https://doi.org/10.5817/RPT2023-2-1

MOŽNOSTI TRESTNEJ ČINNOSTI V METAVERSE

NORBERT HALAS[1]

ABSTRAKT

Autor sa v predmetnom článku zaoberá trestnou činnosťou spojenou s čoraz viac skloňovanou technológiou metaverse. S predmetnou problematikou je možné stretnúť sa aj na pôde Europolu a Rady EÚ, pričom autor poukazuje na aktuálny vplyv, ktorý môže mať metaverse a technológie, na ktorých je založený, na trestnú činnosť. V ďalšom rozoberá, čo táto technológia znamená pre následne presadzovanie práva a aké rizika so sebou môže priniesť v podobe trestnej činnosti.

KĽÚČOVÉ SLOVÁ:

Metaverse; neoprávnené nakladanie s osobnými údajmi; legalizácia výnosu z trestnej činnosti; obťažovanie; terorizmus; extrémizmus.

ABSTRACT

The author of this article addresses criminal activities associated with the increasingly discussed metaverse technology. This issue is also a subject of discussion within Europol and Council of the European Union, and the author highlights the current impact that the metaverse and its underlying technologies may have on criminal activities. Furthermore, the author explores what this technology means for subsequent law enforcement and the potential risks it may bring in the form of criminal activities.

[1] JUDr. Norbert Halas, Ph.D., je vyšším súdnym úradníkem pri Okresným súdem Vranov nad Topľou. Kontaktní e-mail: norbert.halas13@gmail.com

KEYWORDS:

Metaverse; Unauthorized Handling of Personal Data; Money Laundering; Abusement; Terrorism; Extremism

1. ÚVOD

S vývojom technológii sa rovnako vyvíja aj internet, ktorý je každodennou súčasťou nášho života, či už pracovného, alebo súkromného, a denne na ňom trávime niekoľko hodín. V súčasnosti sa v spojení s internetom začína čoraz viac skloňovať pojem metaverse, ktorý sa dostal do popredia najmä v čase, keď Mark Zuckerberg v októbri 2021 oznámil, že spoločnosť Facebook zmení obchodný názov na Meta Platforms, Inc.[2] Predmetné vyhlásenie prinieslo koncept metaverse do pozornosti verejnosti. Tomuto počinu svedčí aj fakt, že rovnako aj ďalšie technologické spoločnosti ohlásili veľké investície namierené do tejto technológie.[3]

To, že metaverse predstavuje výzvu aj pre trestné právo potvrdzuje aj to, že danou problematikou sa zaoberalo aj Inovačné laboratórium Europolu, ktoré v júni 2022 zorganizovalo podujatie o metaverse pre orgány presadzovania práva a justičné orgány členských štátov Európskej únie, aby pomohli pochopiť vplyv, ktorý môže mať metaverse a technológie, na ktorých je založený, na trestnú činnosť a ako sa budú musieť jednotlivé orgány prispôsobiť novým bezpečnostným potrebám občanov. Počas podujatia sa odborníci z viacerých odvetví podelili o výsledky svojho výskumu ľudského správania v digitálnom prostredí, rozvíjajúcich sa ekonomických ekosystémov súvisiacich s týmito prostrediami a s metaverse. Rovnako diskutovali aj o skúsenostiach a myšlienkach týkajúcich sa výziev, aké môže metaverse predstavovať z hľadiska bezpečnosti a o spôsoboch, ako môžu jednotlivé orgány prispôsobiť svoje postupy. Na podujatí sa zúčastnilo viac ako 120 zástupcov orgánov presadzovania práva a justičných orgánov z celej Európ-

[2] Introducing Meta: A social technology company. [online]. 2021. [18. 03. 2023]. Dostupné z: https://about.fb.com/news/2021/10/facebook-company-is-now-meta/

[3] Which companies are investing in the metaverse? 7 stocks to watch. [online]. [18. 03. 2023]. Dostupné z: https://finance.yahoo.com/news/companies-investing-metaverse-7-stocks

skej únie. V sérii prezentácii účastníci vyjadrili jasnú potrebu zdrojov, ktoré by jednotlivým policajným zložkám v členských štátoch EÚ pomohli lepšie pochopiť riziká a príležitosti, ktoré predstavuje metaverse a s ním súvisiace technológie.[4]

