o fungovaní Európskej únie (Konsolidované znenie)

Zákon č. 300/2005 Z. z. Trestný zákon.

4. Zoznam použitej judikatúry

Nález Ústavné súdu - senát zo dňa 25.11.2003, sp. zn. I. ÚS 558/01.

Nález Ústavného súdu zo dňa 23.03.2004, sp. zn. I. ÚS 4/04.

Nález Ústavného súdu zo dňa 20. 8. 2013, sp. zn. I. ÚS 1428/13.

Nález Ústavného súdu zo dňa 16. 6. 2015, sp. zn. I. ÚS 3018/14 – 1.

Nález Ústavného súdu zo dňa 31. 1. 2017, sp. zn. IV.ÚS 3223/16.

Rozhodnutie Najvyššieho súdu zo dňa 30. 1. 2013, sp. zn. Tpjn 300/2012.

Rozsudok Európskeho súdu pre ľudské práva zo dňa 30. 1. 2003, 40877/98, vo veci *Cordova proti Taliansku*.

Rozsudok Súdneho dvora EU zo dňa 16.9.2016, vec C-484/14.

Rozsudky Súdneho dvora Európskej únie z 23. marca 2010 v spojených veciach C-236/08, C-237/08 a C-238/08 Google France SARL a Google Inc. proti Louis Vuitton Malletier SA, Google France SARL proti Viaticum SA a Luteciel SARL.

Rozhodnutie Najvyššieho súdu Spojených štátov vo veci *Sony Corp. of America v. Universal City Studios*, Inc., 464 U.S. 417 (1984). In Supreme.justia.com [online]. [cit. 2017-11-30]. Dostupné z: https://supreme.justia.com/cases/federal/us/464/417/.

Stanovisko Najvyššieho súdu zo dňa 30.01.2013, sp. zn. Tpjn 300/2012.

Uznesenie Najvyššieho súdu zo dňa 28. 12. 2004, sp. zn. 7 Tdo 1077/2004.

Uznesenie Najvyššieho súdu zo dňa 28.05.2014, sp. zn. 6 Tdo 551/2014.

Uznesenie Najvyššieho súdu zo dňa 14. 5. 2015, sp. zn. 4 Tdo 815/2014-37.

Uznesenie Najvyššieho súdu zo dňa 14. 7. 2015, sp. zn. 4 Tdo 843/2015.

Uznesenie Najvyššieho súdu zo dňa 16.12.2015, sp. zn. 7 Td 73/2015.

Uznesenie Najvyššieho súdu zo dňa 13.12.2016, sp. zn. 6 Tdo 1638/2016.

Uznesenie Najvyššieho súdu zo dňa 25. 11. 2020, sp. zn. 8 Tdo 1041/2020.

Trestnoprávna zodpovednosť za šírenie protiprávneho obsahu v prostredí Internetu

Abstrakt

Diplomová práca sa zaoberá problematikou trestnoprávnej zodpovednosti za šírenie protiprávneho obsahu v prostredí internet, pričom sa k danej problematike stavia ako v teoretickej, tak aj v praktickej rovine. V prvej časti diplomová práca v historickom exkurze popisuje vznik internetu a vývoj počítačovej kriminality od prvotnej trestnej činnosti až po aktuálne hrozby. Jej hlavným cieľom je zhodnotiť aktuálnosť a adekvátnosť právnej úpravy v oblasti trestnej zodpovednosti za šírenie obsahu v prostredí internetu.

V rámci trestnoprávnej zodpovednosti práca kategorizuje subjekty podieľajúce sa na šírení nelegálneho obsahu v prostredí internetu do troch samostatných skupín. Konkrétne rozlišuje trestnú zodpovednosť šíriteľov obsahu, zodpovednosť poskytovateľov služieb informačných spoločností a zodpovednosť autonómnych strojov schopných vytvárať a šíriť obsah.

V druhej časti sa konkrétne zaoberá trestnoprávnou zodpovednosťou šíriteľov protiprávneho obsahu. Pričom v rámci tejto časti definuje pojem trestnoprávnej zodpovednosti a zaradzuje ho do kontextu zodpovednosti za šírenie protiprávneho obsahu na internete. V rámci tejto časti podrobnejšie analyzuje právnu úpravu v oblasti šírenia protiprávnej pornografie a trestného konania porušujúceho súkromia v sexuálnej oblasti. Práca z praktického hľadiska hodnotí jej aplikáciu na rôzne druhy konaní v tejto oblasti.

V tretej časti diplomová práca vymedzuje trestnoprávnu zodpovednosť poskytovateľov služieb informačných spoločností, vrátane sociálnych sieti, za obsah šírený ich používateľmi. V rámci tohto vymedzenia zohľadňuje novú európsku legislatívu a rozdiely oproti existujúcej právnej úprave.

Predmetom záverečnej časti diplomovej práce je skúmanie aktuálnej a pripravovanej právnej úpravy v oblasti vyvodzovanie trestnoprávnej zodpovednosti za šírenie protiprávneho obsahu v prostredí internetu zo strany autonómnych strojov, akými sú predovšetkým systémy umelej inteligencie.

Celkovo je možné skonštatovať, že práca poukazuje na potrebu prispôsobenia právnych rámcov novým výzvam, ktoré so sebou technologický pokrok prináša, a to nie len v oblasti trestnoprávnej zodpovednosti v prostredí internetu.

Kľúčové slova: trestnoprávna zodpovednosť, internet, sexuálne súkromie

Criminal liability for the distribution of illegal content on the Internet

Abstract

The thesis deals with the question of criminal liability for the distribution of illegal content in the Internet environment, approaching the issue from both a theoretical and practical point of view. In the first part, the thesis describes in a historical excursion the emergence of the Internet and the development of cybercrime from the first criminal activities to the current threats. Its main objective is to assess the timeliness and adequacy of legislation in the area of criminal liability for the dissemination of content in the Internet environment.

Within the framework of criminal liability, the thesis categories entities involved in the distribution of illegal content in the Internet environment into three distinct groups. Specifically, it distinguishes between the criminal liability of content distributors, the liability of information service providers, and the liability of autonomous machines capable of generating and distributing content.

The second part of the thesis deals specifically with the criminal liability of distributors of illegal content. It defines the concept of criminal liability and places it in the context of liability for the dissemination of illegal content on the Internet. Within this section, the legal framework for the dissemination of unlawful pornography and the offence of invasion of sexual privacy are analyzed in more detail. From a practical perspective, the thesis assesses their application to different types of conduct in this area.

In the third part, the thesis defines the criminal liability of providers of information society services, including social networks, for content disseminated by their users. This definition takes into account the new European legislation and the differences with existing legislation.

The final part of the thesis examines the current and future legislation on criminal liability for the dissemination of unlawful content on the Internet by autonomous machines, in particular artificial intelligence systems.

Overall, the thesis points to the need to adapt legal frameworks to the new challenges posed by technological advances, not only in the area of criminal liability in the Internet environment.

Keywords: criminal liability, internet, sexual privacy