

**VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH  
STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE**

**BAKALÁŘSKÁ PRÁCE**

**TRESTNÁ ČINNOST V SOUVISLOSTI S DĚTSKOU  
PORNOGRAFIÍ V ONLINE PROSTŘEDÍ**

**Autor práce: Jan Korb, DiS.**

**Studijní program: Bezpečnostně právní činnost**

**Forma studia: Kombinovaná**

**Vedoucí práce: Mgr. Jan Faltus**

**Katedra: Katedra právních oborů a bezpečnostních studií**

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.  
Žižkova tř. 1632/5b, 370 01 České Budějovice

### ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Jan Korb  
Studijní program: Bezpečnostně právní činnost  
Forma studia: Kombinovaná  
Místo studia: Píbram

Název bakalářské práce: **Trestná činnost související s dětskou pornografií v online prostředí**



Název bakalářské práce v anglickém jazyce: **Criminal Activity Related to Child Pornography in the Online Environment**

Katedra: Katedra právních oborů a bezpečnostních studií  
Vedoucí bakalářské práce: Mgr. Jan Faltus  
Datum zadání bakalářské práce (měsíc, rok): prosinec 2025




Cíl bakalářské práce:

Hlavním cílem bakalářské práce je identifikovat a zhodnotit postupy a nástroje orgánů činných v trestním řízení při odhalování, dokumentaci a vyšetřování trestné činnosti související s dětskou pornografií v online prostředí.

Vedlejším cílem je posoudit možnosti a limity forenzních a technických metod používaných při vyhledávání a zajišťování digitálních stop.

Student: Jan Korb, DiS.	4.12.2025 datum	 podpis
Vedoucí práce: Mgr. Jan Faltus	23.-01-2026 datum	 podpis

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	20.1.2026 datum	 podpis
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	29.1.2026 datum	 podpis
Rektor: doc. Ing. Jiří Dušek, Ph.D.	1.2.2026 datum	 podpis



Prohlašuji, že jsem bakalářskou práci vypracoval(a) samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí(ho) a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucímu bakalářské práce za cenné rady, připomínky a metodické vedení práce.

## ABSTRAKT

KORB, J. *Trestná činnost v souvislosti s dětskou pornografií v online prostředí: bakalářská práce*. České Budějovice: Vysoká škola evropských a regionálních studií, 2026. 77 s. Vedoucí bakalářské práce: Mgr. Jan Faltus

**Klíčová slova:** dětská pornografie, online prostředí, digitální stopa

Tato bakalářská práce se zabývá problematikou trestné činnosti související s dětskou pornografií v online prostředí, která představuje závažný společenský problém umocněný rychlým technologickým vývojem. Hlavním cílem práce je identifikovat a zhodnotit postupy a nástroje orgánů činných v trestním řízení při odhalování a vyšetřování těchto skutků. Práce je v teoretické části zaměřena na podrobnou právní analýzu vybraných skutkových podstat trestního zákoníku a na hodnocení aplikace příslušné evropské směrnice v podmínkách České republiky. Dále se zabývá možnostmi a limity forenzních metod při zajišťování digitálních stop. Praktická část vychází z polostrukturovaných rozhovorů s příslušníky Policie ČR, státním zástupcem a obhájcem se zaměřením na objasňování této trestné činnosti. Na základě zjištěných poznatků jsou v závěru práce formulována doporučení pro praxi a návrhy změn de lege ferenda.

## **ABSTRACT**

KORB, J. *Criminal Activity Related to Child Pornography in the Online Environment: Bachelor Thesis*. České Budějovice: The College of European and Regional Studies, 2026. 77 pp. Supervisor: Mgr. Jan Faltus.

**Key words:** child pornography, online environment, digital traces

This bachelor thesis deals with the issue of criminal activity related to child pornography in the online environment, which represents a serious social problem exacerbated by rapid technological development. The main objective of the thesis is to identify and evaluate the procedures and tools used by law enforcement authorities in detecting and investigating these crimes. The theoretical part of the thesis focuses on a detailed legal analysis of selected elements of the Criminal Code and on the evaluation of the application of the relevant European directive in the Czech Republic. It also deals with the possibilities and limitations of forensic methods in securing digital evidence. The practical part is based on semi-structured interviews with members of the Czech Police, a public prosecutor, and a defense attorney, focusing on the investigation of this type of crime. Based on the findings, the conclusion of the thesis formulates recommendations for practice and proposals for changes de lege ferenda.

# Obsah

Úvod.....	10
1 Cíl a metodika bakalářské práce .....	12
1.1 Cíle práce .....	12
1.2 Metodika práce.....	12
1.3 Zpracování a vyhodnocení dat .....	13
2 Vysvětlení stěžejních pojmů .....	14
2.1 Pornografie jako součást mravnostní kriminality .....	14
2.2 Osobnosti důležité pro vývoj pornografie.....	15
2.3 Kyberprostor .....	16
2.4 Digitální stopa .....	17
2.5 Dítě.....	19
3 Analýza trestného činu výroba a jiné nakládání s dětskou pornografií (§ 192 TZ) 21	
3.1 Objekt.....	22
3.2 Objektivní stránka .....	22
3.2.1 Objektivní stránka uvedená v odst. 1 .....	22
3.2.2 Objektivní stránka uvedena v odst. ....	23
3.2.3 Objektivní stránka uvedená v odst. 3 .....	24
3.2.4 Rozdíl mezi přímým držením a vzdáleným přístupem přes Informační a komunikační technologie (dále jen IKT) .....	26
3.2.5 Přímé držení .....	27
3.2.6 Vzdálený přístup přes IKT .....	27
3.3 Subjekt .....	28
3.4 Subjektivní stránka.....	28
3.5 Kvalifikovaná skutková podstata uvedená v § 192 odst. 4 TZ .....	28
3.6 Kvalifikovaná skutková podstata uvedená v § 192 odst. 5 TZ .....	30
4 Zneužití dítěte k výrobě pornografie podle § 193 TZ.....	32
4.1 Objekt.....	32

4.2	Objektivní stránka .....	32
4.3	Subjekt .....	34
4.4	Subjektivní stránka.....	34
4.5	Kvalifikovaná skutková podstata v § 193 odst. 2 a 3 TZ.....	34
5	Navazování nedovolených kontaktů s dítětem podle § 193b TZ.....	36
5.1	Objekt.....	36
5.2	Objektivní stránka .....	37
5.3	Subjekt .....	37
5.4	Subjektivní stránka.....	38
6	Analýza Směrnice 2011/93/EU o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii.....	39
6.1	Propojení směrnice a TZ .....	40
6.2	Ochrana obětí a prevence ve směrnici .....	41
7	Způsoby zajišťování dat.....	42
7.1	Zajištění nosiče dat.....	42
7.2	Zajištění vzdálených dat.....	44
8	Praktická část .....	45
8.1	Metodologie a technika sběru dat .....	45
8.2	Charakteristika respondentů.....	46
9	Analýza prvotního zajištění a zajištění dětské pornografie.....	47
9.1	Technické bariéry .....	47
9.2	Personální a metodické limity .....	48
10	Prokazování faktické dispozice a role cloudových uložišť .....	49
10.1	Technické nástroje a forenzní analýza .....	49
10.2	Mezinárodní spolupráce .....	50
10.3	Námítky obhajoby .....	50
11	Právní kvalifikace, systémové limity .....	51
11.1	Přechovávání vs. streaming.....	51

11.2	Systémové limity.....	52
11.3	Vzdělání a odbornost jako limitující faktor .....	52
12	Shrnutí výzkumu .....	53
12.1	Odpovědi na výzkumné otázky .....	53
12.2	Zhodnocení vzdělávacího systému PČR.....	54
13	Návrhy na zefektivnění boje proti dětské pornografii .....	55
13.1	Návrhy De lege ferenda .....	55
13.2	Technické a materiální vybavení základních útvarů.....	56
13.3	Reforma systému odborného vzdělávání policistů .....	56
13.4	Metodická podpora policistů na všech úrovních.....	56
	Závěr .....	59
	Seznam použitých zdrojů .....	61
	Seznam zkratk .....	64
	Seznam příloh.....	65
	Přílohy .....	66

## Úvod

Téma zneužívání dětí k výrobě pornografických materiálů a jejich následné šíření v online prostředí představuje v současnosti jeden z nejzávažnějších a nejaktuálnějších nejen kriminologických, ale také společenských problémů. S neustálým a rychlým vývojem informačních a komunikačních technologií získávají pachatelé široké spektrum nových možností a nástrojů, jak tuto trestnou činnost, i svou identitu úspěšně zastírat. Tato dynamika digitálního světa vytváří zásadní rozdíly mezi technologickým náskokem kriminálních subjektů a technickými i procesními limity, které mají orgány činné v trestním řízení při odhalování této kriminality.

Právní rámec České republiky na tyto hrozby reaguje zejména skutkovými podstatami trestných činů podle § 192, § 193 a § 193b zákona č. 40/2009 Sb. trestního zákoníku ve znění pozdějších předpisů (TZ). Přestože je česká legislativa v této oblasti úzce propojena s evropským právem, zejména směrnicí Evropské unie 2011/93EU, praxe ukazuje, že samotná zákonná úprava bez efektivních technických a forenzních postupů k účinnému potírání této kriminality nepostačuje.

Současný stav poznání a praxe v této oblasti sice zahrnuje podrobné právní výklady a analýzy zákonných znaků, avšak v oblasti praktického objasňování a zejména efektivního dokazování se neustále objevují nové bariéry. Zásadní problém spočívá právě ve vzájemném střetu rychlého technologického rozvoje online prostředí a časově i technicky limitovaných postupů orgánu činných v trestním řízení při vyhledávání a zajišťování digitálních stop. Tato práce proto reaguje na potřebu hlubšího poznání a prozkoumání těchto limitů a hledání cest k jejich překonání v rámci stávajícího právního řádu.

Podle statistik Policie České republiky, které byly získány na základě žádosti o informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím ve znění pozdějších předpisů, došlo v letech 2021 až 2025 k výraznému nárůstu registrovaných případů trestných činů souvisejících s dětskou pornografií podle § 192 a § 193 TZ. Zatímco v roce 2021 bylo registrováno 627 případů, v roce 2025 toto číslo vzrostlo na 925, což představuje přibližně 48% nárůst. Z těchto případů bylo objasněno průměrně kolem 55 % (např. 334 v roce 2021 a 518 v roce 2025). Významnou roli hraje internet

jako prostředí páchaní, kde bylo spácháno 480 případů v roce 2021 a až 727 v roce 2025, což ukazuje na rostoucí trend online distribuce a držení materiálů. Naproti tomu případy spáchané ostatními počítačovými sítěmi se pohybují v rozmezí (6–20 případů ročně). Tento vývoj podtrhuje nutnost efektivních postupů orgánů činných v trestním řízení, zejména v kontextu rychlého technologického pokroku, který umocňuje dostupnost nelegálního obsahu. Podrobný přehled těchto dat je k dispozici v Příloze 1 této práce.

Tato bakalářská práce proto reaguje na potřebu hlubšího poznání a prozkoumání uvedených limitů a hledání cest k jejich překonání v rámci stávajícího právního řádu. Jejím ústředním záměrem je identifikovat a komplexně zhodnotit postupy a nástroje, které orgány činné v trestním řízení (dále jen OČTŘ) uplatňují při odhalování, dokumentaci a vyšetřování trestné činnosti související s dětskou pornografií v online prostředí.

Současně se práce zaměřuje na posouzení stávajících možností, a především limitů forenzních a technických metod, jež jsou využívány při vyhledávání a zajišťování digitálních stop.

K dosažení těchto ambicí je práce členěna na teoretickou a praktickou část. Teoretická část nabídne podrobnou právní analýzu vybrané trestné činnosti, výklad klíčové terminologie a analýzu relevantní evropské směrnice, čímž položí základ pro empirické šetření. Praktická část pak prostřednictvím polostrukturovaných rozhovorů s příslušníky Policie ČR na různých úrovních, státním zástupcem a obhájcem vyhodnotí zjištění z praxe, jež budou následně komparována s právním rámcem a strategickými dokumenty. Závěrečným výstupem bude formulace doporučení pro praxi orgánů činných v trestním řízení a návrhy *de lege ferenda*, které by měly přispět k efektivnějšímu potírání této závažné kriminality.

# 1 Cíl a metodika bakalářské práce

Tato kapitola podrobně definuje záměry, kterých má být v rámci bakalářské práce dosaženo, popisuje zvolené postupy a metody, které budou využity k naplnění těchto cílů.

## 1.1 Cíle práce

Hlavním cíle bakalářské práce je identifikovat a zhodnotit postupy a nástroje, které využívají OČTŘ při odhalování, dokumentaci a vyšetřování trestné činnosti související s dětskou pornografií v online prostředí. Důraz bude kladen především na efektivitu těchto nástrojů v kontextu rychle se vyvíjejících technologií.

Vedlejším cílem práce je posoudit současné možnosti a zejména limity forezních a technických metod, které jsou aplikovány při vyhledávání a zajišťování digitálních stop v digitálním prostoru.

## 1.2 Metodika práce

Pro dosažení stanovených cílů bude práce rozdělena na teoretickou a praktickou část, přičemž každá z nich využívá specifické metodologické přístupy.

V teoretické části bude využita metoda analýzy a komparace odborné literatury, platné legislativy a judikatury. Klíčovým prvkem bude podrobná právní analýza skutkových podstat trestných činů dle § 192, § 193 a § 193b TZ. Dále bude provedena analýza stěžejních kapitol Směrnice Evropské unie 2011/93EU o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii (dále jen směrnice) a zhodnocení způsobu, jakým je tato směrnice aplikována v rámci českého právního řádu.

Praktická část práce je založena na kvalitativním výzkumu. Hlavní metodou sběru dat jsou polostrukturované řízené rozhovory. Tento typ rozhovoru byl zvolen pro svou flexibilitu, která umožňuje respondentům hlouběji popsat specifika vyšetřování a autorovi dává možnost klást doplňující otázky. Výzkumný soubor tvoří 11 respondentů (R1–R11) rozdělených do čtyř cílových skupin:

- Policisté sloužící na základních člancích PČR: Zaměření na prvotní úkony, materiální vybavení a technické zajištění digitálních stop na místě činu.
- Specialisté SKPV: Zaměření na pokročilé forenzní nástroje, prokazování faktické moci nad daty v cloudu a mezinárodní spolupráci.
- Státní zástupci: Zaměření na procesní čistotu, judikaturu a prokazování subjektivní stránky trestného činu.
- Obhájci: Zaměření na argumentační strategie, napadání integrity důkazů a nejčastější procesní pochybení OČTŘ.

Tato skladba respondentů zajišťuje metodu triangulace dat, která je nezbytná pro komplexní pochopení problematiky. V rámci výzkumu jsou stanoveny tyto výzkumné otázky (dále jen VO):

- Jaká jsou hlavní technická a procesní rizika při prvotním zajišťování digitálních stop s obsahem dětské pornografie?
- Jak efektivně dokáže policie prokazovat „faktickou moc“ nad nelegálním obsahem v cloudu a na streamingových platformách?
- Existuje shoda v právním nahlížení na streaming dětské pornografie a jaké jsou limity prokazování úmyslu?

### **1.3 Zpracování a vyhodnocení dat**

Získaná zjištění z řízených rozhovorů budou následně vyhodnocena a porovnána s teoretickým právním rámcem a strategickými dokumenty orgánů činných v trestním řízení. Cílem této komparace je identifikovat největší problémy, se kterými se praxe potýká, a navrhnout možná řešení.

Výstupem celého procesu budou v závěru práce formulovaná doporučení pro praxi OČTŘ a návrhy změn de lege ferenda, které by mohly přispět k zefektivnění boje proti této závažné kriminalitě.

## 2 Vysvětlení stěžejních pojmů

Pro účely této bakalářské práce je nezbytné jasně vymezit terminologický rámec, který tvoří základ pro analýzu trestné činnosti v digitálním prostoru. Jasná definice pojmů je klíčová nejen pro právní analýzu, ale i pro pochopení technických aspektů vyšetřování a dokazování. V této kapitole se tedy autor zaměří na vymezení termínu pornografie, což je klíčové jak pro následnou právní analýzu, tak také pochopení fungování páčání této kriminality v online prostředí, na které se autor zaměří v druhé části této kapitoly, závěrem se tato kapitola bude věnovat pojmu dítě jako takovému v kontextu práva.

### 2.1 Pornografie jako součást mravnostní kriminality

Jak již bylo v úvodu této kapitoly zmíněno, pochopení termínu pornografie je klíčové pro další části této bakalářské práce. Na úvod je důležité zařadit pornografii do celkového systému práva a kriminality, tedy do skupiny mravnostní kriminality. Mravnostní trestná činnost je součástí každé vrstvy společnosti, tedy i těch, kde je přísně trestána přísnými tresty. Mezi její příčiny můžeme zařadit především neukojené sexuální potřeby pachatelů, v menší míře pak také patologické sklony části lidstva, tedy sexuální úchylky.<sup>1</sup>

Mravnostní trestná činnost zahrnuje široké spektrum činů od sexuálního nátlaku, znásilněné až po držení dětské pornografie. Všechny tyto trestné činy mají společný jmenovatel, a to porušování morálních norem, které si naše společnost nastavila jako zásadní pro ochranu lidské důstojnosti a sexuality. To platí především u zranitelných obětí, jako jsou děti. Sexuální zneužití dítěte přináší hned několik negativních důsledků, mimo prvotního poškození samotným aktem, dochází také k sekundárnímu a dlouhodobému poškození, které zasahují především osobnostní a emoční vývoj.<sup>2</sup> Právě kvůli těmto negativním vlivům, díky kterým mohou ovlivnit celý následující život malého dítěte považuje autor tuto problematiku za jednu z nejpodstatnějších, jelikož

---

<sup>1</sup> Srov. Chmelík, Jan. *Mravnost, Pornografie a Mravnostní Kriminalita*. Vyd. 1. Praha: Portál, 2003 s. 9 ISBN 80-7179-739-6

<sup>2</sup> Srov. VANÍČKOVÁ, Eva. *Sexuální zneužívání dětí*. 1. Ilustroval Jiří SLÍVA. Praha: Karolinum, 1997. s. 19 ISBN 80-7184-479-9.

nezletilé oběti jsou snadnou kořistí sexuálních predátorů a mohou si nést celoživotní traumata ovlivňující jejich budoucí život.