V súčasnosti je náročné predvídať skutočné dôsledky trestnej činnosti v spojení s predmetnou technológiou, nakoľko metaverse má v súčasnej dobe aplikačnú vrstvu len veľmi limitovanú. Tieto nové výzvy si budú vyžadovať inovatívne riešenia a spoluprácu medzi technologickým odvetvím a orgánmi činnými v trestnom konaní, aby sa zabezpečilo bezpečné a dôveryhodné prostredie pre používateľov. Preto je už teraz potrebné predstaviť si možné rizika spojené s metaverse. Cieľom tohto príspevku je systematicky preskúmať a kriticky analyzovať narastajúce hrozby a možnosti trestnej činnosti v kontexte metaverse, ktorý sa stáva stále významnejším aktérom v súčasnom digitálnom ekosystéme. Tento príspevok sa ďalej sústreďuje na jednotlivé technológie, ktoré sú základom pre metaverse, ich následné zneužívanie a na dôležité aspekty bezpečnosti a etických záležitostí, ktoré vznikajú v dôsledku rastúcej komplexity a interakcie medzi fyzickým a virtuálnym svetom v rámci metaverse.

2. TECHNOLÓGIE SPOJENÉ S METAVERSE

Metaverse sa často opisuje ako ďalší medzi stupienok vývoja internetu, ktorý by mohol vytvoriť jediný univerzálny virtuálny svet, resp. kyberpriestor, ktorý ponúka používateľom pohlcujúci zážitok a ktorý má svoje základy v reálnom svete. V najnovšej definícii metaverse sa tento koncept stáva ešte ambicióznejším, keďže môže zrušiť hranice medzi fyzickým a virtuálnym svetom a vytvoriť jednu integrovanú realitu. V súčasnosti je metaverse zameraný len na virtuálnu realitu (VR - Virtual Reality), ale čoraz viac sa definuje aj z hľadiska rozšírenej reality (AR - Augmented Reality) alebo zmiešanej reality (XR - Extended Reality).[5]

---

[4] Policing in the metaverse: what law enforcement needs to know. [online]. 2022. [18. 03. 2023]. Dostupné z: https://www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know

[5] What is the metaverse and how will it work? [online]. [18. 03. 2023]. Dostupné z: https://blog.servermania.com/what-is-metaverse/

Z prezentovaných vízií metaverse ponúka prísľub umožniť ľuďom vychutnať si zážitky bez fyzických obmedzení a disponovať väčšou autonómiu vďaka decentralizovanej technológii. Navrhované aplikácie presahujú možnosť online zábavy, tak ako ju poznáme dnes, a zahŕňajú zlepšenie produktivity práce, interaktívne vzdelávacie prostredia, elektronický obchod a i. Zdá sa pravdepodobné, že metaverse bude zahŕňať digitálnu ekonomiku, vďaka ktorej budú môcť používatelia vytvárať, nakupovať a predávať tovar podobne ako je to pri mnohých online hrách, akými sú napr. World of Warcraft. V súčasnosti sa už stretávame s virtuálnymi svetmi v rôznych aplikáciách alebo na webových stránkach, akou je aj napr. platforma Roblox[6], platforma Second Life[7], Fortnite alebo aj Minecraft, kde jednotliví užívatelia medzi sebou vzájomne komunikujú a zároveň aj obchodujú.

Metaverse a súvisiace technológie sú predstavované rôznymi spôsobmi, ale zdieľajú spoločný koncept celkového alebo čiastočného virtuálneho sveta, ktorý prenáša zážitky z fyzického sveta do virtuálnej sféry. Na základe tohto konceptu bol navrhnutý tzv. „internet zmyslov“ [8] a zároveň prebieha vývoj implantovaných čipov, ktoré umožňujú úplné ponorenie sa do virtuálneho sveta. [9] S týmito rozhraniami môže v budúcnosti vzniknúť situácia, kedy bude ťažké alebo dokonca nemožné rozlíšiť virtuálny svet od toho fyzického.

V súčasnosti je ťažké predpovedať, či sa koncept metaverse uchytí ako spoločná technológia viacerých spoločnosti, alebo si každá spoločnosť vytvorí svoju vlastnú verziu. Ako však poznamenáva dokument analytického

---

[6] Roblox je online hracia platforma, umožňujúca hráčom vytvárať vlastné hry s otvoreným svetom a zdieľať ich s ostatnými. Hra je dostupná pre Android, iOS, MacOS, Windows, Xbox One a Fire OS.

[7] Second Life je online multimediálna platforma, ktorá umožňuje ľuďom vytvoriť si avatara a následne komunikovať s ostatnými používateľmi a používateľmi vytvoreným obsahom v rámci online virtuálneho sveta pre viacerých hráčov.