## 2.2 Osobnosti důležité pro vývoj pornografie

Klíčovým milníkem ve vývoji pornografie se stal vynález knihtisku Johannem Gutenbergem kolem roku 1440. Ačkoliv byl původně určen pro šíření náboženských textů, umožnil masovou výrobu a distribuci explicitních děl, čímž se jejich produkce stala dostupnější a vyvolala první debaty o mravnosti a obscénnosti.<sup>3</sup>

Další technologický průlom přišel s francouzským fotografem Louisem-Jacquesem-Mandém Daguerrem a jeho vynálezem daguerrotypie v roce 1839. Realismus fotografie zvýšil vnímání nebezpečnosti takového materiálu, protože dokumentoval reálné osoby, což zesílilo debaty o mravnosti a vedlo k prvním regulacím obscénních fotografií. S rozvojem fotografie se také objevily první případy zneužívání médií k zobrazování lidí v nevhodném kontextu. Realismus fotografie zvýšil vnímání nebezpečnosti takového materiálu, protože dokumentoval reálné lidi, což zesílilo debaty o mravnosti a vedlo k prvním regulacím obscénních fotografií.<sup>4</sup>

Nástup filmové technologie přinesl další zásadní změny. Thomas A. Edison společně s Williamem Dicksonem v roce 1891 vynalezl kinetoskop, předchůdce filmového projektoru, který umožnil realistické zobrazení osob a předmětů v pohybu. Tato technologie vedla k profesionalizaci filmové tvorby a vzniku nahrávacích studií, což vyžadovalo nové právní rámce pro regulaci mravnosti a obscénnosti. Současně se s touto profesionalizací objevilo potenciální riziko zneužívání dětí v audiovizuálních materiálech, neboť film nabízel dynamičtější a sugestivnější formu zobrazení.<sup>5</sup>

---

<sup>3</sup>Srov. ARTSY EDITORIAL. Renaissance Artists Who Brought Pornography to the Masses. Artsy, 2017. [cit. 2026-01-13]. Dostupné z: <https://www.artsy.net/article/artsy-editorial-renaissance-artists-brought-pornography-masses>

<sup>4</sup> Srov. SYBIL. How the Daguerreotype Started a Victorian Black Market for Pornography in London. Sysphoto, 2019. [cit. 2026-01-13]. Dostupné z: <https://sysphoto.wordpress.com/2019/08/20/how-the-daguerreotype-started-a-victorian-black-market-for-pornography-in-london/>

<sup>5</sup> Srov. LIBRARY OF CONGRESS. Origins of Motion Pictures. In: History of Edison Motion Pictures. Washington, D.C.: Library of Congress. [cit. 2026-01-13]. Dostupné z: <https://www.loc.gov/collections/edison-company-motion-pictures-and-sound-recordings/articles-and-essays/history-of-edison-motion-pictures/origins-of-motion-pictures/>

Ve druhé polovině 20. století se pornografie začala postupně stávat součástí mainstreamové kultury, zejména díky osobnostem jako Hugh Hefner, který v roce 1953 založil časopis Playboy. Tento trend přispěl k postupné desenzibilizaci společnosti vůči erotickému obsahu, což nepřímo ovlivnilo i vnímání a šíření explicitních materiálů, včetně těch, které by mohly být později zneužity.<sup>6</sup>

Z uvedeného historického vývoje vyplývá, jak konstatuje Lynn Huntová, že pornografie se po dlouhou dobu vyvíjela jako součást jiných projevů, a jako samostatná kategorie, vnímaná jako zobrazování sexuálních orgánů a praktik s cílem vzbudit vzrušení, se začala profilovat až v období mezi renesancí a francouzskou revolucí.<sup>7</sup>

Tato definice, která zdůrazňuje explicitní sexuální kontext, je zásadní pro rozlišení od jiných forem erotického umění a pro klasifikaci dětské pornografie.

Všechny zmíněné technologické inovace položily, dle mínění autora této práce, základy pro současný stav, kdy se pornografie, a s ní bohužel i dětská pornografie, v online prostředí stala snadno dostupnou. Její distribuce se díky anonymizačním nástrojům a globálnímu dosahu internetu stala pro orgány činné v trestním řízení mimořádně obtížně kontrolovatelnou, což podtrhuje význam problematiky, již se tato práce zabývá.

## 2.3 Kyberprostor

Pojem kyberprostor jako takový, jak uvádí Radim Polčák, využil, a někteří tvrdí, že vymyslel, ve svém díle *Neuromancer* z roku 1984 americký spisovatel William Gibson. Který v tomto díle vytvořil imaginární svět a jazyk a popsal tak kyberprostor již dekádu před revolucí informačních technologií a rozšířením internetu.<sup>8</sup> Samotný kyberprostor nelze vymezit bez toho, aniž by byl zmíněn pojem internet, kdy tyto dva pojmy spolu nerozlučitelně souvisí. Internet byl původně zprovozněn především

---

<sup>6</sup> Srov. HAWKINS, D. Hugh Hefner & the Sexual Objectification of Women. End Sexual Exploitation, 2017. [cit. 2026-01-13]. Dostupné z: <https://endsexualexploitation.org/articles/hugh-hefner-sexual-objectification-women/>

<sup>7</sup> Srov. HUNT, Lynn (ed.). *The invention of pornography: obscenity and the origins of modernity, 1500-1800*. New York: Zone Books, 1993. s. 10 ISBN 0-942299-68-x

<sup>8</sup> Srov. GRÍVNA, Tomáš a POLČÁK, Radim (ed.). *Kyberkriminalita a právo*. Praha: Auditorium, 2008. s. 30 ISBN 978-80-903786-7-4.

k vědeckým a vojenským účelům, kdy se jednalo o propojení několika počítačů, k tomuto došlo v 50. letech 20 století.<sup>9</sup>

Otázkou tedy zůstává, co to internet tedy je, dle Koloucha se jedná o *“celosvětovou distribuovanou počítačovou síť složenou z jednotlivých menších sítí, které jsou navzájem spojeny pomocí protokolů IP a tím je umožněna komunikace, přenos dat, informací a poskytování služeb mezi subjekty navzájem. Tím je vlastně vytvořen dynamický, neustále se měnící a vyvíjející systém vázaný na hardware, avšak zároveň vytvářející těžko definovatelný a prakticky neomezený kyberprostor.”*<sup>10</sup> Kyberprostor je typický svými znaky, mezi které patří globálnost, anonymita a rychlost přenosu informací, čímž se stává ideálním prostředím pro páchaní trestné činnosti. Kolouch přirovnává kyberprostor k ledovci, který je tvořen třemi vrstvami, první vrstvou je Surface Web, tedy prostor, který je dostupný většině společnosti přes běžné internetové prohlížeče. Dále poté na Deep Web a Dark Web, společně nazývány jako Darknets, které obsahují až 96% celého obsahu internetu. A je to právě Darknet, který je nejčastějším prostředím páchaní trestné činnosti, mezi kterou nepochybně patří také šíření dětské pornografie.<sup>11</sup>

## 2.4 Digitální stopa

Pro pochopení dalších kapitol této bakalářské práce je velmi podstatné si stanovit, co je to vlastně digitální stopa. V kontextu dynamického rozvoje moderních technologií se role elektronických důkazů v trestním řízení kontinuálně zvyšuje. Tyto důkazy se od tradičních forem odlišují svými specifickými charakteristikami, mezi něž patří modifikovatelnost, snadná zničitelnost a technická komplexnost jejich zajišťování. I přes svou klíčovou významnost pro teoretické vymezení a praktické zajišťování v trestním řízení postrádá český právní řád jednoznačnou definici elektronického důkazu.<sup>12</sup>

Základní definice stopy jako takové v kriminalistice, tak jak ji uvedl Porada uvádí, že za kriminalistickou stopu lze považovat změnu v materiálním prostředí, nebo vědomí

---

<sup>9</sup> Srov. KOLOUCH, Jan. *CyberCrime*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2016. s. 42 ISBN 978-80-88168-18-8

<sup>10</sup> Tamtéž, s. 43

<sup>11</sup> Srov. KOLOUCH, Jan. *CyberCrime*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2016. s. 46 - 48 ISBN 978-80-88168-18-8.

<sup>12</sup> Srov. GRIVNA, Tomáš; RICHTER, Martin a ŠIMÁNOVÁ, Hana (ed.). *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. Str. 14 ISBN 978-8,-87284-95-7

člověka, která souvisí příčinně, místně, nebo časově s kriminalisticky relevantní událostí, je zjištěitelná, zajištěitelná a využitelná současnými metodami, prostředky a postupy.<sup>13</sup>

Digitální stopu, je poměrně složité vložit do této definici a možná i proto přišla Burdová s definicí: *“Digitální stopa je jakákoliv informace s vypovídající hodnotou, uložená nebo přenášena v digitální podobě”*<sup>14</sup> Tato definice se blíží jedné z nejpoužívanějších definicí jak v České republice, tak v celé Evropě, kterou v roce 1999 navrhla pracovní skupina SWGDE (Scientific Working Group on Digital Evidence) a která je uznávána širokým spektrem expertů jak v České republice, tak v zahraničí. Tato definice zní následovně: *„Digitální stopa je jakákoliv informace s vypovídající hodnotou pro danou relevantní událost, uložená nebo přenášena v digitální podobě“*<sup>15</sup>

Co se týče samotného vzniku digitálních stop, autor této práce se ztotožňuje s tvrzením Koloucha, který tvrdí, že ať v prostředí internetu uděláme jakoukoliv operaci, tak tam stopa po této operaci zůstane už navždy, i když dojde k pokusu o zásah do dat a systému smazat a zakrýt, vždy zůstane stopa. Digitální stopy se dále dělí na stopy ovlivnitelné a neovlivnitelné. Definicí neovlivnitelných stop jsou stopy, které vznikají interakcí mezi dvěma počítačovými systémy. Zručný uživatel dokáže i tyto neovlivnitelné stopy, mezi které se řadí:

- informace z počítačového systému
- připojení k počítačovým sítím, zejména internetu
- využívání poskytovaných služeb aj.

pozměnit, nebo maskovat, například za využití systémů, které maskují, nebo mění IP adresy.

Definici stop ovlivnitelných poté Kolouch popisuje jako informace, které o sobě uživatel počítače a internetu sám předá jiné osobě, ať už napřímo, nebo je dobrovolně zadá do nějakého počítačového systému.<sup>16</sup>

---

<sup>13</sup> Srov. PORADA, Viktor. *Kriminalistika*. Brno: CERM, 2001. s. 70 ISBN 9788072041947

<sup>14</sup> BRUNOVÁ, Markéta. *Dokazování trestné činnosti: s využitím kriminalistických stop a identifikace*. Eupress. Praha: Vysoká škola finanční a správní, 2019. s. 35 ISBN 978-80-7408-196-5.

<sup>15</sup> RAK, Doc. Ing. Roman Ph.D a Prof. JUDr. Ing. Viktor, DrSc, dr.h.c PORADA. *Vlastnosti digitálních stop a jejich dopady na forenzní šetření*. Soudní inženýrství [online]. Praha: Policejní akademie ČR 2005, 16 [cit. 2026-01-15]. Dostupné z: <http://www.sinz.cz/archiv/docs/si-2005-04-183-192.pdf>

<sup>16</sup> Srov. KOLOUCH, Jan. *CyberCrime*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2016. s. 135 -144 ISBN 978-80-88168-18-8.

Tyto informace opět, dle názoru autora této práce, potvrzují technickou náročnost při zajišťování digitálních stop, se kterou se musí orgány činné v trestním řízení a zejména policejní orgány vyrovnat, při zajišťování, a především vyhledáváním těchto digitálních stop. Pokud jen mírně pokročilý uživatel internetu dokáže maskovat svůj pohyb v kyberprostoru pomocí dostupných nástrojů, klade tato skutečnost extrémní nároky na technickou erudici a kontinuální vzdělávání policistů, kteří musí být schopni tyto sofistikované bariéry identifikovat a překonávat.

## 2.5 Dítě

Pro správné vymezení trestných činů souvisejících s dětskou pornografií je nezbytné definovat pojem "dítě", který představuje chráněnou osobu v právním řádu, což stanovuje v § 32 již Listina základních práv a svobod.<sup>17</sup> V českém trestním právu je tento pojem úzce spojen s věkovou hranicí, která určuje hranice sexuální exploatace a ochrany mravnosti.<sup>18</sup>

V mezinárodním prostoru byl pojem dítě stanoven Úmluvou o právech dítěte, která byla přijata dne 20.11.1989 v New Yorku, kdy dle této úmluvy se dítětem rozumí každá bytost, která nedovršila 18 let. Nedílnou součástí této úmluvy je také článek 34, kde je uvedeno, že stát se zavazuje tomu, aby zabránil využívání dítěte k jeho zneužívání k jakémukoliv závadovému jednání se sexuálním podtextem, kdy samotná výroba pornografie, je jmenována jako jedna ze zakázaných forem jednání vůči dítěti.<sup>19</sup>

V českém trestním právu je dítětem definována osoba mladší osmnácti let, tak hovoří § 126 TZ.<sup>20</sup> Tento přístup vychází z principu nulové tolerance k jakémukoli zobrazení nebo zneužití nezletilých v pornografickém materiálu, harmonizovaném se směrnicí EU 2011/93/EU, která zdůrazňuje prevenci a stíhání bez ohledu na souhlas nebo zralost oběti.<sup>21</sup> Stejně tak v občanském právu, regulovaném zákonem č. 89/2012 Sb.,

---

<sup>17</sup> Srov. Ústavní zákon č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, ve znění pozdějších předpisů, čl. 32

<sup>18</sup> Srov. ŠÁMAL, Pavel. *Trestní zákoník: komentář*. III, § 272-421. 3. vydání. Velké komentáře. V Praze: C.H. Beck, 2023. s. 1733 - 1740 ISBN 978-80-7400-893-1

<sup>19</sup> Srov. *Úmluva o právech dítěte a související dokumenty*. [Praha]: Ministerstvo práce a sociálních věcí ČR, 2016. s. 2-12 ISBN 978-80-7421-120-1.

<sup>20</sup> Srov. ŠÁMAL, Pavel. *Trestní zákoník: komentář*. III, § 272-421. 3. vydání. Velké komentáře. V Praze: C.H. Beck, 2023. s. 1733 ISBN 978-80-7400-893-1

<sup>21</sup> Srov. *Směrnice Evropského parlamentu a rady 2011/92/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii*

občanským zákoníkem, ve znění pozdějších předpisů, je dítětem osoba do dosažení plnoletosti (18 let).<sup>22</sup>

Děti jsou navíc považovány za zvláště ohrožené oběti, což je zakotveno v § 4 písm. a) zákona č. 45/2013 Sb., o obětech trestných činů ve znění pozdějších předpisů, který definuje zvláště zranitelnou oběť jako oběť, která je z důvodu svého věku, zdravotního stavu nebo jiné podobné příčiny zvláště zranitelná. Tato kategorie zajišťuje dětem zvýšenou ochranu v trestním řízení, včetně práva na informace, podporu a minimalizaci sekundární viktimizace, což podtrhuje jejich zranitelnost v kontextu online vykořisťování.<sup>23</sup>

---

<sup>22</sup> Srov. ŠVESTKA, Jiří. *Občanský zákoník: komentář*. 2, 604-608. 2. vyd. Velké komentáře. V Praze: C.H. Beck, 2009. s. 106 ISBN 978-80-7400-108-6

<sup>23</sup> Srov. GRIVNA, Tomáš; ŠÁMAL, Pavel a VÁLKOVÁ, Helena. *Oběti trestných činů: komentář*. 2. vydání. Komentované zákony. V Praze: Beck, 2020. s. 18-31 ISBN 978-80-7400-793-4

### 3 Analýza trestného činu výroba a jiné nakládání s dětskou pornografií (§ 192 TZ)

Tato kapitola se zaměřuje na analýzu skutkové podstaty § 192 TZ, který upravuje trestný čin výroby a jiného nakládání s dětskou pornografií. Tento paragraf představuje klíčový nástroj trestního práva pro ochranu dětí před sexuálním vykořisťováním, přičemž zahrnuje širokou škálu chování od výroby materiálů po jejich držení nebo nabízení.

V následujícím textu jsou rozebrány zákonné znaky skutkové podstaty, kvalifikované skutkové podstaty a aplikační praxe, s odkazy na judikaturu a komentáře, což umožňuje lepší pochopení role § 192 TZ v boji proti této formě kriminality. Tato analýza představuje základní kámen pro následující podkapitoly o souvisejících paragrafech a jejich aplikaci v online prostředí.

Klíčové pro následující rozbor skutkové podstaty je vymezení pojmu dětské pornografie, které je jednoznačně stanoveno směrnicí Evropské unie č. 2011/93/EU ze dne 13. prosince 2011. Konkrétně článek 2 písm. c) uvádí, že dětskou pornografií se rozumí:

- „*jakýkoli materiál, který zobrazuje dítě, které se účastní skutečného nebo předstíraného jednoznačně sexuálního jednání,*
- *jakékoli zobrazení pohlavních orgánů dítěte prvotně k sexuálním účelům,*
- *jakýkoli materiál, který zobrazuje osobu se vzhledem dítěte, která se účastní skutečného nebo předstíraného jednoznačně sexuálního jednání, nebo každé zobrazení pohlavních orgánů osoby se vzhledem dítěte k prvotně sexuálním účelům, nebo*
- *realistické obrázky dítěte, které se účastní jednoznačně sexuálního jednání, nebo realistické obrázky pohlavních orgánů dítěte k prvotně sexuálním účelům;*“<sup>24</sup>

Základní skutková podstata zmíněného trestného činu zní: „*Kdo přechovává fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které*

---

<sup>24</sup> Směrnice Evropského parlamentu a rady 2011/92/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii čl. 2 písm. c)

*zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem, bude potrestán odnětím svobody až na dva roky.*<sup>25</sup>

Obdobně hovoří také mezinárodní úmluvy v oblasti kybernetické kriminality, jako je Úmluva Rady Evropy o kybernetické kriminalitě (Budapešť, 2001, např. čl. 9), což svědčí o široké mezinárodní jednotě v přístupu k dětské pornografii. Z výše uvedených ustanovení však vyplývá, že pokud materiál nebyl vytvořen s prvotním úmyslem vyvolat sexuální vzrušení, nelze jej považovat za dětskou pornografii, a to ani v případě, že tyto materiály v jejich originální podobě jsou někým využity k sexuálnímu uspokojení. Výjimku by mohl představovat případ, kdy pachatel tyto materiály upraví a pornografické dílo z nich vytvoří.<sup>26</sup>

### **3.1 Objekt**

Objektem tohoto trestného činu je dle Šámala zájem společnosti na ochraně mravního vývoje dětí a ochraně před jejich sexuálním zneužíváním. Objekt je rozšířen i na osoby, které se jeví být dětmi, což potvrzuje rozsudek Nejvyššího soudu ČR ze dne 28. dubna 2021, sp. zn. 8 Tdo 271/2021. Tímto rozšířením zákonodárce sleduje ochranu nejen samotných dětí před pornografií, ale rovněž snahu o zamezení poptávky po dětské pornografii.<sup>27</sup>

### **3.2 Objektivní stránka**

Objektivní stránka uvedeného trestného činu je specifická, jelikož je vymezena ve 4 základních skutkových podstatách.

#### **3.2.1 Objektivní stránka uvedená v odst. 1**

Objektivní stránkou základní skutkové podstaty uvedené v odst. 1 tohoto trestného činu, je samotné přechovávání dětské pornografie. Za přechovávání se považuje

---

<sup>25</sup> ČESKO. § 192 odst. 1 zákona č. 40/2009 Sb., trestní zákoník ve znění pozdějších předpisů ze dne 8. ledna 2009. In: *Zákony pro lidi* [online]. [cit. 2026-03-14]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-40>

<sup>26</sup> Srov. ŠÁMAL, Pavel. *Trestní zákoník: komentář*. III, § 272-421. 3. vydání. Velké komentáře. V Praze: C.H. Beck, 2023. s. 2398 - 2408 ISBN 978-80-7400-893-1

<sup>27</sup> Srov. Tamtéž s. 2398 - 2040

jakékoli trvalejší držení materiálu, které dává pachateli možnost s ním nakládat, ať už na fyzickém nosiči (např. pevný disk, USB flash disk) nebo v digitálním úložišti (např. cloudové úložiště).

Přechovávání v digitálním prostředí je chápáno jako stav, kdy má osoba nad konkrétním materiálem kontrolu a může s ním podle své vůle nakládat. Pro naplnění skutkové podstaty trestného činu není rozhodující, zda jsou data uložena přímo na pevném disku počítače. Postačuje, pokud k nim má pachatel přístup a může je ovládat, například v rámci e-mailové schránky nebo na vzdáleném cloudovém úložišti.

Významným interpretačním vodítkem v této oblasti je judikatura Nejvyššího soudu ČR, konkrétně usnesení sp. zn. 6 Tdo 551/2014, které konstatuje, že trestní odpovědnost je konstituována již samotným okamžikem nabytí dispoziční moci nad materiálem. Časový rozsah, po který byl materiál držen, není podmínkou pro primární kvalifikaci trestného činu, avšak představuje relevantní přitěžující okolnost v rámci procesu individualizace trestu.