[8] Internet of senses (internet zmyslov) poskytuje rozšírené videnie, sluch, hmat a čuch. Umožňuje užívateľom spájať multisenzorické digitálne zážitky s miestnym prostredím a komunikovať so vzdialenými používateľmi, zariadeniami a pod., ako keby boli priamo pri nich.

[9] Elon Musk má veľké plány: Čochvíľa začne testovať Neuralink aj na ľuďoch! [online]. 2022. [cit. 19. 03. 2023]. Dostupné z: https://www.techbyte.sk/2022/12/elon-musk-zacne-testovat-neuralink-ludoch/

a výskumného tímu Rady Európskej únie týkajúci sa metaverse *„dopyt po technológii vytvorí jej následnú ponuku“*[10]*,* čo vlastne platí pri všetkých najnovších technológiách. Navyše, so spojeným trhom pre VR a AR v odhadovanej hodnote 4 miliardy eur, pričom do budúcna sa odhaduje, že táto čiastka vzrastie na 36 miliárd eur,[11] mnohé spoločnosti neváhajú investovať do tejto vznikajúcej technológie za účelom zisku a tým priniesť metaverse do každodenného života. Aj keď predmetné investície nie sú zárukou jeho prijatia, značné investície od širokého spektra technologických spoločností zvyšujú pravdepodobnosť prijatia aspoň niektorých aspektov s ním spojených. Metaverse je nadviazaný na ďalšie samostatné technológie, ktoré tvoria jeho súčasť a ktoré je potrebné si na účely tohto príspevku aj patrične ozrejmiť.

2.1 WEB3

Web3 sa momentálne nachádza v raných štádiách vývoja a jeho presná definícia ešte nie je ustálená. Avšak prístupné definície sa zhodujú v jednom - že ide o novú verziu internetu, ktorá stojí na princípoch decentralizácie, súkromia a anonymity.[12] V rámci Web3 je decentralizácia dosahovaná využitím technológii akou je peer-to-peer (p2p)[13] a blockchain, ktorá je jeho kľúčovým hnacím motorom. Decentralizácia, anonymita a absencia centrálnej autority môžu mať významné dôsledky pre kriminalitu v kyberpriestore, a to aj pre evidenciu elektronických dôkazov o týchto činnostiach. S decentralizáciou sa môže zvýšiť obťažnosť vyšetrovania a trestania trestnej činnosti v kyberpriestore, keďže neexistuje centrálny orgán, ktorý by mal kontrolu nad týmito sieťami.[14]

---

[10] Rada Európskej únie: Metaverse – virtual world, real challenges. [online]. 2022. [cit. 19. 03. 2023]. Dostupné z: https://www.consilium.europa.eu/media/54987/metaverse-paper-9-march-2022.pdf

[11] Ibidem.

[12] FENWICK, Mark, JURCYS, Paulius: The contested meaning of Web3 and why it matters for (IP) Lawyers. In: *Product and services*. [online]. 2022. [cit. 19. 03. 2023]. Dostupné z:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4017790

[13] Sieť so vzájomným sprístupňovaním obsahu medzi užívateľmi.

V súčasnosti existuje niekoľko projektov, ktoré kombinujú technológie blockchainu a peer-to-peer (p2p) na poskytovanie rôznych služieb, ako napr. herný obsah, nezastupiteľné tokeny (NFT)[15] a riešenia na zdieľanie médií. Tieto technológie predstavujú existujúcu infraštruktúru, ktorá môže byť využitá pre rozvoj metaverse a môže byť ďalej prispôsobená a rozvíjaná, aby vyhovovala jeho špecifickým potrebám. Hoci koncept Web3 má potenciál poskytnúť decentralizovaný internet, veľké korporácie začínajú preberať tieto technológie a integrovať ich do svojich platformových riešení. To vedie k vytváraniu centralizovaných služieb a platformových ekosystémov, ktoré môžu konkurovať decentralizovaným projektom. Tento trend vyvoláva diskusiu o rovnováhe medzi decentralizáciou a centralizáciou v rámci metaverse a otázku, ako udržať decentralizované hodnoty v kontexte rastúcej účasti veľkých technologických hráčov.[16]