Je však nutné odlišovat vědomé držení dat od automatických technických operací, ke kterým dochází při práci s internetem. Za trestné přechovávání se nepovažuje ukládání dočasných souborů, ke kterému dochází automaticky (např. mezipaměť prohlížeče – cache nebo soubory cookies). Specifickou kategorií představuje streamování, tedy online prohlížení obsahu bez jeho faktického stažení. Protože při streamování uživatel soubor trvale neovládá ani neukládá na své médium, nenaplnňuje toto jednání znaky přechovávání podle prvního odstavce příslušného zákona. Takové jednání je však trestně postižitelné podle jiných ustanovení, která se zaměřují na samotné sledování zakázaného materiálu.<sup>28</sup>

### **3.2.2 Objektivní stránka uvedena v odst.**

Podle § 192 odst. 2 TZ je trestně odpovědný ten, „*kdo prostřednictvím informační nebo komunikační technologie získá přístup k dětské pornografii.*“<sup>29</sup> Tato skutková podstata se odlišuje od přechovávání uvedeného v odst. 1 tím, že postihuje pouhé získání přístupu. Zásadní je zde prvek využití informačních nebo komunikačních technologií, což reflektuje specifika online prostředí. Získání přístupu lze chápat jako aktivní činnost

<sup>28</sup> Srov. Tamtéž s. 2398 - 2408

<sup>29</sup> ČESKO. § 192 odst. 2 zákona č. 40/2009 Sb., trestní zákoník ve znění pozdějších předpisů ze dne 8. ledna 2009. In: *Zákony pro lidi* [online]. [cit. 2026-03-14]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-40>

pachatele směřující k tomu, aby se mu dětská pornografie stala dostupnou, aniž by ji nutně musel trvale ukládat na své zařízení. Může jít například o prohlížení streamovaného obsahu, otevření souboru v online úložišti bez stažení, nebo přístup na webovou stránku obsahující dětskou pornografii. Tato formulace zdůrazňuje prevenci a snahu zamezit i pasivní konzumaci takového materiálu, která stimuluje poptávku.

Tato skutková podstata byla do českého právního řádu implementována novelou č. 141/2014 Sb. jako přímý odraz požadavků směrnice Evropského parlamentu a Rady 2011/93/EU. Cílem této úpravy je postihovat i vědomé vyhledávání a prohlížení nelegálního obsahu v online prostředí, čímž dochází k naplnění mezinárodních závazků v boji proti pohlavnímu vykořisťování dětí.<sup>30</sup>

Zde se dle autora projevuje propojení s problematikou digitálních stop, neboť i takovýto zdánlivě pomíjivý přístup zanechává v kyberprostoru detekovatelné stopy, jak bylo uvedeno v podkapitole 2.5.

### 3.2.3 Objektivní stránka uvedená v odst. 3

Navazující § 192 odst. 3 TZ stanovuje přísnější tresty za širší spektrum aktivit, které přesahují pouhé přechovávání či získání přístupu: „Kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem, anebo kdo kořistí z takového pornografického díla, bude potrestán odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci.“<sup>31</sup> Jednotlivé formy objektivní stránky definované v tomto odstavci mají následující specifika, kdy Šámal odkazuje při jejich popisu na komentář k § 191 TZ:

- **Výroba** představuje jakékoli zhotovení pornografického díla zobrazujícího dítě. Nejedná se pouze o průmyslovou či řemeslnou produkci, nýbrž i o činnosti jako fotografování dětské pornografie, natáčení filmů či jiných záznamů s takovým

---

<sup>30</sup> Srov. ŠÁMAL, Pavel. *Trestní zákoník: komentář*. III, § 272-421. 3. vydání. Velké komentáře. V Praze: C.H. Beck, 2023. s. 2398 - 2408 ISBN 978-80-7400-893-1

<sup>31</sup> ČESKO. § 192 odst. 3 zákona č. 40/2009 Sb., trestní zákoník ve znění pozdějších předpisů ze dne 8. ledna 2009. In: *Zákony pro lidi* [online]. [cit. 2026-03-14]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-40>

obsahem, nebo vytváření počítačových či jiných animací. Není rozhodné, zda je dílo vyráběno pro vlastní potřebu pachatele či pro potřebu jiné osoby. Za výrobu je rovněž považováno ukládání audiovizuálního či vizuálního přenosu dětské pornografie z webové kamery náležející oběti na harddisk počítače pachatele prostřednictvím počítačové sítě.

- **Dovoz, vývoz, průvoz:** Tyto termíny se vztahují na přeshraniční pohyb materiálu dětské pornografie. Ačkoliv pouhé stahování dat prostřednictvím internetu ze serveru umístěného v jiném státě není automaticky považováno za dovoz či vývoz, import nebo export může být uskutečněn přenosem počítačových dat (např. e-mailovou poštou) nebo na fyzických nosičích informací. Dovoz, vývoz a průvoz mohou být realizovány jak pro vlastní, tak pro cizí potřebu.
- **Nabídka** dětské pornografie zahrnuje jakékoli předložení takového díla s cílem, aby si jej jiná osoba převzala. Motivy pro převzetí (např. prodej, směna, darování, výpůjčka) nejsou relevantní, stejně jako není podstatné, zda je nabídka uskutečněna za úplatu či bezplatně. Pro naplnění skutkové podstaty není rozhodující, zda adresát nabídku skutečně přijme.
- **Zprostředkování** spočívá v určité formě pomoci, kdy pachatel působí jako prostředník mezi osobou nabízející a osobou, která si opatřuje dětskou pornografií. Činnost pachatele může zahrnovat zprostředkování nabídky i poptávky (včetně fyzického kontaktu), ale v digitálním prostředí se často jedná o zprostředkování přístupu k webovým či jiným internetovým stránkám s dětskou pornografií, například zasláním odkazu, sdělením hesla nebo přístupového kódu, či zřízením dálkového přístupu k serveru s takovým obsahem.
- **Uvedení** dětské pornografie **do oběhu** představuje jednání pachatele, jehož cílem je, aby se pornografické dílo v originále či v kopiích dostalo k širšímu okruhu osob. Pro naplnění této skutkové podstaty není nezbytné, aby se s obsahem skutečně seznámil širší okruh lidí, neboť trestné je již počáteční jednání pachatele, které má za následek zpřístupnění díla.<sup>32</sup> Jak vyplývá z judikatury, k naplnění pojmu „uvádění do oběhu“ postačuje, aby se předmět stal přístupným více lidem, jelikož se jedná o ohrožovací trestný čin, kde se nevyžaduje zjištění, zda se s obsahem skutečně seznámili.<sup>33</sup>

---

<sup>32</sup> Srov. ŠÁMAL, Pavel. *Trestní zákoník: komentář*. III, § 272-421. 3. vydání. Velké komentáře. V Praze: C.H. Beck, 2023. s. 2387-2397 ISBN 978-80-7400-893-1

<sup>33</sup> Srov. rozhodnutí Nejvyššího soudu ČR sp. zn. 1 Tz 33/1986

Rozdíl mezi § 191 TZ a 192 TZ je ten, že u dětské pornografie je za trestné považováno také kořistění z dětského pornografického díla, což je považováno za čtvrtou základní skutkovou podstatu tohoto trestného činu.

Pod pojmem **kořistění** se rozumí jakýkoli způsob získávání majetkového prospěchu z dětské pornografie. Trestně odpovědná může být například osoba, která za úplatu pronajme prostor využívaný k výrobě takového díla, nebo za úplatu zhotoví reklamní předměty související s touto činností. Dále sem spadá pronájem prostoru na vlastním serveru pro ukládání dětské pornografie nebo úplatné umístění odkazu na webové stránky s takovým obsahem. Nezbytnou podmínkou pro naplnění této skutkové podstaty je vědomost pachatele o tom, že se jedná o pornografické dílo zobrazující děti.<sup>34</sup>

### **3.2.4 Rozdíl mezi přímým držením a vzdáleným přístupem přes Informační a komunikační technologie (dále jen IKT)**

V kontextu dynamického rozvoje informačních a komunikačních technologií se trestná činnost stále častěji přesouvá do kyberprostoru, což klade zvýšené nároky na orgány činné v trestním řízení při jejím odhalování a dokazování. Obzvláště závažným fenoménem je šíření dětské pornografie online, které profituje z anonymity a globálního dosahu internetu, a proto se stále častěji přesouvá do kyberprostoru, což naznačují také data získaná od policejního prezidia, zmíněná v úvodu této práce. Pochopení charakteru kybernetické kriminality a specifik elektronických důkazů je proto stěžejní pro efektivní boj proti tomuto druhu trestné činnosti.

V rámci páchaní trestné činnosti související s dětskou pornografií v online prostředí je klíčové rozlišovat mezi dvěma základními formami přístupu k tomuto materiálu: držením (přechováním) a vzdáleným přístupem. Každá z těchto forem má odlišné právní implikace a vyžaduje specifické postupy při vyšetřování a dokazování ze strany OČTŘ.

---

<sup>34</sup> Srov. ŠÁMAL, Pavel. *Trestní zákoník: komentář*. III, § 272-421. 3. vydání. Velké komentáře. V Praze: C.H. Beck, 2023. s. 2398 - 2040 ISBN 978-80-7400-893-1

### 3.2.5 Přímé držení

Tato forma páčání spočívá v aktivním stahování a ukládání obsahu dětské pornografie na lokální úložiště, jako jsou pevné disky počítačů, externí disky, paměťové karty, cloudová úložiště pod přímou kontrolou pachatele nebo mobilní zařízení. V tomto případě má pachatel fyzickou kontrolu nad digitálním souborem, který je trvale uložen v jeho držení. K zajištění takového důkazu je často nutná fyzická operace OČTŘ s cílem zabavit a forenzně analyzovat příslušné médium. Pro účely dokazování je stěžejní prokázat úmysl pachatele materiál držet, jelikož jak bylo zmíněno při analýze skutkových podstat, ke spáchání těchto trestných činů je zapotřebí úmyslného jednání pachatele.<sup>35</sup> Toto jednání reflektuje skutkovou podstatu uvedenou v § 192 odst. 1 TZ.

### 3.2.6 Vzdálený přístup přes IKT

Až do 31.7.2014 nebyl vzdálený přístup k dětské pornografii, přes komunikační technologie trestný, což se změnilo novelou trestního zákoníku, platnou od 1.8.2014, kdy došlo k promítnutí požadavku vyplývajícího z článku 5 odst. 3 směrnice. Ustanovení vyžaduje, aby se i vědomé získávání přístupu k dětské pornografii prostřednictvím informačních a komunikačních technologií trestalo, a to odnětím svobody s horní hranicí trestní sazby nejméně jeden rok.<sup>36</sup>

Získat přístup k dětské pornografii znamená mít prostřednictvím informační a komunikační technologie možnost prohlédnout si dětskou pornografii, přičemž při tomto pouhém prohlížení pachatel pornografické dílo, které zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem, nepřevádí do svého držení, tedy jej ještě nepřechovává ve smyslu odstavce 1, jehož znaky by naplnil až tím, že by si, byť některé, soubory stáhl a uložil na nosič informací.

Definičním znakem je prostředek, kterým si pachatel získá přístup. Musí se tak díť prostřednictvím informační nebo komunikační technologie. Oba výrazy sice mají svůj obsah, ale jejich oddělování nebude mít praktický význam. Výraz informační

---

<sup>35</sup> Srov. SMEJKAL, Vladimír. *Kybernetická kriminalita*. Pro praxi. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. s. 192 -196 ISBN 978-80-7380-501-2

<sup>36</sup> Srov. SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV. \*Úřední věstník Evropské unie\*, 17.12.2011, L 335 s. 8

a komunikační technologie (v angl. zkratce ICT) má vystihnout úzké propojení technologií informačních (v angl. zkratce IT) a komunikačních. I počítačové systémy propojené v síti musí spolu při výměně dat komunikovat, k čemuž využívají jak technického (hardware), tak programového (software) vybavení. V praxi se bude nejčastěji jednat o využití internetu k přístupu k dětské pornografii.<sup>37</sup> Jednání popsané výše reflektuje skutkovou podstatu uvedenou v § 192 odst. 2 TZ.

### 3.3 Subjekt

Pachatelem může být jakákoliv fyzická osoba, která splňuje obecné znaky trestného činu, ale také právnická osoba, neboť tento trestný čin, není uveden v § 7 zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob ve znění pozdějších předpisů (dále jen TOPO).<sup>38</sup>

### 3.4 Subjektivní stránka

Subjektivní stránka všech uvedených základních skutkových podstat trestného činu podle § 192 TZ vyžaduje úmyslné zavinění, v souladu s § 13 odst. 2 TZ, avšak postačí i úmysl eventuální, což je specifikováno v § 15 odst. 1 písm. b) a § 15 odst. 2 TZ.<sup>39</sup>

### 3.5 Kvalifikovaná skutková podstata uvedená v § 192 odst. 4 TZ

Odstavec § 192 4 TZ stanovuje další okolnost podmiňující použití vyšší trestní sazby, která zní: *“Odnětím svobody na dvě léta až šest let nebo propadnutím majetku bude pachatel potrestán, spáchá-li čin uvedený v odstavci 3 a) jako člen organizované skupiny, b) tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem, nebo c) v úmyslu získat pro sebe nebo pro jiného značný prospěch.”*<sup>40</sup>

---

<sup>37</sup> Srov. ŠÁMAL, Pavel. *Trestní zákoník: komentář*. III, § 272-421. 3. vydání. Velké komentáře. V Praze: C.H. Beck, 2023. s. 2398 – 2408 ISBN 978-80-7400-893-1

<sup>38</sup> Srov. Tamtéž s. 2398 - 2040

<sup>39</sup> Srov. Tamtéž

<sup>40</sup> ČESKO. § 192 odst. 4 zákona č. 40/2009 Sb., trestní zákoník ve znění pozdějších předpisů ze dne 8. ledna 2009. In: *Zákony pro lidi* [online]. [cit. 2026-03-14]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-40>

Tato skutková podstata výrazně zpřísňuje trestní sazbu za jednání popsaná v odstavci 3, tedy za výrobu, dovoz, vývoz, provedení, nabídnutí, veřejné zpřístupnění, zprostředkování, uvedení do oběhu, prodej nebo jiné opatření dětské pornografie, anebo kořistění z ní. Zvýšená trestní sazba, konkrétně odnětí svobody na dvě léta až šest let nebo propadnutí majetku, je aplikována v případě naplnění některé z následujících okolností:

- Pojmem **organizovaná skupina** se v kontextu trestního práva rozumí sdružení více osob, v jehož rámci je provedena určitá dělba úkolů mezi jednotlivé členy. Činnost takové skupiny se vyznačuje plánovitostí a koordinovaností, což zvyšuje pravděpodobnost úspěšného provedení trestného činu a tím i jeho celkovou společenskou škodlivost. **Členem** je myšlen kdokoli, kdo se na činnosti skupiny vědomě podílí a plní konkrétní, předem stanovené úkoly v rámci společného plánu, a to bez ohledu na to, zda zastává roli vedoucího či vykonavatele. Pro naplnění tohoto znaku nestačí pouhá nahodilá součinnost, ale vyžaduje se aktivní zapojení do vnitřní struktury skupiny a akceptování koordinovaného postupu.<sup>41</sup>
- Za **tisk** se považuje jakékoli mechanické nebo chemické rozmnožení textu, znaku či obrazu (např. pomocí tiskařského lisu, fotokopírky, rotaprintu), jehož výsledkem je tiskovina. Zahrnuje veškeré periodické (noviny, časopisy) i neperiodické publikace (knihy, sborníky), přičemž podstatný je obsah tiskoviny, její uspořádání a případné výtvarné zpracování.
- **Filmem** se zde rozumí děj, text nebo obraz zachycený na filmový pás, určený k veřejnému promítání, tedy krátkometrážní i dlouhometrážní filmy určené k veřejné produkci. Do této kategorie se neřadí televizní filmy a inscenace, které spadají pod pojem televize.
- **Rozhlasem** je veřejné šíření řeči, zvuků a hudby z jednoho místa na dálku k posluchačům prostřednictvím elektrických signálů rádiovou cestou nebo vedením, bez ohledu na frekvenci či provozovatele. Lokální a závodní rozhlasové systémy sem nejsou primárně zařazeny, mohou však spadat pod "jiný obdobně účinný způsob".
- **Televize** představuje sdělovací prostředek pro přenos pohyblivých obrazů elektrickou cestou na dálku k divákům, založený na principu rychlého rozkladu

---

<sup>41</sup> Srov. Rozhodnutí Nejvyššího soudu ČSR ze dne 28. 5. 1976, sp. zn. 4 To 13/76

obrazu na elementární body, přenosu informací o jejich světlosti a barvě a následném znovusestavení v televizním přijímači.

- **Veřejně přístupná počítačová síť** označuje funkční propojení počítačů do sítí s cílem vytvořit informační systém pracující s dálkovým přístupem, jehož hlavním představitelem je internet a podobné informační systémy. Z technického hlediska jde o soustavu serverů, datových komunikací a připojených počítačů; z organizačního hlediska zahrnuje provozovatele sítí, poskytovatele připojení a uživatele. Internet jako globální síť vznikl propojením původně privátních sítí, které se postupně staly veřejnými a přístupnými. Rozhodující byl vznik služby WWW (World Wide Web) v letech 1992 až 1993, která umožnila tvorbu a propojení webových stránek prostřednictvím hypertextových odkazů a multimédií. Klíčovou podmínkou je veřejná přístupnost, což vylučuje uzavřené podnikové či organizační sítě.
- Termín **jiný obdobně účinný způsob** pokrývá veškeré další, dosud neexistující nebo specifické metody, které mají srovnatelnou kapacitu pro masové a efektivní šíření dětské pornografie, a které by v budoucnu mohly vzniknout.<sup>42</sup>
- **Úmysl získat pro sebe nebo pro jiného značný prospěch**, jak vyplývá z § 138 odst. 1, 2 TZ, značný prospěch činí nejméně 1 000 000 Kč. Značný prospěch může mít pachatel v úmyslu získat jak pro sebe, tak i pro jiného.<sup>43</sup>

Pro naplnění okolností podmiňující použití vyšší trestní sazby uvedených v § 192 odst. 4 TZ je vyžadováno úmyslné zavinění, neboť podle § 17 písm. b) TZ se vyžaduje úmysl, pokud zákon výslovně nestanoví, že postačí zavinění z nedbalosti. V případě § 192 odst. 4 TZ takové ustanovení chybí.<sup>44</sup>

### 3.6 Kvalifikovaná skutková podstata uvedená v § 192 odst. 5 TZ

Odstavec § 192 5 TZ zní: „Odnětím svobody na tři léta až osm let nebo propadnutím majetku bude pachatel potrestán, spáchá-li čin uvedený v odstavci 3 a) jako člen organizované skupiny působící ve více státech, nebo b) v úmyslu získat pro sebe

---

<sup>42</sup> Srov. ŠÁMAL, Pavel. *Trestní zákoník: komentář*. III, § 272-421. 3. vydání. Velké komentáře. V Praze: C.H. Beck, 2023. s. 2387-2397 ISBN 978-80-7400-893-1

<sup>43</sup> Srov. Tamtéž s. 2397-2408

<sup>44</sup> Srov. Tamtéž

nebo pro jiného prospěch velkého rozsahu.“<sup>45</sup> Tento odstavec představuje další stupeň zpřísnění trestní odpovědnosti za jednání související s dětskou pornografií, přičemž se zaměřuje na nejzávažnější formy páčání, které jsou spjaty s organizovaným zločinem mezinárodního charakteru a rozsáhlým finančním prospěchem. Na základě této okolnosti podmiňující použití vyšší trestní sazby je možné dále navýšit trestní sazbu za činy popsané v odstavci 3 (výroba, dovoz, vývoz, zprostředkování, šíření, kořistění atd.). Konkrétně je možné uložit trest odnětí svobody na tři léta až osm let, nebo propadnutí majetku, v případě naplnění některé z následujících okolností:

- Je-li pachatel **člen organizované skupiny působící ve více státech**. Organizovaná skupina je považována za působící ve více státech, jsou-li její aktivity vykonávány nejméně ve dvou státech, přičemž jedním z nich může být Česká republika.<sup>46</sup>
- Úmysl získat pro sebe nebo pro jiného prospěch velkého rozsahu: Prospěch velkého rozsahu je definován v § 138 odst. 1 a 2 TZ a jeho minimální hodnota činí 10 000 000 Kč. Pachatel může mít v úmyslu získat tento prospěch buď pro sebe, nebo pro jinou osobu. Jedná se o nejvyšší kvantitativní hranici prospěchu, která je upravena TZ.<sup>47</sup>

Závěrem lze konstatovat, že aplikace § 192 TZ v online prostředí představuje pro OČTŘ specifickou výzvu danou charakteristikami kyberprostoru, jako je globálnost a anonymita. Judikatura v tomto směru poskytuje důležitá vodítka pro výklad jednotlivých znaků skutkové podstaty. Klíčovým je v tomto směru například rozsudek Nejvyššího soudu ČR ze dne 28. dubna 2021, sp. zn. 8 Tdo 271/2021, který sjednotil výklad objektu trestného činu tak, že ochrana se vztahuje i na osoby, které se dětmi jeví být (tzv. zdánlivá dětská pornografie). Tento výklad sice zvyšuje ochranu obětí, ale zároveň klade specifické nároky na dokazování a expertízu při posuzování věku zobrazených osob.

---

<sup>45</sup> ČESKO. § 192 odst. 5 zákona č. 40/2009 Sb., trestní zákoník ve znění pozdějších předpisů ze dne 8. ledna 2009. In: *Zákony pro lidi* [online]. [cit. 2026-03-14]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-40>

<sup>46</sup> Srov. Usnesení Nejvyššího soudu ČR ze dne 15. 7. 2004, sp. zn. 5 Tdo 794/2004

<sup>47</sup> Srov. ŠÁMAL, Pavel. *Trestní zákoník: komentář*. III, § 272-421. 3. vydání. Velké komentáře. V Praze: C.H. Beck, 2023. s. 2408 ISBN 978-80-7400-893-1

## 4 Zneužití dítěte k výrobě pornografie podle § 193 TZ

Tato kapitola se věnuje analýze trestného činu zneužití dítěte k výrobě pornografie podle § 193 TZ. Zatímco § 192 TZ se zaměřuje na nakládání s již existující dětskou pornografií, § 193 TZ postihuje samotný akt aktivního zapojení dítěte do jejího vzniku, čímž představuje přímou formu sekundární viktimizace. Tento paragraf je dle názoru autora klíčový pro ochranu dětí před nejzávažnějšími formami sexuálního vykořisťování, které v online prostředí nabývají nových, často zákeřných podob.

Základní skutková podstata tohoto trestného činu je formulována následovně: *„Kdo přiměje, zjedná, najme, zláká, svede, nebo zneužije dítě k výrobě pornografického díla, nebo kořistí z účasti dítěte na takovém pornografickém díle, bude potrestán odnětím svobody na jeden rok až pět let.“*<sup>48</sup>

### 4.1 Objekt

Objektem daného trestného činu je společenský zájem na ochraně dětí před sexuálním zneužíváním, zajištění jejich řádného mravního a citového vývoje a ochrana svobody jejich rozhodování. Z tohoto důvodu je zvýšená ochrana poskytována osobám mladším osmnácti let, zejména s ohledem na jejich zneužití k produkci pornografického materiálu. Je důležité poznamenat, že pojem výroba v tomto kontextu nemusí vždy implikovat přímé zneužití dané osoby, neboť zahrnuje i činnosti jako rozmnožování pornografických fotografií, střih a zpracování filmového materiálu či produkci videokazet a DVD z již existujících zdrojů.<sup>49</sup>

### 4.2 Objektivní stránka

Objektivní stránka daného trestného činu je definována především dvěma základními okruhy jednání pachatele. Prvním z nich je přiměnění, zjednání, najmutí, zlákáání, svedení nebo zneužití dítěte k výrobě pornografického díla. Druhým je pak

---

<sup>48</sup> ČESKO. § 193 odst. 1 zákona č. 40/2009 Sb., trestní zákoník ve znění pozdějších předpisů ze dne 8. ledna 2009. In: *Zákony pro lidi* [online]. [cit. 2026-03-14]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-40>

<sup>49</sup> Srov. ŠÁMAL, Pavel. *Trestní zákoník: komentář*. III, § 272-421. 3. vydání. Velké komentáře. V Praze: C.H. Beck, 2023. s. 2408 ISBN 978-80-7400-893-1

kořistění z účasti dítěte na takovém pornografickém díle. První skupina jednání vykazuje paralelu s návodem podle § 24 odst. 1 písm. b) TZ, zatímco druhá je podobná legalizaci výnosů z trestné činnosti (§ 216 TZ). Detailněji lze jednotlivé způsoby jednání specifikovat následovně:

- **Přimění** dítěte k výrobě pornografického díla může být dosaženo jak využitím vlivu vyplývajícího ze vzájemného vztahu pachatele a dítěte, tak i násilím či jinými donucovacími prostředky, což potvrzuje také Usnesení Nejvyššího soudu ČR ze dne 9. 12. 2015, sp. zn. 6 Tdo 1398/2015.
- **Zjednáním** se rozumí uzavření dohody, a to i konkludentní, mezi dítětem a pachatelem o účasti dítěte na výrobě pornografického díla, přičemž tato dohoda předpokládá souhlasný projev vůle obou stran.
- **Najmutí** představuje specifickou formu zjednání, kdy dohoda zahrnuje úplatu, jež nemusí být výhradně peněžní povahy.
- **Zlákáním** je získání dítěte k účasti prostřednictvím předestírání různých výhod či pozitiv, a to zejména v situaci, kdy dítě váhá, avšak bez přímé úhrady.
- **Svedení** spočívá v úmyslném vyvolání rozhodnutí v dítěti ze strany pachatele účastnit se výroby pornografického díla, a to jinými prostředky než zlákáním.<sup>50</sup>
- **Zneužití** dítěte může nastat ze strany osoby, která má vůči němu práva a/nebo povinnosti (např. rodič nebo jiná pečující osoba), avšak nemusí jít o formálně ustavený vztah. V případě zneužívání může pachatel jednat zcela bez ohledu na vůli dítěte, například jeho uvedením v omyl (např. prezentováním uměleckého či lékařského účelu snímků) nebo využitím jeho omylu či stavu snížené přičetnosti (např. pod vlivem alkoholu nebo omamných látek).<sup>51</sup>
- **Kořistěním** se v tomto kontextu rozumí jakýkoli způsob získávání majetkového prospěchu nebo jiné výhody (například formou protislužby), který pramení z účasti dítěte na výrobě pornografického díla. Mezi typické případy takového jednání lze zařadit například činnost řidiče, jenž za úplatu přepravuje dítě na místo produkce pornografie, vizážisty poskytujícího dítěti své služby za finanční odměnu, nebo osoby placené za doprovod či zabavení dítěte. Podstatné je, aby tato osoba jednala s vědomím skutečného účelu své činnosti. Toto pojetí má analogii v § 192 odst. 3 TZ, avšak s důležitým rozdílem. Pachatel trestného činu

---

<sup>50</sup> Srov. Tamtéž s. 2408 - 2412

<sup>51</sup> Srov. usnesení Nejvyššího soudu ČR ze dne 9. 12. 2015, sp. zn. 6 Tdo 1398/2015

podle § 192 odst. 3 TZ kořistí z jednání týkajícího se výroby, dovozu či vývozu dětské pornografie, tedy přímo z pornografického díla jako takového. Naproti tomu v případě § 193 TZ se kořistění vztahuje výhradně na účast dítěte na výrobě pornografického díla, což činí toto ustanovení užším a speciálnějším ve svém záběru jednání.<sup>52</sup>

### 4.3 Subjekt

Stejně jako u § 192 TZ může být pachatelem jakákoliv fyzická, nebo právnická osoba, jelikož tento trestný čin není uveden v § 7 TOPO.<sup>53</sup>

### 4.4 Subjektivní stránka

Předmětný trestný čin je klasifikován jako úmyslný skutek v souladu s ustanovením § 13 odst. 2 TZ. K naplnění subjektivní stránky trestného činu postačuje úmysl eventuální, přičemž se vyžaduje, aby pachatel disponoval vědomostí a srozuměním s faktem, že se jedná o osobu mladší osmnácti let, která je zneužívána k výrobě pornografie nebo k profitování z její účasti.<sup>54</sup>

### 4.5 Kvalifikovaná skutková podstata v § 193 odst. 2 a 3 TZ

Kvalifikovaná skutková podstata uvedená v odstavci v § 193 odst. 2 zní: „Odnětím svobody na dvě léta až šest let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 a) jako člen organizované skupiny, nebo b) v úmyslu získat pro sebe nebo pro jiného značný prospěch.“<sup>55</sup> Z této formulace vyplývá, že uvedená skutková podstata je totožná se skutkovou podstatou stanovenou v § 192 odst. 4 TZ, přičemž podrobnější popis jednotlivých druhů jednání byl již prezentován v kapitole 3.7. Obdobně, v kapitole 3.8. bylo analyzováno jednání definované v § 192 odst. 5 TZ, které vykazuje shodu se

---

<sup>52</sup> Srov. ŠÁMAL, Pavel. *Trestní zákoník: komentář*. III, § 272-421. 3. vydání. Velké komentáře. V Praze: C.H. Beck, 2023. s. 2408 - 2412 ISBN 978-80-7400-893-1

<sup>53</sup> Srov. ŠÁMAL, Pavel; DĚDIČ, Jan; GŘIVNA, Tomáš a PÚRY, František. *Trestní odpovědnost právnických osob: komentář*. 2. vydání. V Praze: C.H. Beck, 2018. s. 135 ISBN 978-80-7400-592-3.

<sup>54</sup> Srov. ŠÁMAL, Pavel. *Trestní zákoník: komentář*. III, § 272-421. 3. vydání. Velké komentáře. V Praze: C.H. Beck, 2023. s. 2408 - 2412 ISBN 978-80-7400-893-1

<sup>55</sup> ČESKO. § 193 odst. 2 zákona č. 40/2009 Sb., trestní zákoník ve znění pozdějších předpisů ze dne 8. ledna 2009. In: *Zákony pro lidi* [online]. [cit. 2026-03-14]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-40>

zněním skutkové podstaty popsané v § 193 odst. 3 TZ, jež stanoví: „*Odnětím svobody na tři léta až osm let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 a) jako člen organizované skupiny působící ve více státech, nebo b) v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.*”<sup>56</sup>

Trestný čin zneužití dítěte k výrobě pornografie podle § 193 TZ představuje dle autora jednu z nejbrutálnějších forem sexuálního zneužívání dětí, která je navíc umocněna možnostmi digitálního prostředí. Jeho účinné potírání vyžaduje nejen robustní právní rámec, ale především neustálý rozvoj technických a forezních kapacit orgánů činných v trestním řízení, stejně jako intenzivní mezinárodní spolupráci. Pochopení a adresování těchto výzev je stěžejní pro splnění cíle této práce a pro ochranu nejzranitelnějších členů společnosti.

---

<sup>56</sup> ČESKO. § 192 odst. 3 zákona č. 40/2009 Sb., trestní zákoník ve znění pozdějších předpisů ze dne 8. ledna 2009. In: *Zákony pro lidi* [online]. [cit. 2026-03-14]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-40>

## 5 Navazování nedovolených kontaktů s dítětem podle § 193b TZ

Tato kapitola se zaměřuje na analýzu § 193b TZ, který upravuje trestný čin navrhování setkání s dítětem v úmyslu spáchat sexuálně motivovaný trestný čin. Tento paragraf představuje klíčový preventivní nástroj trestního práva pro ochranu dětí před online groomingem a sexuálním vykořisťováním, přičemž postihuje přípravné jednání směřující k závažnějším skutkům.

V následujícím textu jsou rozebrány zákonné znaky skutkové podstaty, specifika úmyslu pachatele a aplikační praxe, s odkazy na judikaturu a komentáře, což umožňuje lepší pochopení role § 193b TZ v boji proti této formě kriminality v digitálním prostředí. Tato analýza představuje základní kámen pro následující podkapitoly o souvisejících paragrafech a jejich aplikaci v online prostředí.

Základní skutková podstata trestného činu podle § 193b TZ zní: “ *Kdo navrhne setkání dítěti mladšímu patnácti let v úmyslu spáchat trestný čin podle § 187 odst. 1, § 192, 193, § 202 odst. 3 nebo jiný sexuálně motivovaný trestný čin, bude potrestán odnětím svobody až na dvě léta.*<sup>57</sup>

### 5.1 Objekt

Primárním chráněným zájmem v případě tohoto ustanovení, obdobně jako u souvisejících skutkových podstat, je ochrana dítěte mladšího patnácti let. Konkrétně je cílem právní úpravy chránit jeho mravní a tělesný vývoj před navazováním předčasných sexuálních kontaktů a v konečném důsledku před sexuálním zneužíváním. Pro naplnění subjektivní stránky trestného činu přitom není nezbytné, aby došlo k reálnému narušení mravního či tělesného vývoje dítěte; postačuje pouhá možnost hypotetického vzniku takové ohrožující situace.<sup>58</sup>

---

<sup>57</sup> ČESKO. § 193b zákona č. 40/2009 Sb., trestní zákoník ve znění pozdějších předpisů ze dne 8. ledna 2009. In: *Zákony pro lidi* [online]. [cit. 2026-03-14]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-40>

<sup>58</sup> Srov. ŠÁMAL, Pavel. *Trestní zákoník: komentář*. III, § 272-421. 3. vydání. Velké komentáře. V Praze: C.H. Beck, 2023. s. 2416 - 2419 ISBN 978-80-7400-893-1

## 5.2 Objektivní stránka

Objektivní stránka skutkové podstaty je naplněna jednáním pachatele, který navrhne setkání dítěti mladšímu patnácti let za zvláštního tzv. druhého úmyslu spáchat některý z vyjmenovaných trestných činů podle § 187 odst. 1, § 192, § 193, § 202 odst. 3 TZ nebo jiný sexuálně motivovaný trestný čin.

Setkáním se v tomto kontextu rozumí fyzické, reálné a osobní střetnutí pachatele s dítětem v reálném světě (tzv. kontakt „face-to-face“). Nejde tedy o pouhé pokračování komunikace ve virtuálním prostoru, ale o záměrné vyvolání situace, kdy se obě osoby ocitnou ve vzájemné bezprostřední fyzické přítomnosti na určitém místě. Samotný návrh na takové setkání může být učiněn jakýmkoliv způsobem, nejčastěji však prostřednictvím informačních a komunikačních technologií v rámci fenoménu zvaného *cybergrooming*. Pro naplnění zákonných znaků je rozhodující povaha zvolených formulací (případně i piktogramů či plynulého užití emotikonů), ze kterých lze dovodit záměr pachatele směřující k získání důvěry dítěte za účelem následné realizace sexuálních praktik.<sup>59</sup>

Cílem právní úpravy je trestně postihnout přípravné jednání směřující k sexuálně motivovaným skutkům, které nesplňují znaky zvláště závažných zločinů podle § 14 odst. 3 TZ, a u nichž tedy není příprava samostatně trestná. Jedná se tak o tzv. předčasně dokonaný delikt, což potvrzuje také Usnesení Nejvyššího soudu ČR ze dne 25. 11. 2020, sp. zn. 8 Tdo 1041/2020.

## 5.3 Subjekt

Subjektem trestného činu podle § 193b TZ může být kterákoli fyzická osoba, neboť se v tomto případě nevyžaduje žádná specifická vlastnost, způsobilost či postavení pachatele. Jedná se tedy o tzv. obecný subjekt. Dle § 7 TOPO, je rovněž možné, aby se tohoto trestného činu dopustila právnická osoba.<sup>60</sup>

---

<sup>59</sup> Srov. Tamtéž s. 2416 - 2419

<sup>60</sup> Srov. ŠÁMAL, Pavel; DĚDIČ, Jan; GRIVNA, Tomáš a PÚRY, František. *Trestní odpovědnost právnických osob: komentář*. 2. vydání. V Praze: C.H. Beck, 2018. s. 135 ISBN 978-80-7400-592-3.

## 5.4 Subjektivní stránka

Pro naplnění skutkové podstaty daného trestného činu je dle ustanovení § 13 odst. 2 TZ vyžadováno úmyslné zavinění. Tento úmysl, byť ve formě srozumění, musí specificky zahrnovat i skutečnost, že předmětem útoku je osoba mladší patnácti let. V případě, že by došlo ke skutkovému omylu negativnímu týkajícímu se věku oběti, byla by v souladu s § 18 odst. 1 TZ vyloučena trestní odpovědnost za spáchání tohoto deliktu.<sup>61</sup>

Závěrem lze konstatovat, že trestný čin dle § 193b TZ tvoří dle autora esenciální pilíř v boji proti zneužívání dětí, jehož účinné potírání vyžaduje neustálou adaptaci právních, technických a forenzních postupů na rychle se vyvíjející online realitu.

---

<sup>61</sup> Srov. ŠÁMAL, Pavel. *Trestní zákoník: komentář*. III, § 272-421. 3. vydání. Velké komentáře. V Praze: C.H. Beck, 2023. s. 2416 - 2419 ISBN 978-80-7400-893-1

## **6 Analýza Směrnice 2011/93/EU o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii**

Ochrana dětí před sexuálním zneužíváním a vykořisťováním, včetně boje proti dětské pornografii, představuje jednu z priorit Evropské unie. V reakci na rostoucí výskyt této trestné činnosti, zejména v souvislosti s rozvojem online prostředí, což potvrzuje tabulka o vývoji v této trestné činnosti, která byla zmíněna již v úvodu této práce, přijala Evropská unie směrnici, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV. Tato směrnice si klade za cíl harmonizovat právní úpravy členských států a posílit mezinárodní spolupráci v oblasti prevence, vyšetřování a stíhání pachatelů, jakož i v ochraně obětí. Její význam spočívá především ve sjednocení definic klíčových pojmů a v závazku členských států kriminalizovat specifické formy jednání související s dětskou pornografií a sexuálním zneužíváním dětí.

Tato směrnice představuje klíčový právní nástroj pro boj proti pohlavnímu zneužívání a vykořisťování dětí, který sjednocuje definice a požadavky na kriminalizaci napříč členskými státy EU. Jejím cílem je zajistit, aby činy jako dětská pornografie nebo sexuální zneužívání dětí byly ve všech členských zemích postihovány obdobně a účinně.<sup>62</sup>

Jádrem boje proti dětské pornografii je její jednoznačná definice, která umožňuje efektivní právní postih. Článek 2 písm. c) směrnice definuje dětskou pornografii, kdy tato identifikace byla již zmíněna v kapitole 3 této práce. Tato definice je široká a zahrnuje rozsáhlou škálu vizuálního materiálu, včetně realistických i fiktivních vyobrazení, která jsou určena pro sexuální účely.<sup>63</sup>

Dále se směrnice komplexně zabývá různými formami pohlavního zneužívání a vykořisťování dětí v článcích 3 až 7, které vyžadují, aby členské státy kriminalizovaly širokou škálu jednání, včetně sexuálního zneužívání dětí, dětské prostituce, nucené účasti

---

<sup>62</sup> Srov. SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV. \*Úřední věstník Evropské unie\*, 17.12.2011, L 335 s. 1-7

<sup>63</sup> Srov. Tamtéž s. 1-7

děti na pornografických představeních a podněcování k pohlavnímu zneužívání dětí. Důraz je kladen na ochranu dětí mladších 18 let, přičemž jsou stanoveny minimální věkové hranice pro souhlas se sexuálním jednáním a jsou zdůrazněny situace, kdy souhlas dítěte nemůže být platný. Směrnice rovněž explicitně zmiňuje zneužívání informačních a komunikačních technologií k navazování kontaktu s dětmi pro sexuální účely.<sup>64</sup>

## 6.1 Propojení směrnice a TZ

Skutková podstata trestného činu dle § 192 TZ, pokrývající nedovolenou výrobu dětské pornografie, úzce koreluje s požadavky směrnice na kriminalizaci produkce a jiného nakládání s dětskou pornografií, což je zmíněno ve čl. 4. Tímto ustanovením je zajištěn postih za vytváření, pořizování a šíření materiálu, který dle definice směrnice a trestního zákoníku zobrazuje sexuální jednání dětí.