2.2 AVATAR POUŽÍVATEĽA

Avatar (známy aj ako digitálne dvojča) reprezentuje digitálnu replikáciu objektov a systémov z reálneho do virtuálneho sveta. V súčasnosti je definovaný ako virtuálna entita, ktorá má charakteristiky svojho tvorcu - používateľa. Tento koncept umožňuje zrkadlenie fyzických entít a zároveň predpovedanie a optimalizáciu ich virtuálnych inkarnácií prostredníctvom analýzy senzorických dát, fyzikálnych modelov a historických informácií v reálnom čase.[17]

Avatary slúžia ako nástroje pre získavanie údajov od fyzických entít na následné samoučenie a prispôsobenie v rámci virtuálneho prostredia. Okrem toho majú avatary schopnosť poskytovať presné digitálne modely predpokladaných objektov s požadovanými atribútmi v metaverse. Táto

[14] FENWICK, Mark, JURCYS, Paulius: The contested meaning of Web3 and why it matters for (IP) Lawyers. In: *Product and services*. [online]. 2022. [cit. 19. 03. 2023]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4017790

[15] Non-fungible token

[16] Porovnaj MA Winston, HUANG Ken. *Blockchain and Web3: Building the Cryptocurrency, Privacy, and Security Foundations of the Metaverse.* 1st Edition, Wiley, 2022, s. 56.

[17] BANAEIAN FAR Saeed, RAD IMANI Azadeh. Applying Digital Twins in Metaverse: User Interface, Security and Privacy Challenges. [online]. 2022. [cit. 08. 08. 2023]. Dostupné z: https://arxiv.org/pdf/2204.11343.pdf

presnosť je dosiahnutá simuláciou komplexných fyzikálnych procesov a využitím technológií umelej inteligencie, čo je významné pre rozvoj a renderovanie metaverse na veľkej škále. Ďalej, avatary podporujú prediktívnu údržbu a monitorovanie bezpečnosti fyzického sveta prostredníctvom obojsmerného pripojenia medzi fyzickými entitami a ich virtuálnymi reprezentáciami.[18]

2.3 VIRTUÁLNA, ROZŠÍRENÁ A ZMIEŠANÁ REALITA

Zatiaľ čo niektoré technológie virtuálnej a rozšírenej reality existujú už nejaký čas, ďalšie sa stále intenzívne vyvíjajú a sú podporované mnohými rôznymi technológiami, akými sú priestorové výpočty, senzory, haptika a lokalizačné služby. rozšírený hardvér a softvér na prístup k platforme, ako aj sprievodná technológia na uľahčenie používania platforiem.

Rozšírená realita (AR) je technologický koncept, ktorý umožňuje používateľom interagovať s digitálnym obsahom a virtuálnymi objektmi v reálnom svete prostredníctvom grafiky, videonahrávok a hologramov. Na druhej strane, virtuálna realita (VR) poskytuje používateľom pohlcujúce zážitky v plne digitálnom prostredí, kde sú odtrhnutí od fyzického sveta. MR[19] predstavuje koncept, ktorý umožňuje prechod medzi AR a VR, čím ponúka komplexnejšie a dynamické interakcie medzi digitálnym a reálnym svetom. Tieto technológie spadajú pod rámec rozšírenej reality (XR), čo je zastrešujúci termín, zahŕňajúci VR, AR a MR. XR umožňuje používateľom prežiť rozmanité zážitky v spojení s metaverse, čím im otvára dvere k rôznorodým službám a aktivitám, ktoré sa odohrávajú v rámci fyzického aj digitálneho sveta.[20]

---

[18] Ibidem.

[19] MR - mixed reality, vo voľnom preklade „zmiešaná realita“. Na účely tohto príspevku sa ale „zmiešanou realitou“ rozumie pojem Extended reality (XR).

[20] RASHID, Mamunur, CHOI, Piljoo, KWON, Ki-Ryong. Emergence of the Metaverse: How Blockchain, AI, AR/VR, and Digital Transformation Technologies will change the Future World. [online]. 2022. [cit. 09.08.2023]. Dostupné z: https://www.researchgate.net/publication/
362302545_Emergence_of_the_Metaverse_How_Blockchain_AI_ARVR_and_Digital_Transformation_Technologies_will_change_the_Future_World

S vyspelosťou miniaturizovaných senzorov, vstavanej technológie a technológie zmiešanej reality (XR) sa očakáva, že XR zariadenia, ako sú helmy s montovanými displejmi (HMD[21]), budú hlavným terminálom pre vstup do metaverse. XR začleňuje technológie virtuálnej a rozšírenej reality (VR/AR), aby ponúklo multisenzorické ponorenie, zvýšený zážitok a interakciu v reálnom čase medzi používateľom/avatarom/prostredím prostredníctvom holografického displeja s predným projektorom, HCI[22] (najmä BCI[23]) a rozsiahleho 3D modelovania. Nosiace XR zariadenia vykonávajú vnímanie informácií o ľudských špecifikáciách s vysokým rozlíšením, ako aj všeobecné vnímanie objektov a prostredia s pomocou vnútorných inteligentných zariadení (napr. kamier).[24]

Týmto spôsobom interaktivita medzi používateľom a avatarom už nebude obmedzená na mobilné vstupy (napr. na držanie smartfónov a notebookov), ale na všetky druhy interaktívnych zariadení pripojených k metaverse.

2.4 TECHNOLÓGIA UMELEJ INTELIGENCIE

Technológia umelej inteligencie (AI) slúži ako centrálny systém alebo „mozog“ metaverse, ktorý zabezpečuje personalizované služby pre používateľov v tomto virtuálnom svete. Tieto služby zahŕňajú vytváranie živých a prispôsobených avatarov, renderovanie rozsiahlych scén metaverse a poskytovanie multijazykovej podpory prostredníctvom analýzy multimodálnych vstupov a spracovania dát.

AI v metaverse má schopnosť inteligentných interakcií s používateľmi, ako napr. poskytovanie inteligentných sprievodcov pri nakupovaní alebo predpovedanie pohybu používateľa. Tieto interakcie prebiehajú medzi používateľmi a avatarom alebo NPC[25] prostredníctvom inteligentného roz-

[21] Helmet-mounted display

[22] Human–computer interaction (Interakcia človeka s počítačom)

[23] Brain–computer interface (neuralink)

[24] WANG Yuntao, SU Zhou, ZHANG Ning et. A Survey on Metaverse: Fundamentals, Security, and Privacy. [online]. 2022. [cit. 09. 08. 2023]. Dostupné z: https://arxiv.org/pdf/2203.02662.pdf

[25] Non-player character

hodovania. Jedným z príkladov je kontinuálne učenie sa výrazov tváre, emócií, účesov a iných faktorov zo strany AI algoritmov. Tieto algoritmy následne vytvárajú živé a personalizované avatary, ktoré reagujú na používateľov a sú schopné inteligentne odporúčať produkty alebo informácie, ktoré by mohli byť pre používateľov v rámci metaverse zaujímavé.[26]

2.5 NETWORKING

V poslednom desaťročí bolo predstavených niekoľko inovatívnych technológií na zlepšenie celkového výkonu bezdrôtových komunikačných a sieťových systémov, v ktorých sa AI intenzívne využíva na viacerých vrstvách sieťovej architektúry. Multimediálne služby a aplikácie v reálnom čase zvyčajne vyžadujú spoľahlivé pripojenie s vysokou priepustnosťou a nízkou latenciou, aby bola zaručená aspoň základná používateľská skúsenosť. Podľa požiadaviek sietí piatej generácie (5G) by maximálna rýchlosť prenosu údajov mala byť okolo 10 Gbps (gigabitov za sekundu) a oneskorenie medzi koncovými bodmi nemôže presiahnuť 10 ms (milisekundy). V súčasnosti sú už v testovacej fáze aj 6G siete.[27]

V metaverse je prítomný všeobecný sieťový prístup, ktorý umožňuje prenos veľkého objemu dát v reálnom čase medzi virtuálnym a reálnym svetom, ako aj medzi rôznymi sub-metaversmi. Tento sieťový prístup je podporovaný širokým spektrom sieťových technológií vrátane Internetu vecí (IoT), softvérovo definovanej siete (SDN), B5G a potenciálne aj 6G. V rámci 6G sa rozvíja potenciálna paradigma integrovanej siete Space-Air-Ground (SAGIN), ktorá má za cieľ zabezpečiť všeobecný a plynulý sieťový prístup k aplikáciám metaverse. Okrem toho technológia SDN umožňuje škálovateľné a flexibilné riadenie rozsiahlych sietí metaverse tým, že oddelí dátovú rovinu od riadiacej roviny. Logicky centralizovaný kontrolér využíva štandardizované rozhranie na správu zdrojov a fyzických zariadení

[26] Pozri viac napr. HUYNH-THE Thien, PHAM Quoc-Viet, PHAM Xuan-Qui et. Artificial Intelligence for the Metaverse: A Survey. [online]. 2022. [cit. 11. 08. 2023]. Dostupné z: https://arxiv.org/pdf/2202.10336.pdf