Trestný čin pohlavního zneužití podle § 193 TZ pak cílí na ochranu dětí před přímým sexuálním zneužitím, což zahrnuje i případy zneužití dítěte k výrobě pornografie. Zde se postihuje zneužití bezbrannosti, důvěry či závislosti dítěte, nebo vykonání soulože či jiného pohlavního styku s osobou mladší patnácti let, přičemž motivace k výrobě pornografie představuje zvlášť závažný aspekt takového jednání.

Ustanovení § 193b TZ, týkající se navazování nedovolených kontaktů s dítětem, přímo odpovídá článku 6 směrnice, který požaduje kriminalizaci navazování kontaktu s dětmi k sexuálním účelům, zejména prostřednictvím informačních a komunikačních technologií. Tím je zajištěn postih za tzv. grooming, tedy snahu pachatelů navázat s dítětem kontakt za účelem spáchání sexuálního deliktu.

Obě ustanovení reflektují podstatu směrnice o ochraně dětí před sexuálním zneužíváním a vykořisťováním, a to i s ohledem na věkovou hranici a neschopnost dítěte dát platný souhlas. Důležitým aspektem je zde též úmyslné zavinění pachatele, které se musí vztahovat i na skutečnost, že předmětem útoku je dítě mladší patnácti let. Směrnice navíc výslovně uznává, že dětská pornografie, která sestává z vyobrazení pohlavního zneužívání dětí, a jiné zvlášť závažné formy pohlavního zneužívání a pohlavního vykořisťování dětí stále narůstají a šíří se pomocí nových technologií a internetu. Tato

---

<sup>64</sup> Srov. Tamtéž s. 1-7

realita, kdy se pachatelům v online prostředí otevírá široká škála možností, jak svou činnost anonymizovat a ztížit identifikaci, klade zvýšené nároky na vyšetřovací orgány. Česká legislativa, včetně trestního zákoníku, je s těmito dynamikami online prostředí do značné míry v souladu, neboť definice trestných činů dle § 192, § 193 a § 193b TZ a související trestní sazby jsou aplikovatelné bez ohledu na to, zda k činu došlo v offline nebo online světě.<sup>65</sup>

Dle názoru autora lze konstatovat, že česká právní úprava, zejména trestní zákoník a trestní řád, je s požadavky směrnice do značné míry v souladu. Definice dětské pornografie, skutkové podstaty pohlavního zneužívání a vykořisťování dětí, jakož i procesní nástroje pro vyšetřování a stíhání, reflektují principy a minimální standardy stanovené směrnicí. Důraz je kladen na ochranu dětí jako nejzranitelnější skupiny a na účinné postihování pachatelů.

## **6.2 Ochrana obětí a prevence ve směrnici**

Články 18 až 20 směrnice se věnují právům obětí, jejich ochraně a podpoře. Zahrnují ustanovení o přístupu obětí k informacím, právu na podporu, ochranu soukromí, odškodnění a specializovanou pomoc. Členské státy mají zajistit, aby oběti dostaly komplexní podporu odpovídající jejich specifickým potřebám.<sup>66</sup> Tato ustanovení jsou v České republice reflektována v zákoně č. 45/2013 Sb., o obětech trestných činů ve znění pozdějších předpisů, který stanovuje práva obětí, včetně práva na informace, právní pomoc, psychologickou a sociální podporu a odškodnění. Specifický přístup je uplatňován právě u dětí jako zvláště zranitelných obětí.

Součástí směrnice jsou také požadavky na prevenci pohlavního zneužívání a vykořisťování dětí, včetně osvěty a vzdělávání, zejména v online prostředí.

Česká republika se těmito požadavkům věnuje prostřednictvím různých kampaní, vzdělávacích programů a činnosti nevládních organizací, které se zaměřují na prevenci a zvyšování povědomí o rizicích spojených s online komunikací a dětskou pornografií.<sup>67</sup>

---

<sup>65</sup> Srov. Tamtéž s. 1-14

<sup>66</sup> Srov. Tamtéž s. 12

<sup>67</sup> Srov. Chmelík, Jan. *Mravnost, Pornografie a Mravnostní Kriminalita*. Vyd. 1. Praha: Portál, 2003 s. 33-40 ISBN 80-7179-739-6

## 7 Způsoby zajišťování dat

### 7.1 Zajištění nosiče dat

V tomto případě se dle autora jedná o ten jednodušší způsob zajištění dat. Nosiče, či zařízení, na nichž se data spojená s dětskou pornografií uchovávají, může pachatel dobrovolně vydat na základě ustanovení § 78 zákona č. 141/1961 Sb. o trestním řízení soudním ve znění pozdějších předpisů (dále jen TRŘ), kde je psáno: „*Kdo má u sebe věc důležitou pro trestní řízení, je povinen ji na vyzvání předložit soudu, státnímu zástupci nebo policejnímu orgánu; je-li ji nutno pro účely trestního řízení zajistit, je povinen věc na vyzvání těmto orgánům vydat.*“<sup>68</sup>

Osoba, jež má věc vydat, musí být poučena o následcích neuposlechnutí výzvy. V případě odmítnutí vydání může být věc, kromě uložení pořádkového opatření, odňata na základě rozhodnutí státního zástupce nebo policejního orgánu (s předchozím souhlasem státního zástupce). Při odnětí věci by měla být přítomna nezúčastněná osoba a o celém úkonu (jak vydání, tak odnětí) je nutné pořídit podrobný protokol, který přesně identifikuje zajištěnou věc a její příslušen, aby nemohla být zaměněna. Osoba vydávající nebo, již je věc odňata, musí obdržet potvrzení nebo opis protokolu, což musí být rovněž v protokolu zaznamenáno.<sup>69</sup>

Další možností zajištění zařízení nebo nosičů informací obsahujících relevantní data je v rámci domovní prohlídky nebo prohlídky jiných prostor. Tyto prohlídky může nařídit předseda senátu, a v přípravném řízení soudce na návrh státního zástupce. Jde o specifické rozhodnutí, proti kterému není přípustné odvolání. Samotný příkaz musí být písemný a řádně odůvodněný. Podobně jako při vydání a odnětí věcí, je nezbytné při prohlídkách zajišťovat zařízení a nosiče s náležitou odbornou péčí a pořízený protokol by měl obsahovat detailní technickou specifikaci nejen zajištěných předmětů, ale i postupu

---

<sup>68</sup> ČESKO. § 78 zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád). In: *Zákony pro lidi* [online]. [cit. 2026-03-14]. Dostupné z: <https://www.zakonyprolidi.cz/cs/1961-141>

<sup>69</sup> Srov. ŠÁMAL, Pavel. *Trestní řád: komentář*. 7., dopl. a přeprac. vyd. Velké komentáře. V Praze: C.H. Beck, 2013.s. 1014 - 1026 ISBN 978-80-7400-465-0

příslušného orgánu. Z tohoto důvodu by se takové prohlídky měly ideálně konat za účasti náležitě vyškoleného vyšetřovatele nebo znalce.<sup>70</sup>

Praktický postup při zajišťování zařízení a datových nosičů musí vyvažovat požadavek zdrženlivosti a přiměřenosti orgánů činných v trestním řízení, zakotvených v § 2 odst. 1 a § 52 TŘ, s požadavky na efektivní a bezpečné zajištění důkazního materiálu, které vyplývají z volatelní povahy digitálních dat a specifik zařízení. V situaci, kdy je zajišťován samostatný, nepřipojený datový nosič nebo vypnuté zařízení, je postup relativně jednoduchý: věci se řádně identifikují v protokolu a zapečetí do antistatického vaku. Zajištění by mělo probíhat tak, aby přístup k uchovaným datům mohl mít jako první znalec, proto je vhodné zapečetit veškerá rozhraní zařízení nebo celé zařízení vložit do zapečetitelného obalu.

Pokud však policejní orgán zajišťuje zařízení, které je v provozu, je situace komplikovanější. Odpojení a vypnutí zařízení by totiž mohlo vést nejen ke ztrátě některých dat, ale i ke ztrátě přístupu k datům na vzdáleném úložišti nebo k zašifrovaným datům v zařízení. Před odpojením je proto nutné provést protokolované ohledání věci dle § 113 TŘ, při němž se ověří, zda je zařízení zabezpečeno šifrováním, zda umožňuje přístup do vzdálených služeb, či zda neexistují jiné překážky pro forenzní analýzu. V průběhu ohledání je doporučeno pořídit fotodokumentaci nebo videozáznam, které se přiloží k protokolu. Po ohledání je třeba zařízení zajistit tak, aby nedošlo ke kompromitaci dat jejich smazáním nebo úpravou. Měly by být odpojeny veškeré periferie, zařízení kompletně vypnuto a zapečetěno do antistatického vaku. Je-li to možné, preferuje se zajišťování celých zařízení namísto pouze demontovaných datových úložišť nebo bitových kopií dat, neboť jejich zpřístupnění může být vázáno na konkrétní zařízení (např. prostřednictvím TPM čipu). Tento postup však nelze vždy uplatnit; pokud by zajištění celého zařízení představovalo neodůvodněný zásah do základních práv a svobod držitele, je vhodné provést pouze ohledání nebo zajistit pouze otisky datových nosičů. Vždy je třeba zohlednit specifika a okolnosti konkrétního případu a možnost následného využití institutů vydání a odnětí věci.<sup>71</sup>

---

<sup>70</sup> Srov. POLČÁK, Radim; PÚRY, František a HARAŠTA, Jakub. *Elektronické důkazy v trestním řízení*. Spisy Právnické fakulty Masarykovy univerzity v Brně. Řada teoretická, Edice Scientia. Brno: Masarykova univerzita, 2015. s. 101 ISBN 978-80-210-8073-7

<sup>71</sup> srov. Tamtéž s. 102 - 103

## 7.2 Zajištění vzdálených dat

Vedle přímého zajištění fyzických zařízení existuje druhý způsob získávání elektronických důkazů, který se týká dat uložených ve vzdálených úložištích nebo službách.

Jednou z metod zajišťování vzdálených dat je zajištění dat, které jsou volně dostupné v síti. Pokud není nutné překonávat žádná bezpečnostní opatření, lze k takovému obsahu přistupovat a pořizovat z něj důkazní prostředky bez dalších omezení. V tomto případě je však klíčové dodržet pravidla pro ohledání věci dle § 112 TŘ, což zahrnuje sepsání podrobného protokolu. S ohledem na specifické vlastnosti elektronických dat a dynamické fungování internetu je nezbytné zajistit vhodnou a komplexní dokumentaci. Například při ohledání webové stránky se sice mohou pořizovat fotografie nebo snímky obrazovky, avšak pro zajištění maximálního množství důkazního materiálu a s ohledem na potenciální dynamičnost webu se doporučuje uchovat i její zdrojový kód.<sup>72</sup>

Pokud se jedná o data, která nejsou volně dostupná v síti a jsou nějakým způsobem zabezpečena, lze k nim získat přístup prostřednictvím dobrovolně poskytnutých přístupových údajů, například během výslechu nebo podání vysvětlení. OČTŘ k nim mohou přistupovat pouze na základě předchozího povolení soudce, nebo pokud s tím výslovně souhlasí osoba, do jejíž práv a svobod je tím zasahováno. Pro využití těchto dat jako důkazu je nezbytné sepsat řádný protokol, který musí obsahovat informaci o způsobu získání přístupu a výslovný souhlas dotčené osoby.<sup>73</sup>

---

<sup>72</sup> srov. Tamtéž s. 103 - 104

<sup>73</sup> srov. Tamtéž s. 104

## 8 Praktická část

Teoretická část této práce vymezila právní a kriminologické aspekty související s nelegálním zobrazováním a přechováváním dětské pornografie. Praktická část na tyto poznatky navazuje a klade si za cíl podrobně analyzovat, jakým způsobem OČTŘ v reálné praxi postupují při odhalování, dokumentaci a prokazování této specifické trestné činnosti v online prostředí.

Dětská pornografie v digitální podobě představuje pro vyšetřovatele unikátní výzvu. Na rozdíl od klasických stop je digitální stopa (soubor, log, přístup do cloudu) extrémně náchylná k znehodnocení, či smazání, a to i na dálku. Hlavním cílem tohoto výzkumu je tedy identifikovat kritická místa v procesu dokazování, posoudit technickou vybavenost policie v první linii a zhodnotit efektivitu právních nástrojů při potírání distribuce tohoto závadového obsahu na cloudových a streamingových platformách.

### 8.1 Metodologie a technika sběru dat

Pro naplnění cílů práce byla zvolena metoda kvalitativního výzkumu. Vzhledem k vysoké odbornosti a citlivosti tématu dětské pornografie bylo jako nejvhodnější technika zvoleno expertní dotazování. Tato metoda umožňuje hloubkovou analýzu problémů, které nelze statisticky zachytit, jako jsou procesní strategie obhajoby, technické limity forenzních programů nebo praktické zkušenosti s mezinárodní právní pomocí.

Výzkum byl realizován prostřednictvím strukturovaných dotazníků, které byly distribuovány vybraným odborníkům z řad policie, justice a advokacie. Dotazníky byly tematicky rozděleny tak, aby reflektovaly specifika vyšetřování kyberkriminality se zaměřením na mravnostní delikty páchané na dětech.

„V souvislosti se stanoveným cílem práce byly pro praktickou část definovány tři hlavní výzkumné otázky, které budou značeny jako VO1 – VO3:

- **VO1:** Jaká jsou hlavní technická a procesní rizika při prvotním zajišťování digitálních stop s obsahem dětské pornografie na úrovni základních útvarů?

- **VO2:** Jakými nástroji a s jakou efektivitou dokážou OČTŘ prokazovat faktickou moc nad nelegálním obsahem uloženým v cloudových úložištích?
- **VO3:** Jakým způsobem se v rozhodovací praxi OČTŘ a obhajoby liší nahlížení na streaming dětské pornografie oproti jejímu fyzickému držení?“

## 8.2 Charakteristika respondentů

Aby výzkum poskytl komplexní pohled na problematiku dětské pornografie páchané v online prostředí, byl seznam respondentů sestaven tak, aby reprezentoval celý procesní řetězec trestního řízení. Pro zajištění objektivit byla využita metoda triangulace dat (porovnání pohledů různých stran).

Složení skupiny respondentů:

- Policisté sloužící na obvodního oddělení, v této skupině byli dotazováni členové prvosledové hlídky, zpracovatel běžné obecné trestné kriminality, specialista na kyberkriminalitu a zástupce vedoucího oddělení pro trestní řízení (označení R1, R2, R3, R4)
- Pracovníci služby kriminální policie a vyšetřování (dále jen SKPV), v této skupině byl proveden výzkum s vyšetřovatelem obecné kriminality na krajské úrovni a dvěma operativci z problematiky mravnostní kriminality s více než 20 lety zkušeností jak z okresní, tak krajské úrovně (označení R5, R6, R7)
- Státní zástupci Okresního státního zastupitelství zabývající se nejen problematikou kyberkriminality (označení R8, R9)
- Obhájci (označení R10, R11)

Vzhledem k povaze zkoumaného tématu jsou veškerá vyjádření respondentů v textu anonymizována. Citace a závěry jsou uváděny pod kódy R1 až R11, aby byla zachována ochrana osobních údajů expertů i taktika vyšetřování konkrétních útvarů. Veškerá data byla využita výhradně pro účely této bakalářské práce s důrazem na identifikaci systémových nedostatků při potírání online distribuce dětské pornografie.

## 9 Analýza prvotního zajištění a zajištění dětské pornografie

Prvním a kritickým bodem celého procesu dokazování trestné činnosti související s dětskou pornografií je moment prvotního zajištění nosiče dat. Tato fáze je rozhodující pro zachování integrity digitální stopy, která je, jak bylo uvedeno v teoretické části, extrémně náchylná k znehodnocení.

### 9.1 Technické bariéry

Z výzkumného šetření vyplývá zásadní rozpor mezi metodickými požadavky na zajišťování digitálních stop a reálnými možnostmi policistů na obvodních odděleních. Respondenti z řad prvosledových hlídek a zpracovatelů na OOP (R1, R2, R3, R4) shodně uvádějí, že k detekci dětské pornografie dochází nejčastěji náhodně.

R4 (zástupce vedoucího OOP) uvádí: „Většinou jde vyloženě o náhodné oznámení, například někdo přinese nalezený telefon nebo bývalá partnerka oznámí nález nelegálního obsahu.“ V takové chvíli je policista postaven před úkol zajistit zařízení tak, aby nedošlo k dálkovému smazání dat pachatelem. Zde se však naráží na fatální nedostatek technického vybavení.

R1 (člen prvosledové hlídky) k tomu dodává: „Doted' jsem ani netušil, že PČR disponuje nějakými antistatickými sáčky či stínícími pouzdry na mobilní telefony.“ Obdobně se vyjadřuje i R2 (zpracovatel obecné kriminality), který potvrzuje absenci speciálních pomůcek na útvaru. V praxi to znamená, že mobilní telefon s podezřením na výskyt dětské pornografie je vložen do běžné papírové obálky, čímž zůstává aktivně připojen k síti.

Tento stav je v přímém rozporu s nároky, které na digitální důkaz kladou státní zástupci. R9 (státní zástupce) sice uvádí, že „v praxi k závažným procesním vadám při zajišťování důkazů nedochází“, nicméně tento optimismus nesdílejí specialisté ani obhajoba.

Absence stínících pouzder (Faradayových klecí) na obvodních odděleních vytváří prostor pro dálkovou manipulaci se zařízením (např. přes službu Find My iPhone nebo

Google Find My Device). Pokud pachatel stihne data vymazat dříve, než je zařízení předáno specialistům SKPV k forenzní analýze, dochází k nevratné ztrátě klíčového důkazu dětské pornografie.

Právě na tyto technické nedostatky se zaměřuje strategie obhájců. R11 (obhájce) v dotazníku otevřeně přiznává, že nedostatečná dokumentace integrity je pravidelným bodem útoku na obžalobu: *„Pokud policie nepoužije stínící pouzdro a zařízení zůstane online, mohlo dojít k modifikaci dat na dálku. Jakmile vyšetřovatel nemůže doložit, že se obsah disku od momentu zajištění nezměnil ani o jeden bit, je celý důkaz procesně mrtvý.“*

Tento postoj potvrzuje i R10 (obhájce), který jako častý argument uvádí zneužití zařízení jinou osobou (např. přes otevřenou Wi-Fi). Bez precizního zajištění hned na místě činu je pro policii extrémně těžké tyto námitky vyvrátit.

## **9.2 Personální a metodické limity**

Dalším identifikovaným problémem je neochota nebo nemožnost výjezdových skupin SKPV zasahovat u každého nálezu. R4 (zástupce vedoucího OOP) popisuje negativní praxi: *„Dost často se stává, že i na věci, které by mělo zpracovávat SKPV, výjezd nepřijede. Prostě se řekne, ať to obvod nabere a potom postoupí.“*

Výsledkem je stav, kdy složitou agendu dětské pornografie v online prostředí zajišťují policisté, kteří se dle slov R1 necítí proškoleni prakticky vůbec. Školení formou teoretických prezentací bez praktického nácviku zajišťování elektroniky vnímají respondenti z první linie jako neefektivní a sloužící pouze k formálnímu vykázání činnosti pro vedení.