[27] HUYNH-THE Thien, PHAM Quoc-Viet, PHAM Xuan-Qui et. Artificial Intelligence for the Metaverse: A Survey. [online]. 2022. [cit. 11. 08. 2023]. Dostupné z: https://arxiv.org/pdf/2202.10336.pdf

v metaverse a umožňuje dynamické prerozdeľovanie virtualizovanej šírky pásma, úložného priestoru a výpočtových zdrojov v reálnom čase na základe požiadaviek rôznych sub-metaversov. Senzory internetu vecí (IoT) v metaverse slúžia ako rozšírenie ľudských zmyslov, čím pridávajú ďalšie dimenzie interakcie medzi virtuálnym a reálnym svetom. Tieto senzory zlepšujú vnímanie a monitorovanie prostredia v metaverse a umožňujú efektívnejšiu interakciu a komunikáciu medzi používateľmi a prostredím metaverse.[28]

V metaverse založenom na SDN sú fyzické zariadenia a zdroje riadené logicky centralizovaným radičom pomocou štandardizovaného rozhrania, ako je OpenFlow, čím je možné dynamicky prideľovať virtualizované výpočty, úložisko a zdroje šírky pásma podľa požiadaviek rôznych čiastkových metaverse v reálnom čase. Okrem toho je internet vecí sieť mnohých fyzických objektov, do ktorých sú zabudované senzory, softvér, komunikačné komponenty a ďalšie technológie s cieľom spájať, vymieňať si a spracovávať údaje medzi vecami, systémami, cloudmi a používateľmi cez internet. V metaverse sú senzory internetu vecí rozšírením ľudských zmyslov.[29]

2.6 BLOCKCHAIN

V kontexte metaverse sa použitie blockchain technológie navrhuje ako prostriedok, ktorý umožňuje používateľom prenášať svoje avatary a aktíva z jedného virtuálneho sveta do druhého. Blockchain je tiež úzko spojený s konceptom virtuálnych mien, pričom sa predpokladá, že tieto budú zohrávať dôležitú úlohu v ekonomickej činnosti v rámci metaverse. Technológia blockchain ponúka decentralizovaný a bezpečný spôsob zaznamenávania a overovania vlastníctva digitálnych aktív a virtuálnych mien v metaverse. To umožňuje používateľom prenášať svoje digitálne hodnoty

[28] ALI Mansoor, NACEM Faisal, KADDOUM, Georges, HOSSAIN, Ekram. Metaverse Communications, Networking, Security, and Applications: Research Issues, State-of-the-Art, and Future Directions. [online]. 2022. [cit. 18. 08. 2023]. Dostupné z: https://arxiv.org/pdf/2212.13993.pdf

[29] WANG Yuntao, SU Zhou, ZHANG Ning et. A Survey on Metaverse: Fundamentals, Security, and Privacy, [online]. 2022. [cit. 18. 08. 2023]. Dostupné z: https://arxiv.org/pdf/2203.02662.pdf

medzi rôznymi metaversmi bez potreby závislosti na centrálnej autorite alebo entite. Týmto spôsobom môžu používatelia ľahko spravovať svoje aktíva a virtuálne meny v rámci rozmanitých virtuálnych svetov. Virtuálne meny, ktoré sú často považované za kryptomeny vytvorené na blockchaine, môžu byť v metaverse využité na nákup digitálnych aktív, služieb alebo produktov. Predpokladá sa, že tieto virtuálne meny budú mať v metaverse významný vplyv na hospodársku aktivitu, pretože umožnia používateľom vykonávať rôzne transakcie a obchody v digitálnom prostredí. Celkovo vzato, blockchain technológia prispieva k decentralizácii a bezpečnosti vlastníctva digitálnych aktív a virtuálnych mien v metaverse a zohráva dôležitú úlohu v budúcej ekonomike tohto virtuálneho sveta.[30]

Blockchainy sú distribuované digitálne účtovné knihy kryptograficky podpísaných transakcií, ktoré sú zoskupené do blokov. Každý blok je po overení a podstúpení konsenzuálneho rozhodnutia kryptograficky prepojený s predchádzajúcim, čím sa vytvorí reťaz (chain). Tento reťazec znamená, že žiadny jednotlivý záznam nemožno zmeniť bez toho, aby sa zmenili aj všetky nasledujúce záznamy. Implementácia blockchainu ako verejnej distribuovanej účtovnej knihy znamená, že všetky záznamy sú verejné a každá zmena je overená niekoľkými uzlami v sieti, čím sa vytvárajú dodatočné záruky integrity údajov na blockchaine.[31]

Použitie blockchainu v tejto technológii je navrhnuté ako spôsob na uľahčenie interoperability rôznych platforiem metaverse. V tomto prípade by záznamy obsahovali všetky relevantné informácie o používateľskom avatare, ako sú jeho atribúty a vlastníctvo. Nahliadnutím do blockchainu by všetky platformy našli zhodné informácie o používateľovi. Používatelia sa tak môžu na všetkých týchto platformách javiť rovnako (t. j. oblečenie a aktíva,

[30] HUYNH, Thien, REDDY GADEKALLU, Thippa, WANG Weizheng et al. Blockchain for the metaverse: A Review. [online]. 2022. [cit. 18. 08. 2023]. Dostupné z: https://www.sciencedirect.com/science/article/pii/S0167739X23000493

[31] KUMAR, Randhir, TRIPATHI, Rakesh. Implementation of distributed file storage and access framework using IPFS and blockchain, *Fifth international conference on image information processing*, 2019. s. 250.

ale aj metadáta o nich) a teda môžu mať jednu identitu na všetkých platformách.[32]

3. HMOTNOPRÁVNE ASPEKTY TRESTNEJ ČINNOSTI SPOJENEJ S METAVERSE

Ako sme si načrtli v úvode, rýchly technologický vývoj v posledných desaťročiach viedol k mnohým pozitívnym zmenám v našich životoch. Avšak tento vývoj priniesol aj nové výzvy, najmä v oblasti trestného práva. S nástupom nových technológií vznikajú nielen nové príležitosti pre trestnú činnosť, ale aj komplexné výzvy v oblasti vyšetrovania a následného trestania. Jedným z kľúčových aspektov, ktorý by mal byť zdôraznený, je rýchly vývoj internetu a mobilných, resp. počítačových zariadení. Podľa viacerých autorov je nárast počítačovej kriminality zapríčinený tým, že tieto technológie a cezhraničná povaha internetu umožňujú páchateľom páchať trestné činy rýchlo, efektívne a anonymne.[33] Orgány činné v trestnom konaní sa častokrát musia vyrovnávať s rozdielnymi právnymi systémami a jurisdikciami, čo komplikuje vyšetrovanie a trestanie trestných činov na globálnej úrovni.[34]

Rovnako ako s nástupom éry internetu aj s nástupom metaverse je pravdepodobné, že dôjde k zneužitiu tejto technológie na účely trestnej činnosti, či už z dôvodu možnej decentralizácie, anonymity alebo aj cezhraničnej povahy tejto technológie.

---

[32] Policing in the metaverse: what law enforcement needs to know. [online]. 2022. [cit. 19.08.2023]. Dostupné z: https://www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know

[33] Napr. CURTIS, Joanna, OXBURGH, Gavin. Understanding cybercrime in 'real world' policing and law enforcement. [online]. 2022. [cit. 07. 11. 2023]. Dostupné z: https://journals.sagepub.com/doi/10.1177/0032258X221107584

[34] Viac pozri napr. Rozhodnutie Rady, ktorým sa členské štáty poverujú podpísať v záujme Európskej únie Druhý dodatkový protokol k Dohovoru o počítačovej kriminalite o posilnenej spolupráci a sprístupňovaní elektronických dôkazov. [online]. 2022. [cit. 27. 03. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:52021PC0718

3.1 NEOPRÁVNENÉ NAKLADANIE S OSOBNÝMI ÚDAJMI A KRÁDEŽE IDENTITY

V dnešnej dobe sa na internete zhromažďuje obrovské množstvo údajov o jednotlivcoch, ktoré sa využívajú na sledovanie ich správania a preferencií. Táto digitálna stopa môže byť zneužitá na manipuláciu s ľuďmi a dokonca na ich identifikáciu. Avšak, ako sme už uviedli v predchádzajúcej časti, metaverse prináša nové technológie, ktoré umožnia ešte hlbšie a pohlcujúcejšie interakcie medzi používateľmi. Týmto spôsobom sa budú zhromažďovať ešte väčšie objemy údajov, ktoré umožnia presnejšie predikcie správania jednotlivcov a dokonca aj ich jedinečnú identifikáciu na základe týchto interakcií. To môže mať obrovský vplyv na súkromie a bezpečnosť ľudí, pretože tieto údaje môžu byť následne zneužité na neetické a nezákonné účely.