## 10 Prokazování faktické dispozice a role cloudových úložišť

S rozvojem technologií se těžiště důkazních materiálů v souvislosti s dětskou pornografií přesouvá z pevných disků počítačů na cloudová úložiště a streamingové platformy. Pro OČTŘ to znamená nutnost prokázat tzv. faktickou moc nad daty, tedy že pachatel měl k obsahu vědomý a ovladatelný přístup.

### 10.1 Technické nástroje a forenzní analýza

Klíčovou rolí v této fázi hrají specialisté SKPV. R5 (vyšetřovatelka krajské úrovně) uvádí, že pro prokázání faktické moci nad daty na vzdálených serverech jsou zásadní důkazní prostředky jako vlastnictví přístroje a znalost přístupových hesel. K dokumentaci četnosti a způsobu přístupu pak specialisté využívají pokročilé forenzní softwary: „*Četnost přístupů dokumentujeme v programech Cellebrite Reader, případně Magnet Axiom,*“ specifikuje R5.

Tyto nástroje umožňují vyšetřovatelům zrekonstruovat historii uživatele a odlišit náhodné zobrazení od aktivního vyhledávání a třídění dětské pornografie. R6 (operativce SKPV) doplňuje, že silným důkazem jsou zejména logy o dvoufázovém ověření (např. potvrzovací SMS nebo e-mail) a evidence plateb provozovateli vzdáleného úložiště. Pokud pachatel za úložiště se závadovým obsahem pravidelně platí, je argumentace náhodným přístupem prakticky vyloučena.

Zajímavým aspektem je prokazování úmyslu v případech, kdy pachatel v zařízení neuchovává samotné soubory, ale pouze databáze odkazů na nelegální obsah. R6 (SKPV) uvádí, že se v praxi setkávají spíše s přístupy na Darkweb, odkud směřují odkazy na konkrétní cloudová úložiště.

V těchto případech probíhá prokazování úmyslu skrze ohledávání zařízení na specializovaných pracovištích oddělení analytiky a kybernetické kriminality za přítomnosti obhájce. Jak uvádí R6, prokazování je sice složitější, ale skrze analýzu historie prohlížeče a specifické komunikace v rámci komunit sdílejících dětskou pornografii je možné úmyslné zavinění dovést.

## 10.2 Mezinárodní spolupráce

Největší překážkou při dokumentaci dětské pornografie v online prostředí zůstává fakt, že data jsou často fyzicky uložena na serverech mimo jurisdikci České republiky. R5 (vyšetřovatelka) i R9 (státní zástupce) se shodují, že mezinárodní právní pomoc je v této oblasti extrémně zdlouhavá.

R5 v dotazníku upozorňuje na existenci institutu datafreezing, což znamená zmrazení dat u zahraničního subjektu prostřednictvím Národní centrály proti terorismu, extremismu a kybernetické kriminalitě SKPV (dále jen NCTEKK), který by měl sloužit k okamžitému zajištění důkazů. Zároveň však dodává: „*V praxi se z důvodu přílišné zdlouhavosti prakticky nevyužívá.*“ To v kombinaci s poznatkami z kapitoly 9 (riziko dálkového smazání) vytváří situaci, kdy je vyšetřování dětské pornografie na mezinárodních platformách často odsouzeno k neúspěchu kvůli pomalé reakci systému.

## 10.3 Námitky obhajoby

Zatímco policie sází na forenzní software, obhajoba se zaměřuje na zpochybnění identity uživatele v okamžiku přístupu. R11 (obhájce) uvádí: „*Dnes hodně pracujeme s fenoménem sdílených rodinných účtů. Pokud má rodina jeden iCloud pro pět lidí, policie velmi těžko dokazuje, kdo konkrétně nelegální soubor nahrál.*“

Tato námitka vytváří tlak na kvalitu policejní práce. R8 (státní zástupce) v reakci na to zdůrazňuje, že pouhé určení zařízení (IP adresy) často nestačí a je nezbytné provést podrobné vyhodnocení digitálního řetězce, který propojí konkrétní soubor s konkrétním profilem a aktivitou dané osoby v čase.

## 11 Právní kvalifikace, systémové limity

Tato kapitola se věnuje právnímu posouzení moderních forem konzumace dětské pornografie a identifikuje systémové překážky, které brání efektivnímu postihu pachatelů v online prostředí.

### 11.1 Přechovávání vs. streaming

S rozvojem vysokorychlostního internetu dochází k posunu od stahování souborů k jejich online sledování (streamování). Z hlediska trestního práva vyvstává otázka, zda je pouhý přístup k obsahu bez jeho trvalého uložení stejně škodlivý jako klasické přechovávání.

R8 (státní zástupce) v tomto směru zastává striktní výklad zákona: *„Přechovávání na nosiči je § 192 odst. 1 TZ, získání přístupu v úložišti (streaming) postihuje § 192 odst. 2 TZ. Odstavec 3 a vyšší jsou pak popsány tak obecně, že na formě vlastně nezáleží.“* Z jeho pohledu tedy digitální forma (fyzický soubor vs. streaming) nehraje pro naplnění skutkové podstaty zásadní roli.

Naproti tomu R9 (rovněž státní zástupce) poukazuje na aplikační praxi soudů: *„Mám za to, že v praxi jsou případy 'pouhého' streamingu postihovány méně přísně, neboť soudy při ukládání trestu vždy posuzují závažnost konkrétního případu.“* Tento rozpor mezi literou zákona a soudní praxí vnímá obhajoba jako prostor pro zmírnění trestů u klientů, u nichž nebyla prokázána aktivní distribuce či tvorba sbírek dětské pornografie.

Zatímco u fyzického nosiče je úmysl zřejmý, u online platform se OČTŘ potýkají s prokazováním vědomí pachatele o nelegálnosti obsahu. R5 (vyšetřovatelka SKPV) uvádí jako nejčastější úskalí *„množství zajištěných dat, která je nutno fyzicky vyhodnotit“*, aby bylo možné vyloučit verzi o náhodném prokliku na klamavý odkaz.

Obhajoba (R10, R11) na tento fakt často sází. R11 (obhájce) namítá, že OČTŘ často zaměňuje zobrazení za přechovávání. *„Pokud klientovi vyskočí pornografický banner a on na něj klikne, není to úmyslné držení. Bez důkazu o aktivním vyhledávání specifických klíčových slov je prokazování úmyslu pouhá spekulace žalobce,“* uvádí R11.

## 11.2 Systémové limity

Výzkum odhalil hlubokou roztržitost nejen v technickém vybavení, ale i v legislativě. R8 (státní zástupce) vidí největší slabinu v roztržitosti úpravy zajišťování digitálních stop: „*Odstranit roztržitost právní úpravy a duplicity a triplicity – viz např. chceme-li logy, je to § 88a TR, chceme-li monitorovat komunikaci, je to § 88 TR...*“ Tato nepřehlednost vede k tomu, že i drobná procesní chyba může znehodnotit důkaz o dětské pornografii.

Důležitým zjištěním je také rozdíl v součinnosti poskytovatelů. R5 (vyšetřovatelka) i R6 (operativce) se shodují, že zatímco tuzemští poskytovatelé spolupracují bez problémů, u zahraničních subjektů je vymahatelnost dat téměř nulová bez zdlouhavých mezinárodních smluv.

## 11.3 Vzdělání a odbornost jako limitující faktor

Závěrečným identifikovaným tématem je kritický nedostatek praktického vzdělávání v první linii. Respondenti z obvodních oddělení (R1, R2, R4) vnímají současný systém školení jako formální. R1 (člen prvosledové hlídky) k tomu uvádí: „*Školení odbornosti spočívá v tom, že cca dvě hodiny je výklad teorie doslovným čtením prezentace a na konci se vypracuje test. Vedení si odškrtně splnění, ale v terénu stále nevíme, jak správně zajistit mobil, aby nedošlo k vymazání.*“

Tato „formální odbornost“ je největší slabinou, neboť, jak uvádí R4 (zástupce vedoucího OOP), policista v první linii nese odpovědnost za prvotní úkony, ale při chybě se za něj v důsledku chybějící metodiky nikdo nepostaví.

## 12 Shrnutí výzkumu

Cílem praktické části bylo identifikovat a kriticky zhodnotit postupy OČTŘ při potírání trestné činnosti v souvislosti s dětskou pornografií v online prostředí. Na základě analýzy vyjádření jedenácti respondentů z praxe (R1 – R11) lze formulovat komplexní závěry, které odkrývají hlubokou propast mezi legislativními požadavky, technickými možnostmi a každodenní policejní praxí.

### 12.1 Odpovědi na výzkumné otázky

**Jaká jsou hlavní technická a procesní rizika při prvotním zajišťování digitálních stop s obsahem dětské pornografie?**

Výzkum odhalil, že nejkritičtější článkem řetězce digitálního dokazování je prvotní zásah na úrovni obvodních oddělení. Zatímco teoretické příručky mluví o sterilitě digitálního prostředí, respondenti z obvodních oddělení (R1, R2, R4) popsali stav materiální nouze. Zásadním zjištěním je absolutní absence Faradayových klecí a stínících obalů na základních útvarech. V kontextu dětské pornografie, kde pachatelé často využívají cloudová úložiště se synchronizací v reálném čase, je toto pochybení fatální.

Jakmile je zařízení (např. chytrý telefon) zajištěno do standardní papírové obálky bez odpojení od sítě, zůstává „živým“ cílem. Tento technický deficit přímo nahrává strategii obhajoby (R10, R11), která může u soudu úspěšně argumentovat možností dálkové manipulace s daty. Dochází tak k paradoxu: policie sice zajistí nosič s dětskou pornografií, ale kvůli chybějícímu vybavení za pár set korun může dojít ke zpochybnění důkazu v hodnotě měsíců vyšetřování.

**Jak efektivně dokáže policie prokazovat „faktickou moc“ nad nelegálním obsahem v cloudu a na streamingových platformách?**

V oblasti forenzní analýzy (fáze po zajištění) je situace výrazně optimističtější. Specialisté SKPV (R5, R6) prokázali vysokou úroveň odbornosti při práci s nástroji jako Cellebrite a Magnet Axiom. Prokazování faktické moci se již neopírá o pouhou

přítomnost souboru, ale o tzv. digitální otisk uživatele – tedy kombinaci logů o dvoufázovém ověření, plateb za úložiště a historie vyhledávání.

Značným problémem však zůstává mezinárodní prvek. Respondenti (R5, R9) se shodli, že právní rámec pro okamžité zmrazení dat v zahraničí (datafreezing) je v praxi „mrtvým institutem“ pro svou extrémní zdlouhavost. U dětské pornografie, která je často hostována na anonymních zahraničních serverech, se tak vyšetřování často zastaví u hranic České republiky, což vede k faktické beztrestnosti šířitelů operujících mimo EU.

### **Existuje shoda v právním nahlížení na streaming dětské pornografie a jaké jsou limity prokazování úmyslu?**

Diskuse mezi státními zástupci (R8, R9) a obhájci (R11) ukázala, že „streaming“ je právně stále nejednoznačnou oblastí. Přestože novela TZ v rámci § 192 odst. 2 postihuje získání přístupu k dětské pornografii, obhajoba se úspěšně soustředí na zpochybňování subjektivní stránky. Argumentace náhodným kliknutím nebo klamavým odkazem je v online prostředí velmi silná. Policisté v první linii (R1) přiznávají, že bez hloubkové forenzní analýzy historie prohlížeče, kterou provádí až specializovaná pracoviště, není obvodní oddělení schopno úmyslné zavinění spolehlivě doložit.

## **12.2 Zhodnocení vzdělávacího systému PČR**

Jedním z nejvýraznějších zjištění výzkumu je neefektivita současného systému vzdělávání policistů ČR. Respondent R1 (člen prvosledové hlídky) podrobil ostré kritice formalismus školení, která spočívají v pasivním čtení prezentací bez praktického nácviku. Tento názor sdílí i R4 (zástupce vedoucího OOP), který upozorňuje na nebezpečný trend: na obvodní oddělení jsou delegovány úkony (nabírání věcí), na které policisté nejsou školeni, a v případě procesní chyby nese odpovědnost konkrétní policista, nikoliv systém, který mu neposkytl vybavení. Pro vyšetřování dětské pornografie je tento stav nepřijatelný, neboť jde o jednu z nejsložitějších agend z hlediska dokazování.

## 13 Návrhy na zefektivnění boje proti dětské pornografii

Na základě provedeného výzkumného šetření a analýzy expertních vyjádření respondentů R1–R11 identifikoval autor několik kritických oblastí, které vyžadují neodkladnou pozornost. Následující návrhy jsou rozděleny na opatření technicko-organizační a legislativní.

### 13.1 Návrhy De lege ferenda

Na základě analýzy současného stavu autor konstatuje, že stávající aplikace § 192 TZ se v dynamickém online prostředí potýká s limity, které judikatura nemůže plně obsáhnout. Pachatelé využívají technologické inovace, jako jsou VPN, Tor, decentralizované sítě a šifrovaná cloudová úložiště, k efektivnímu zastírání své činnosti, což vyžaduje systémovou legislativní adaptaci. V oblasti procesního práva je pak nezbytné reagovat na roztržitost norem, kterou v rámci výzkumného šetření kritizoval zejména státní zástupce (R8).

V návaznosti na tato zjištění autor předkládá následující návrhy změn:

- **Sjednocení procesních institutů:** Autor navrhuje vytvoření ucelené hlavy v trestním řádu, která by se věnovala výhradně digitálním důkazům a specifickým postupům při práci s nimi. Současná fragmentace úpravy mezi § 88, § 88a a § 113a TŘ je v praxi nepřehledná, neodpovídá technologické realitě a zvyšuje riziko procesních vad, které mohou vést k nepoužitelnosti důkazů.
- **Zjednodušení mezinárodního zajištění dat:** Je nezbytné posílit pravomoci NCTEKK v rámci institutu *datafreezing*. Současná procesní zdlouhavost (zmíněná respondentkou R5) nahrává pachatelům dětské pornografie, kteří využívají zahraniční cloudové služby jako „bezpečný přístav“ v naději, že data budou smazána dříve, než dojde k jejich legálnímu zajištění cestou mezinárodní právní pomoci.
- **Zrychlení implementace e-Evidence:** Autor plně podporuje legislativní kroky na úrovni EU, které umožní OČTŘ přímý kontakt s poskytovateli služeb (např. Meta, Google) bez nutnosti zdlouhavých cest klasické mezinárodní právní pomoci. Tento posun, vyzdvižený respondentem R9, je klíčový pro zachování integrity digitálních stop v reálném čase.

## 13.2 Technické a materiální vybavení základních útvarů

Výzkum (zejména u respondentů R1 – R4) prokázal, že největší riziko znehodnocení digitální stopy s obsahem dětské pornografie nastává v „první linii“.

- **Povinné vybavení Faradayovými obaly:** Navrhuji, aby každé obvodní oddělení bylo povinně vybaveno sadou stínících pouzder pro mobilní telefony a tablety. Jak uvedl R11, absence tohoto vybavení je nejslabším článkem důkazního řetězce, který obhajoba pravidelně napadá. Není dostačující vybavení těmito nástroji pouze specializovaných oddělení, jelikož pracovníci těchto oddělení nejsou často k dispozici, nebo jsou zaneprázdněni.
- **Zavedení mobilních forenzních sad:** Pro prvosledové hlídky a hlídky obvodních oddělení by měly být dostupné základní sady pro fixaci „živých dat“, které by umožnily odpojit zařízení od sítě, ale zachovat jej v zapnutém stavu (powerbanky, blokátory USB zápisu).

## 13.3 Reforma systému odborného vzdělávání policistů

Současný model školení je respondenty (R1, R8) vnímán jako neefektivní.

- **Praktické simulace zajištění:** Školení by mělo být přesunuto z roviny teoretických prezentací do roviny praktických simulací na místě činu. Policisté musí mít zažitý postup, jak v rukavicích a bezpečně zajistit odemčený telefon, aniž by došlo k přepsání metadat nebo aktivaci dálkového smazání přes iCloud/Google účet.
- **Specializace na úrovni OOP:** Na každém větším obvodním oddělení by měl být určen a nadstandardně vyškolen alespoň jeden specialista na digitální stopy, který by byl garantem pro prvosledové hlídky v případě, že výjezdová skupina SKPV není k dispozici (problém zmíněný R4).

## 13.4 Metodická podpora policistů na všech úrovních

Tento návrh reaguje na nejčastější procesní obranu (R10, R11) založenou na zpochybnění identity uživatele v okamžiku přístupu k nelegálnímu obsahu. Cílem je

vytvořit závazný metodický pokyn, který naučí policisty propojovat technická data s lidským chováním.

### **Obsah metodiky (Klíčové důkazní body)**

Metodika by měla definovat povinnost shromažďovat data, která tvoří mozaiku identity:

- **Práce na místě činu** Policista na místě činu se nezaměří jen na telefon, ale na kontext. Zdokumentuje, kdo u zařízení seděl, zda bylo odemčeno biometrií (obličej/otisk) a provede okamžitý výslech k tomu, kdo další má k zařízení přístup a kdo zná heslo k domácí Wi-Fi.
- **Korelace s běžnou aktivitou:** Sledování, zda se čas přístupu k dětské pornografii shoduje s časy, kdy uživatel ze stejného zařízení prováděl běžné úkony (přihlášení do internetového bankovníctví, odesílání e-mailů, komunikace na sociálních sítích).
- **Analýza dvoufázového ověření (2FA):** Povinné dokumentování, zda byl přístup do cloudu podmíněn potvrzením v mobilním telefonu (SMS, autentizační aplikace), který má podezřelý u sebe.
- **Uživatelské zvyklosti a personalizace:** Dokumentace nastavení plochy, uložených hesel v prohlížeči a specifického způsobu třídění souborů, což vylučuje náhodné zobrazení (R5, R6).

### **Přínos pro trestní řízení**

- **Eliminace námitky „jiné osoby“:** Spojením technických logů s biometrií a bankovními identitami se okruh možných uživatelů zúží výhradně na podezřelého.
- **Průkaznost úmyslu:** Aktivní vyhledávání a následné třídění materiálů do složek jasně dokazuje vědomé přechovávání, nikoliv náhodný proklik na banner (námitka R11).
- **Standardizace kvality spisu:** Metodika zajistí, že i méně zkušený policista (R1) bude vědět, jaké důkazy musí zajistit, aby „digitální řetězec“ v pozdější fázi řízení nepraskl.

- **Kvalita digitálních důkazů:** Státní zástupce dostane ucelený „digitální podpis“ pachatele, který je u soudu prakticky nevyvratitelný běžnými námitkami o viru či otevřené Wi-Fi.

## Závěr

Předložená bakalářská práce se zabývala problematikou trestné činnosti v souvislosti s dětskou pornografií v online prostředí, přičemž hlavním cílem bylo zhodnotit efektivitu stávajících postupů orgánů činných v trestním řízení a identifikovat slabá místa v procesu dokazování. Vzhledem k dynamickému vývoji technologií a přesunu těžiště nelegálních aktivit do cloudových úložišť a na streamingové platformy se ukázalo, že tradiční metody vyšetřování již nejsou v mnoha ohledech dostačující.

V teoretické části byla provedena podrobná analýza skutkových podstat trestných činů podle § 192, § 193 a § 193b TZ a vymezeny specifické vlastnosti digitálních stop. Analýza potvrdila, že zákonná dikce, ačkoliv prošla v roce 2014 zásadní novelizací, naráží v digitálním prostředí na limity interpretace pojmu „přechovávání“. Ukazuje se, že hranice mezi pouhým přístupem (odst. 2) a faktickým držením (odst. 1) je v éře cloudových služeb a automatického mezipaměťového ukládání velmi nejasná. Právní vymezení sice pokrývá široké spektrum jednání, ale jeho efektivita je přímo závislá na schopnosti orgánů činných v trestním řízení prokázat tzv. dispoziční moc nad daty a úmyslné zavinění pachatele, což u dynamických digitálních stop představuje zásadní výzvu. Teoretický rozbor potvrdil, že klíčovým aspektem moderní kriminalistiky je zajištění integrity dat a prokazování faktické moci nad obsahem, který není fyzicky uložen na pevném disku, ale v kyberprostoru.

Praktická část, realizovaná formou expertního dotazování jedenácti respondentů (R1 – R11) z řad Policie ČR, státního zastupitelství a advokacie, přinesla zásadní poznatky o reálném stavu vyšetřování. Výzkum odhalil rozpor mezi technologickou vyspělostí pachatelů a materiálním vybavením policistů v tzv. první linii. Absence stínících pouzder a nedostatečné praktické vzdělání prvosledových hlídek představují největší riziko pro znehodnocení digitálních důkazů hned v počátku řízení. Na tyto nedostatky pak úspěšně reaguje obhajoba zpochybňováním identity uživatele a integrity dat.

Na základě zjištěných nedostatků byly v práci zformulovány konkrétní návrhy pro zefektivnění boje proti dětské pornografii. Mezi nejdůležitější patří:

- Legislativní zjednodušení mezinárodní spolupráce skrze posílení pravomocí NCTEKK a urychlenou implementaci nařízení e-Evidence, což by zamezilo využívání zahraničních serverů jako bezpečných přístavů pro nelegální obsah.
- Materiální dovybavení základních útvarů mobilními forenzními sadami pro zajištění „živých dat“.
- Vytvoření metodiky pro práci s digitálními stopami, která by sjednotila postup při prokazování subjektivní stránky trestného činu.

Závěrem lze konstatovat, že cíle práce byly naplněny. Výzkum potvrdil, že pro efektivní boj s dětskou pornografií v online prostředí je nezbytná těsná synergie mezi technickou připraveností policie, moderní legislativou a precizní procesní praxí. Boj proti této závažné trestné činnosti nesmí končit u technických limitů zastaralého vybavení, ale musí se adaptovat na realitu digitálního věku, ve kterém se odehrává.

# Seznam použitých zdrojů

## Literární zdroje

1. BRUNOVÁ, Markéta. *Dokazování trestné činnosti: s využitím kriminalistických stop a identifikace*. Eupress. Praha: Vysoká škola finanční a správní, 2019. ISBN 978-80-7408-196-5. 127 s.
2. GŘIVNA, Tomáš a POLČÁK, Radim (ed.). *Kyberkriminalita a právo*. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4. 220 s.
3. GŘIVNA, Tomáš; RICHTER, Martin a ŠIMÁNOVÁ, Hana (ed.). *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. ISBN 978-80-87284-95-7. 440 s.
4. GŘIVNA, Tomáš; ŠÁMAL, Pavel a VÁLKOVÁ, Helena. *Oběti trestných činů: komentář*. 2. vydání. Komentované zákony. V Praze: Beck, 2020. ISBN 978-80-7400-793-4. 792 s.
5. HUNT, Lynn (ed.). *The invention of pornography: obscenity and the origins of modernity, 1500-1800*. New York: Zone Books, 1993. ISBN 0-942299-68-x. 412 s.
6. CHMELÍK, Jan. *Mravnost, Pornografie a Mravnostní Kriminalita*. Vyd. 1. Praha: Portál, 2003. ISBN 80-7179-739-6. 216 s.
7. KOLOUCH, Jan. *CyberCrime*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-18-8. 524 s.
8. LAVICKÝ, Petr. *Občanský zákoník I: komentář*. 2. vydání. Velké komentáře. V Praze: C.H. Beck, 2022. ISBN 978-80-7400-852-8. 2296 s.
9. POLČÁK, Radim; PÚRY, František a HARAŠTA, Jakub. *Elektronické důkazy v trestním řízení*. Spisy Právnické fakulty Masarykovy univerzity v Brně. Řada teoretická, Edice Scientia. Brno: Masarykova univerzita, 2015. ISBN 978-80-210-8073-7. 254 s.
10. PORADA, Viktor. *Kriminalistika*. CERM 2001. ISBN 9788072041947. 746s.
11. POŠTULKA, Vladimír. *Dějiny pornografie v datech*. V Praze: XYZ, 2007. ISBN 978-80-87021-30-9. 320 s.
12. SMEJKAL, Vladimír. *Kybernetická kriminalita*. Pro praxi. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. ISBN 978-80-7380-501-2. 640 s.
13. ŠÁMAL, Pavel. *Trestní řád: komentář*. 7., dopl. a přeprac. vyd. Velké komentáře. V Praze: C.H. Beck, 2013. ISBN 978-80-7400-465-0. 4720 s.

14. ŠÁMAL, Pavel. *Trestní zákoník: komentář*. III, § 272-421. 3. vydání. Velké komentáře. V Praze: C.H. Beck, 2023. ISBN 978-80-7400-893-1. 4968 s.
15. ŠÁMAL, Pavel; DĚDIČ, Jan; GRIVNA, Tomáš a PÚRY, František. *Trestní odpovědnost právnických osob: komentář*. 2. vydání. V Praze: C.H. Beck, 2018. ISBN 978-80-7400-592-3. 992 s.
16. ŠVESTKA, Jiří. *Občanský zákoník: komentář*. 2. vyd. Velké komentáře. V Praze: C.H. Beck, 2009. ISBN 978-80-7400-108-6. 2321 s.
17. VANÍČKOVÁ, Eva. *Sexuální zneužívání dětí*. 1. Ilustroval Jiří SLÍVA. Praha: Karolinum, 1997. ISBN 80-7184-479-9. 82 s.

### Elektronické zdroje

1. <https://www.artsy.net/article/artsy-editorial-renaissance-artists-brought-pornography-masses> [citováno 2026-01-13]
2. <https://sysyphoto.wordpress.com/2019/08/20/how-the-daguerreotype-started-a-victorian-black-market-for-pornography-in-london/> [citováno 2026-01-13]
3. <https://www.loc.gov/collections/edison-company-motion-pictures-and-sound-recordings/articles-and-essays/history-of-edison-motion-pictures/origins-of-motion-pictures/?referrer=grok.com> [citováno 2026-01-13]
4. <https://endsexualexploitation.org/articles/hugh-hefner-sexual-objectification-women/> [citováno 2026-01-13]
5. RAK, Doc. Ing. Roman Ph.D a Prof. JUDr. Ing. Viktor, DrSc, dr.h.c PORADA. Vlastnosti digitálních stop a jejich dopady na forenzní šetření. Soudní inženýrství [online]. Praha: Policejní akademie ČR 2005, 2005, 16 [cit. 2026-01-15]. Dostupné z: <http://www.sinz.cz/archiv/docs/si-2005-04-183-192.pdf>

### Legislativní dokumenty

1. SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV. \*Úřední věstník Evropské unie\*,

- 17.12.2011, L 335 *Úmluva o právech dítěte a související dokumenty*. [Praha]: Ministerstvo práce a sociálních věcí ČR, 2016. ISBN 978-80-7421-120-1.
2. Ústavní zákon č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, ve znění pozdějších předpisů
  3. ČESKO. Zákon č. 40/2009 Sb., trestní zákoník ve znění pozdějších předpisů ze dne 8. ledna 2009 . In: *Zákony pro lidi* [online]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-40>
  4. ČESKO. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád). In: *Zákony pro lidi* [online]. Dostupné z: <https://www.zakonyprolidi.cz/cs/1961-141>
  5. ČESKO. Zákon č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů (zákon o obětech trestných činů). In: *Zákony pro lidi* [online]. Dostupné z: [45/2013 Sb. Zákon o obětech trestných činů](#)

## **Judikatura**

1. Usnesení Nejvyššího soudu ČR, ze dne 25. 11. 2020, sp. zn. 8 Tdo 1041/2020
2. Usnesení Nejvyššího soudu ČR, ze dne 9. 12. 2015, sp. zn. 6 Tdo 1398/2015
3. Usnesení Nejvyššího soudu ČR, ze dne 15. 7. 2004, sp. zn. 5 Tdo 794/2004
4. Usnesení Nejvyššího soudu ČR, ze dne 28. 5. 2014 sp. zn. 6 Tdo 551/2014
5. Rozhodnutí Nejvyššího soudu ČSR ze dne 28. 5. 1976, sp. zn. 4 To 13/76
6. Rozhodnutí Nejvyššího soudu ČSR ze dne 10 .6. 1986 sp. zn. 1 Tz 33/1986

## Seznam zkratek

**TZ:** zákon č. 40/2009 Sb. trestního zákoník ve znění pozdějších předpisů

**OČTR:** orgány činné v trestním řízení

**ČR:** Česká republika

**sp. zn.:** spisová značka

**např.:** například

**odst.:** odstavec

**srov.:** srovnejte

**TOPO:** trestní odpovědnost právnických osob

**TŘ:** zákon č. 141/1961 Sb. o trestním řízení soudním

**Kč:** koruna česká

**ČSR:** Československá republika

**písm.:** písmeno

**SKPV:** služba kriminální policie a vyšetřování

**PČR:** policie České republiky

**OOP:** obvodní oddělení policie

**VO:** výzkumné otázky

**IKT:** Informační a komunikační technologie

**NCTEKK:** Národní centrála proti terorismu, extremismu a kybernetické kriminalitě  
SKPV

## **Seznam příloh**

**Příloha č. 1:** tabulka vývoje trestné činnosti

**Příloha č. 2:** Vzory otázek pro rozhovory

**Příloha č. 3:** Přepisy odpovědí respondentů

# Přílohy

## Příloha 1

	(§ 192 a § 193)	(§ 193a)	(§ 192 a § 193)	(§ 193a)	(§ 192 a § 193)	(§ 193a)	(§ 192 a § 193)	(§ 193a)
Rok	registrováno		z toho objasněno		spácháno internetem		spácháno ostatními počítačovými sítěmi	
2021	627	0	334	0	480	0	20	0
2022	780	1	448	0	611	1	18	0
2023	716	2	401	2	533	2	13	0
2024	755	1	422	1	566	1	6	0
2025	0	0	0	0	0	0	0	0

Zdroj: Policejní prezidium České republiky, Odbor pro prevenci a kriminologické analýzy, Statistická data k trestné činnosti související s dětskou pornografií za roky 2021-2025. Data získaná na základě žádosti o informace podle zákona č. 106/1999 Sb.

## Příloha č. 2 Vzory otázek pro rozhovory

### Otázky pro obvodní oddělení:

1. Jak se ve vaší službě nejčastěji setkáte s podezřením na nelegální obsah (dětskou pornografií)? Jde spíše o náhodné zjištění (např. při řešení jiné věci, domácího násilí apod.), nebo o oznámení od občanů?
2. Pokud při zákroku narazíte na zapnutý počítač nebo odemčený mobilní telefon s podezřelým obsahem, co je vaším úkolem? Jak v takové chvíli postupujete, abyste data neznehodnotili?
3. Máte ve výbavě na oddělení nějaké speciální pomůcky pro zajištění elektroniky (např. antistatické sáčky, stínící pouzdra na mobily), nebo používáte běžné kriminalistické obaly?
4. Komu věc z místa činu následně předáváte a jak probíhá komunikace se specialisty z kriminální policie?
5. Cítíte se dostatečně proškoleni v tom, jak správně technicky zajistit mobil nebo PC (např. aby nedošlo k dálkovému smazání dat), nebo byste uvítali v této oblasti více praktických kurzů?

### Otázky pro SKPV

1. Jaké důkazní prostředky (vyjma samotného obsahu) považujete za klíčové pro prokázání, že pachatel měl k datům uloženým na vzdáleném serveru skutečně „faktickou moc“ a nejednalo se o náhodný přístup?
2. Setkáváte se v praxi s případy, kdy pachatel nevlastní žádná data, ale disponuje rozsáhlou databází odkazů na cloudová úložiště? Jakým způsobem se z právního

hlediska vypořádáváte s prokazováním úmyslu k přechovávání u těchto „virtuálních sbírek“?

3. Jaké procesní problémy vyvstávají při zajišťování dat, která jsou v okamžiku prohlídky otevřena v prohlížeči, ale fyzicky se nacházejí na serveru mimo jurisdikci ČR? Považujete současný právní rámec za dostatečný pro okamžité zajištění takových dat?
4. Z pohledu vyšetřovatele, jaká jsou nejčastější úskalí při dokazování, že uživatel streamovací platformy věděl, že konzumuje nelegální obsah, a nejednalo se o klamavý odkaz?
5. Jak hodnotíte právní vymahatelnost součinnosti od tuzemských poskytovatelů připojení při identifikaci koncových uživatelů v porovnání s mezinárodními platformami?
6. Pokud byste mohl/a navrhnout jednu změnu (legislativní či procesní), která by zrychlila nebo zefektivnila trestní řízení v oblasti dětské pornografie, jaká by to byla?

### **Otázky pro státní zástupce**

1. S jakými nejčastějšími nedostatky u zajištění dat se setkáváte u spisových materiálů týkajících se dětské pornografie předložených policií? (Např. nedostatečné vytěžení dat, procesní chyby při zajištění?)
2. Jaké nároky kladete na digitální důkazy, aby byly bezpečně použitelné před soudem? Stačí Vám IP adresa a logy, nebo vyžadujete vždy zajištění koncového zařízení?
3. Jaký je Váš názor na společenskou škodlivost a trestnost pouhého „vědomého přístupu“ (streaming) k dětské pornografii oproti jejímu fyzickému stažení? Měl by zákon tyto formy postihovat stejně přísně?
4. Pokud byste mohl/a navrhnout jednu změnu (legislativní či procesní), která by zrychlila nebo zefektivnila trestní řízení v této oblasti, jaká by to byla?

### **Otázky pro obhájce**

1. Jaké jsou nejčastější argumenty obhajoby v případech, kdy je klient obviněn na základě digitálních stop? (Např. zneužití Wi-Fi, virus v PC, nevědomé stahování?)
2. Setkáváte se s případy, kdy policie při zajišťování digitálních důkazů pochybila tak závažně, že byl důkaz nepoužitelný? Pokud ano, o jaký typ pochybení šlo?

3. Jak vnímáte schopnost OČTŘ prokazovat úmyslné zavinění, zejména u tzv. nahodilého přístupu k dětské pornografii na internetu (pop-up okna, nevyžádané zprávy)?
4. Je podle Vašeho názoru současná praxe OČTŘ spravedlivá v rozlišování mezi skutečnými pachateli a osobami, které se k obsahu dostaly náhodou či z nedbalosti?
5. Kde vidíte největší slabinu současného systému vyšetřování trestné činnosti v souvislosti s dětskou pornografií? (Legislativa, odbornost policie, znalecké posudky?)

### **Příloha č. 3 Přepis odpovědí respondentů**

#### **Přepis odpovědí respondenta R1 (policista prvosledové hlídky)**

1. S případem tohoto charakteru jsem se ve službě setkal naštěstí pouze jednou. Nebyla to však dětská pornografie v tom pravém slova smyslu. Nezřídka se totiž stává, že poškozené osoby na obvod dojdou oznámit, že jejich bývalý přítel/přítelkyně mají v telefonu natočené jejich intimní hrátky, kdy se obávají z jejich šíření. Toto přišla oznámit cirka před půl rokem jedna mladá slečna, avšak s rozdílem, že s ex přítelem taková videa natáčela ještě v době, kdy nebyla plnoletá. Navíc se měla dozvědět, že tato videa měl podezřelý šířit mezi svými kamarády. Situace se nepodcenila a na muže byl vydán souhlas se zadržením.
2. Já osobně nejsem technický typ, tudíž bych v tom asi tápal. Ale logicky bych věc nafotil a věcně zajistil, jako jakoukoliv jinou stopu. Nezdá se mi však, že bych v dané problematice byl nějak zvlášť proškolen. Vzpomínám si však, že když jsme podezřelému zajišťovali mobilní telefon, tak nám musel sdělit PIN kód. Mobilní telefon jsme následně v obálce předali našemu vedoucímu, který ho poté dočasně uskladnil v trezoru.
3. Domnívám se, že máme pouze obyčejné papírové obálky. Kolikrát se nám na místě stane, že ani ty nemáme, a tak jsme nuceni improvizovat a například z papíru formátu A4 jsem již několikrát skládal jakousi obálku na stopu. Doteď jsem ani netušil, že PČR disponuje nějakými antistatickými sáčky, či stínícími pouzdry na mobilní telefony.
4. Jak jsem již zmínil, osobně jsem věc řešil pouze jednou, a to ještě tak, že jsme byli z kapacitních důvodů nuceni věc nabrat na našem obvodu a posléze ji předat. Navíc jsem pouze člen prvosledové hlídky, kdy následná komunikace s kompetentním oddělením jde kolem mě.

5. Proškolen se necítím prakticky vůbec. Ale otázkou je, jestli by tomu napomohlo školení, ve stylu, který PČR praktikuje. Zdá se mi totiž, že školení nějaké odbornosti spočívá v tom, že cca dvě hodiny je výklad teorie, zásadně doslovným čtením nepřehledné prezentace a na konci se vypracuje test, který vždy všichni splní. Vedení si tak může odškrtnout splnění těchto školení u svých podřízených a od té doby se na běžné policisty pohlíží jako na odborníky napříč všemi obory. Samozřejmě bych uvítal školení, avšak novém pojetí. Efektivnější by dle mého názoru bylo, kdyby se na specifické kurzy hlásili jen ti policisté, kteří se opravdu chtějí zdokonalovat v dané problematice. Plošné školení není efektivní v žádném směru, kromě kvantity proškolených.

### **Přepis odpovědi respondenta R2 (specialista na kyberkriminalitu OOP)**

1. Já osobně jsem se během šesti let s podezřením na nelegální obsah nesetkal. Každopádně si myslím, že nejvíce pravděpodobné je oznámení od občanů, které posléze prověříme.
2. Já osobně bych se zařízením výrazně nemanipuloval a kontaktoval bych operačního důstojníka, aby mi předal kontakt na specialistu pro tuto problematiku a následně bych postupoval podle jeho pokynů. Během doby čekání na spojení, bych na zařízení, v rukavicích, provedl alespoň nějakou aktivitu. U PC např. pohyb myši, u telefonu přejetí v rohu obrazovky, aby se zařízení neuzamklo.
3. Nejsem si vědom, že bychom na útvaru měly speciální pomůcky pro zajištění elektroniky. Každopádně bych si na zajištění přivolal krim. technika, který by tuto výbavu mohl mít k dispozici a také by na tomto zařízení mohl zajistit další stopy.
4. Věc bych po předchozí konzultaci předal pravděpodobně oddělení analytiky, kteří by např. mobilní telefon detailně prohledali a zajistili z něj upotřebitelná data.
5. Já osobně jsem žádné školení k této problematice neabsolvoval a jednal bych intuitivně na základě dosud získaných zkušeností při výkonu služby. Praktické kurzy bych rozhodně uvítal.

### **Přepis odpovědi respondenta R3 (zpracovatel obecné kriminality OOP)**

1. Ještě jsem se ve službě s touto problematikou nesešel. Zároveň jsem ani nebyl přítomen oznámení občana na obvodním oddělení z důvodu podezření na tento trestný čin.
2. Zajistit, aby žádná osoba s tímto zařízením dále nemanipulovala. Bezpečně zjistit majitele tohoto zařízení, případně další uživatele a poslední osobu, která s tímto zařízením manipulovala. Pořídím fotografickou dokumentaci zařízení společně s náhledem obrazovky nebo displeje toho zařízení. Následně vyzvu majitele k vydání věci dle §78 odst. 1 tr. řádu, případně věc bude odňata v případě odmítnutí vydání. Se zařízením zajistím rovněž nabíjecí příslušenství a ohledáním místa případně zajistím rovněž další podezřelé nosiče (CD, DVD, flashdisk nebo harddisk). Poté bude zařízení přiloženo ke spisovému materiálu a hlavní zpracovatel spisu následně vyžádá spolupráci s IT oddělením PČR za účelem ohledání zařízení.
3. Žádné speciální pomůcky či prostředky nemáme, tudíž využíváme běžné kriminalistické obaly.
4. Věc bude následně přiložena ke spisovému materiálu, kdy hlavní zpracovatel vyhotoví žádost o ohledání zařízení a případná další opatření k zařízení, kdy toto fakticky provede specialista SKPV. Prvotní komunikace probíhá formálně vyhotovením písemné žádosti o provedení úkonu a následně v případě nutnosti řádného splnění úkolu specialista kontaktuje zpracovatele telefonicky, přičemž výsledek úkonu ze strany specialisty SKPV je vyhotoven opět formálně písemnou formou. Osobně jsem ještě takto nepostupoval, jelikož jsem v této problematice neprováděl ani dílčí úkony.
5. Cítím se dostatečně znalý pro problematiku věcně náležící OOP na základě komunikace se specialisty SKPV a zároveň osobního přístupu ZVO v této problematice. Rozhodně bych uvítal možnost praktických kurzů za účelem zvýšení své odborné kvalifikace v dané problematice.

### **Přepis odpovědi respondenta R4 (zástupce vedoucího obvodního oddělení pro trestní řízení )**

1. Většinou jde vyloženě o náhodné oznámení, setkal jsem se s pár případy, například někdo přijde na oddělení, že našel telefon a když se do něj podíval, tak viděl dětskou pornografii, nebo oznámení bývalých partnerek, že jejich bývalý

přítel má v telefonu dětské porno. Ale všeobecně se k těmto případům na obvodě moc nedostáváme.

2. V tu chvíli postupujeme většinou jako s každou jinou stopou, nafotit, zajistit do obálky a odvést na oddělení. Následně předat specialistům z analytiky. My se do toho vlastně ani nijak montovat nemůžeme, jelikož nejsme proškoleni na zajišťování digitálních stop. S čím jsem se setkal v praxi, tak je například vypnutí možnosti vzdáleného přístupu přes Icloud tak, aby nemohlo dojít k vymazání dat na dálku.
3. Vůbec ne, používáme jen klasické obálky na stopy od techniků.
4. Pokud se taková věc zjistí někde venku, tak se přes dosahového důstojníka volá výjezdová skupina, ale bohužel se dost často stává, že i na věci, které by mělo zpracovávat SKPV výjezd nepřijede, prostě se řekne ať to obvod nabere a potom postoupí. Což není úplně ideální, protože policisté, co slouží pár let potom zpracovávají takto složitou kriminalitu, na kterou vlastně nejsou ani proškoleni a když udělají nějakou chybu, tak se za ně nikdo nepostaví.
5. Probíhají pouze základní školení na kyberkriminalitu, ale školení na zajišťování digitálních dat atd. moc neprobíhá, vlastně si ani nejsem jistý, jestli se ho někdo z obvodu kdy zúčastnil, spíš se to školí jen analytici.

### **Přepis odpovědi respondenta R5 (vyšetřovatel odboru obecné kriminality)**

1. Zásadní je pro mě samozřejmě vlastnictví samotného zařízení a znalost přístupových hesel. Velmi důležitá je ale i dokumentace četnosti těchto přístupů. K tomu v praxi využíváme forenzní softwary, konkrétně pracujeme s programy Cellebriation Reader a Magnet Axiom, které nám umožní aktivitu uživatele přesně zmapovat.
2. V mé vyšetřovací praxi se s případy, kdy by pachatel nevlastnil žádná fyzická data, ale disponoval by pouze rozsáhlou databází odkazů na cloudy, zatím neseťkávám.
3. Tato data se dají získat cestou mezinárodní pomoci. Máme sice možnost prostřednictvím NCTEKK požádat o tzv. datafreezing u zahraničního subjektu, což by mělo data okamžitě zajistit, ale musím konstatovat, že v reálné praxi se tento institut z důvodu přílišné zdlouhavosti prakticky nevyužívá.
4. Z pohledu vyšetřovatele vidím největší problém v obrovském množství zajištěných dat. Pokud mám prokázat, že uživatel streamovací platformy věděl,

co konzumuje, a nešlo jen o klamavý odkaz, musím se prokousat kvantem materiálů a fyzicky je vyhodnotit, což je nesmírně časově náročné.

5. Co se týče součinnosti, tuzemští poskytovatelé připojení s námi při identifikaci koncových uživatelů spolupracují bez jakýchkoliv problémů. U zahraničních subjektů je to ale mnohem složitější. Tam musíme jít cestou mezinárodní pomoci nebo využívat Evropský vyšetřovací příkaz, a i tak jsme závislí na tom, zda ten konkrétní subjekt vůbec nějakou databází disponuje.
6. Pokud bych měla navrhnout nějakou změnu v zákoně, která by nám skutečně pomohla, pak bych byla pro zrušení ustanovení § 113a trestního řádu. Jsem přesvědčena, že návrat k předchozí úpravě by celé trestní řízení v naší oblasti výrazně urychlil.

### **Přepis odpovědi respondenta R6 (operativce mravnostní kriminality na krajské úrovni)**

1. Pro prokázání faktické dispozice s daty na vzdáleném serveru považuji za stěžejní znalost přístupových údajů, tedy přezdívky (nicku) a hesla, a především překonání dvoufázového ověření – například potvrzení v e-mailu nebo SMS kódu. Velmi silným důkazem jsou pro mě také prokázané platby, které pachatel zasílá provozovateli vzdáleného úložiště. Ideální situací je pak dobrovolné zpřístupnění obsahu podezřelým přímo na našem specializovaném pracovišti (OAKK) za přítomnosti jeho obhájce.
2. V praxi se s případy, kdy by pachatel nevlastnil žádná data a disponoval pouze databází odkazů, prakticky nesetkávám. Častěji zjišťujeme aktivní přístupy na Darkweb, odkud uživatelé směřují na konkrétní zájmové odkazy související s dětskou pornografií
3. Z vlastní zkušenosti si nejsem vědom žádných procesních problémů při zajišťování dat otevřených v prohlížeči a současný právní rámec pro jejich zajištění považuji za dostatečný. Stejně tak neshledávám problémy při dokazování vědomé konzumace u streamingu. Součinnost s tuzemskými i zahraničními poskytovateli služeb je v současnosti na velmi dobré úrovni a lze u nich zaznamenat velmi proaktivní přístup k našim žádostem.
4. Ačkoliv nejsem přímo vyšetřovatel, ze své operativní praxe mohu říct, že jsem se s tímto konkrétním problémem dosud nesetkal.

5. V současné době hodnotím součinnost jako velmi dobrou, a to jak u tuzemských poskytovatelů, tak u mezinárodních platforem. U obou skupin lze v poslední době pozorovat velmi proaktivní přístup k našim žádostem
6. Nad konkrétními legislativními změnami jsem zatím hlouběji neuvažoval, protože v tuto chvíli neshledávám, že by v této oblasti byla nějaká zásadní změna potřeba.

### **Přepis odpovědi respondenta R7 (operativce mravnostní kriminality na krajské úrovni)**

1. Možno pouze cestou forenzní analýzy logů uložených v zařízeních, ze kterých osoba přistupovala k obsahu, a ze kterých je možno určit i druh operací s jednotlivými soubory, uložení, kopírování, sdílení. V souvislosti s dalšími aktivitami osoby na internetu (vyhledávání, emailová komunikace a další) pak lze dovodit faktickou dispozici ke konkrétnímu uloženému obsahu.
2. Zatím pouze v jednom případě, kdy se však analýzou přístupů o ukládání, kopírování a přeposílání konkrétních souborů v prostoru sociálních sítí s konkrétním zaměřením a zájmy osoby mimo virtuální svět, ověřenými výsledky dalších osob a posudky k osobnosti podařilo úmysl prokázat.
3. Nemám zkušenosti.
4. V tomto případě je zapotřebí získat širší přehled o četnosti přístupů, způsobech vyhledávání nelegálního obsahu, případně dalšího nakládání se sledovanými soubory (stahování, přeposílání do zájmových skupin apod.).
5. Z mého pohledu je bezproblémová, provozovatelé v této oblasti spolupracují, což je dáno i zakotvením spolupráce v mezinárodních smlouvách, např. Úmluvy o právech dítěte.
6. Přesnější zakotvení pojmu „dětská pornografie“ tak, aby nebylo nutno vyžadovat zpracování znaleckého posudku na každý soubor.

### **Přepis odpovědi respondenta R8 (Okresní státní zástupce, se zkušenostmi z celorepublikového útvaru PČR)**

1. Problematika dětské pornografie se v mé praxi většinou neobjevuje samostatně, ale spíše se vynořuje jako vedlejší produkt při vyšetřování jiné trestné činnosti. Pokud jde o úskalí při zajišťování stop, rozdělil bych je do několika rovin. Prvním tématem je rozsah vytěžení dat. Zde se domnívám, že nedostatečné vytěžení nemusí být nutně zásadním problémem. Pro naplnění skutkové podstaty a zahájení stíhání totiž postačuje i jediný obrázek, takže kvantita děl není pro

základní právní kvalifikaci určující. Většina státních zástupců a soudců se v praxi ani nepouští do hloubkové analýzy nepřetříděných dat, pokud to není výslovně namítáno obhajobou (například tvrzením, že konkrétní materiál nesplňuje definici dětské pornografie). Existují však dvě podstatné výjimky, kde na úplnosti vytěžení dat záleží. První nastává v momentě, kdy policejní orgán přehlédne, že kromě dětské pornografie (§ 192, § 193 TZ) jde i o jinou závadovou pornografii (§ 191 TZ), což vede k neúplné právní kvalifikaci. Druhou výjimkou jsou případy podle § 192 odst. 4 písm. c), odst. 5 písm. a) a § 193 odst. 2 písm. b), odst. 3 písm. b) TZ, kde je nutné zkoumat otázku získaného prospěchu nebo úmyslu takový prospěch získat. Z pohledu procesních chyb vnímám jako nejrizikovější oblast odůvodnění neodkladnosti domovní prohlídky. Je naprosto klíčové, aby byla neodkladnost řádně zdůvodněna v příkazech i protokolech v souladu s § 160 odst. 4 trestního řádu a ustálenou judikaturou (zejména nálezy Ústavního soudu Pl. ÚS 47/13). Často se také setkávám s obecně špatnou protokolací úkonů, ať už se jedná o vydání věci podle § 78, nebo o odnětí věci při prohlídkách. Velmi kritickou oblastí jsou pak chyby kriminalisticko-technické a taktické. Klasickou strategií obhajoby u náhodných nálezů (například když provádíme domovní prohlídku kvůli hospodářské kriminalitě a najdeme dětské porno) je tvrzení, že data do zařízení nastrčila policie nebo že zařízení nepatří obviněnému. U domovních prohlídek či vydání věcí se často zapomíná na zajištění stop pro další kriminalistické zkoumání, jako jsou otisky prstů či DNA, což je u jiných deliktů (např. drogových) samozřejmostí. U soudu to pak bývá velký problém. Slabým místem je i samotný způsob balení a pečetění. Věci se často vkládají do obyčejných obálek bez řádného zajištění proti neoprávněné manipulaci. Správně by se měly používat bezpečnostní obaly (např. *orgatechy*), které se ihned po zajištění vyfotí a neumožňují otevření bez viditelného poškození. Je však třeba dbát na to, aby v plastovém obalu vlhké předměty nezplesnivěly, čímž by se zničila stopa DNA. Závěrem lze říci, že alfou a omegou vyšetřování je udržení integrity a autenticity dat. Policie musí být schopna nezpochybnitelně prokázat, že zajištěná data jsou přesně ta, která měl dotyčný v dispozici. K tomu slouží nejen správné balení, ale i technická opatření – například použití beden, které odcloní signál a zabrání dálkovému smazání mobilu, nebo vytváření kontrolních součtů (hashů) při vytváření bitových kopií disků.

2. Je spousta forem, a proto také spousta rozličných možností digitálních stop. Bude-li koncové zařízení mobil, zajistíme, ostatně počítač taky, ale diskové pole někde 20.000 mil pod mořem (připouštím ovšem, že to není koncové zařízení, ale naopak zařízení, k němuž si z toho koncového nějak zjednáváme přístup), tak ho in natura nezajistíte. S ohledem na shora uvedené nedokážu jednoznačně odpovědět, co stačí anebo nestačí, opět je to o tom, že musíme vždy být schopni prokázat, že toto jsou data, která měl pachatel v držení (a je jedno, zda na CD anebo na cloudu)
3. Z mého pohledu je tato otázka v podstatě vyřešena jasným zněním zákona a současnou právní úpravu považuji za zcela dostačující. Rozlišení mezi formami držení nelegálního obsahu je v trestním zákoníku jasně definováno. Zatímco klasické přechovávání dat na fyzickém nosiči spadá pod ustanovení § 192 odst. 1 trestního zákoníku, situace, kdy pachatel získává přístup k datům v úložišti nebo prostřednictvím streamingu, je přímo postihována podle § 192 odst. 2, tedy jako získání přístupu prostřednictvím informační nebo komunikační technologie. Pokud jde o vyšší odstavce tohoto paragrafu (odst. 3 a výše), ty jsou formulovány natolik široce a obecně, že forma, jakou k trestnému činu dochází, v podstatě nehraje roli. Domnívám se, že pod tato ustanovení lze podřadit prakticky jakoukoli formu online distribuce nebo nakládání s obsahem, na kterou lze v praxi pomyslet. Zákon je v tomto směru nastaven velmi flexibilně a nepředstavuje pro nás při kvalifikaci skutků překážku.
4. Zdaleka se netýká jen pornografie, ale zajišťování „digitálních“ důkazů jako celku – odstranit roztržitost právní úpravy a duplicitu a triplicitu – viz např. chceme-li logy, je to § 88a, chceme-li monitorovat probíhající komunikaci, je to nejčastěji § 88 (i když někdo zase tvrdí, že je to § 158d), chceme-li zjistit obsah vzdáleného úložiště, je to § 158d/3.... Nikdo se v tom nevyzná, spisy bobtnají tíhou a tloušťkou příkazů, přitom fakticky jde o jediné – zda zájem společnosti na odhalení TČ je tak velký, aby to odůvodnilo prolomení jinak ústavně chráněných práv na soukromí, tajemství dopravovaných zpráv apod.

**Přepis odpovědi respondenta R9 (Okresní státní zástupce zabývající se kyberkriminalitou)**

1. Mám za to, že v praxi k závažným procesním vadám při zajišťování důkazů nedochází. Od 1.1.2026 nabyla účinnosti nová právní úprava ohledávání dat na zajištěných zařízeních (§ 113a trestního řádu), která proces při zajišťování dat

zformalizovala. Problematické jsou kauzy, kdy je zajištěno velké množství dat, včetně pornografie (nejen „dětské“). V takové případě je nezbytně třeba, aby policejní orgán provedl podrobné vyhodnocení těchto dat.

2. Obecně platí, že elektronické důkazy soudy akceptují jako jakýkoliv jiný důkaz a rovněž je hodnotí v souvislosti s jinými důkazy. Je žádoucí, pokud se podaří spolehlivě určit konkrétní zařízení, ze kterého pachatel s daty nakládal. Je však třeba konstatovat, že ani zjištění (a zajištění) konkrétního koncového zařízení nemusí být v konkrétním případě dostatečným důkazem o vině konkrétní osoby. V praxi nastávají případy, kdy podezřelý tvrdí, že k jeho zařízení měly přístup další osoby, což může být obtížné vyvrátit.
3. Platná právní úprava (§ 192 odst. 1, 2 TZ) postihuje získání přístupu stejně jako přechovávání. Mám za to, že v praxi však jsou případy „pouhého“ streamingu postihovány méně přísně, neboť soudy při ukládání trestu vždy posuzují závažnost konkrétního případu.
4. Mám za to, že v současné době výrazně ztěžuje možnost rychlého a účinného zajištění elektronických dat skutečnost, že tato data jsou uchována na serverech v zahraničí. Stejně tak ke komunikaci pachatelé využívají služby zahraničních poskytovatelů. Zajišťování těchto dat je proto nutno často provádět cestou mezinárodní justiční spolupráce, což je administrativně i časově náročné. K větší efektivitě trestního řízení v těchto věcech by nepochybně přispěla možnost tyto elektronické důkazy pro trestní řízení vyžadovat přímo (což by však bylo patrně reálně legislativně proveditelné pouze v rámci EU).

### **Přepis odpovědí respondenta R10 (obhájce se zkušenostmi z policejní praxe, vyšetřování mravnostní kriminality)**

1. Že došlo ke zneužití zařízení, případně že bylo zneužito tím, že nebylo v držení obviněného a bez jeho vědomí tak došlo k takovému zneužití, případně že zprávy byly nevyžádány.
2. Policie zcela zjevně v takových případech zajistí důkazy, které však lze pouze zpochybnit a ve většině případů nelze jednoznačně uvádět, že by pochybila policie.
3. U tohoto zavinění lze prokazovat úmyslné zavinění když podezřelý a jeho záznamy jednoznačně potvrdí že se jedná o osoby nezletilé a z jejich tělesného stavu lze toto usoudit. Samozřejmě se musí prokázat i přeposílání a případně i uchovávání, je pak na OČTŘ zda toto prokáží.

4. Dle mého názoru se jedná o případné přitěžující a nebo polehčující okolnosti a rovněž se přihlíží i k trestní minulosti, je pak na uvážení soudu jaká je společenská nebezpečnost.
5. Vzhledem k tomu, že největší trestná činnost tohoto charakteru je páchána v organizovaných skupinách, které mezi sebe nepustí neproěřené osoby, je velmi těžké do takové skupiny proniknout, dále je problém v tom, že sociálně slabé rodiny za úplatu poskytnou děti a vzhledem k tomu, že jim tato možnost přináší snadný výdělek, není v jejich zájmu něco oznamovat. Následně se pak stanou i oni pachateli a to je nutí v tomto jednání pokračovat, případně nic neoznámít. Největší slabina je nemožnost proniknout do takové organizované skupiny, kterou většinou tvoří vzdělaní a majetní lidé, kteří jsou na venek spořádanými občany.

### **Přepis odpovědi respondenta R11 (obhájce s mnohaletou zkušeností)**

1. Kromě klasické 'otevřené Wi-Fi' dnes hodně pracujeme s fenoménem sdílených rodinných účtů. Pokud má rodina jeden iCloud nebo Google Drive pro pět lidí, policie velmi těžko dokazuje, kdo konkrétně nelegálně soubor nahrál nebo zobrazil. Stačí vnést důvodnou pochybnost, a ta musí jít ve prospěch klienta.
2. Pravidelně napadáme nedostatečnou dokumentaci integrity. Pokud policie nepoužije stínící pouzdro (Faradayovu klec) a zařízení zůstane online, mohlo dojít k modifikaci dat na dálku. Jakmile vyšetřovatel nemůže doložit, že se obsah disku od momentu zajištění nezměnil ani o jeden bit, je celý důkaz procesně mrtvý.
3. OČTŘ často zaměňuje 'zobrazení' za 'přechovávání'. Pokud klientovi vyskočí pornografický banner a on na něj klikne, není to úmyslné držení. Bez důkazu o aktivním vyhledávání specifických klíčových slov nebo dlouhodobém třídění souborů do složek je prokazování úmyslu pouhá spekulace žalobce.
4. Jednoznačně nekritické přejímání znaleckých posudků soudci. Soudci často nerozumí rozdílu mezi logem routeru a logem operačního systému. Považují digitální stopu za nezpochybnitelnou pravdu, přitom v digitálním světě je falzifikace identity jednodušší než ve světě fyzickém.