Rastúci vývoj technológií v metaverse prináša nové a závažné výzvy v oblasti ochrany osobných údajov a digitálnych identít. S nárastom možností reálneho a trvalého virtuálneho zobrazovania používateľov v metaverse sa otvárajú nové príležitosti na vytváranie presvedčivých kópií vzhľadu používateľov, známych ako deepfakes. Toto zvyšuje riziko zneužitia digitálnej identity, keďže manipulácia a falzifikácia môžu byť na úrovni metaverse ešte sofistikovanejšie a presvedčivejšie. S rozvojom pokročilých senzorov pre sledovanie očí, tváre a haptiky sa získavajú podrobnejšie biometrické informácie o jednotlivých používateľoch, ktoré môžu byť využité na účely manipulácie a zneužitia digitálnych identít, čo predstavuje ďalšie riziko. Metaverse poskytuje nové a efektívnejšie spôsoby interakcie medzi používateľmi a systémom, čo môže zvýšiť úroveň komplexity a sofistikovanosti manipulácie s digitálnymi identitami. Preto je nevyhnutné zvýšiť úroveň ochrany a bezpečnosti digitálnych identít v rámci metaverse. Toto opatrenie je kľúčové na minimalizovanie rizika zneužitia a manipulácie, ktoré môžu viesť k situáciám, kde používatelia budú komunikovať s falošnými identitami, čo má potenciál značne narúšať dôveru a bezpečnosť v tomto virtuálnom prostredí. Môže tak kľudne dôjsť k situácii, keď si jeden

používateľ bude myslieť, že komunikuje s iným známym, avšak reálne pôjde o cudziu osobu.

V oblasti metaverse vznikajú nové výzvy súvisiace s dôverou v digitálnu identitu. S rastúcou kvalitou virtuálnej reprezentácie používateľov, ako aj s pokročilými senzormi, ktoré monitorujú interakciu používateľov s virtuálnym priestorom, sa zhromažďuje značné množstvo biometrických informácií, ktoré môžu byť zneužité na neoprávnený prístup k citlivým informáciám alebo na manipuláciu s používateľmi. Takisto existuje potenciál na využitie umelej inteligencie na spracovanie informácií o používateľoch, ktoré sa zhromažďujú v rámci metaverse a na následnú manipuláciu s nimi. Je zrejmé, že v oblasti metaverse by mali platiť rovnaké otázky o ochrane osobných údajov a bezpečnosti ako v iných oblastiach digitálneho sveta.

Rovnako dôležité je určenie toho, kto vlastní virtuálnu identitu používateľa. Tento problém vlastníctva virtuálnej identity je kľúčový pre používateľov metaverse a vyvoláva rôzne otázky týkajúce sa práv na ochranu osobných údajov a duševného vlastníctva. Ak platforma nárokuje vlastníctvo nad virtuálnymi identitami používateľov a s nimi súvisiacimi osobnými údajmi, môže to mať zásadné následky pre používateľov v oblasti dôveryhodnosti a súkromia. Navyše, ak používateľ poskytne biometrické informácie na prihlásenie sa do platformy, tieto informácie môžu byť použité na ďalšie účely bez súhlasu používateľa, ak to platforma explicitne nezakáže.

Údaje generované používateľmi v metaverse môžu poskytnúť veľmi podrobný obraz o ich identite a správaní, ktoré môže byť viac definujúce ako vzhľad používateľského avatara. Tieto údaje môžu byť zhromažďované, spracovávané a využívané rôznymi spôsobmi, čo môže mať dôležité následky pre súkromie a bezpečnosť používateľov. Existujú riziká, že tieto údaje môžu byť predané alebo duplikované bez súhlasu používateľov, čo môže spôsobiť potenciálne vážne dôsledky pre ich identitu a súkromie. Je dôležité, aby jednotlivé korporácie chránili tieto údaje a zabezpečili, aby boli používané v súlade s právnymi predpismi a etickými zásadami. Takisto je dôležité, aby používatelia boli informovaní o tom, ktoré ich údaje sú zhromažďované a ako sú následne používané, aby mohli urobiť rozhodnutia o tom, ako sa v metaverse prezentovať a aké údaje poskytovať. Rovnako

ako na internete, aj v metaverse by mali používatelia byť obozretní a chrániť svoje súkromie a bezpečnosť. Uvidí sa, do akej miery bude následná implementácia týchto platforiem v súlade s GDPR v rámci EÚ.

V súčasnosti sa stretávame s predajom digitálnych biometrických údajov na dark webe, čo umožňuje páchateľovi použiť takýto údaj obete na účely obídenia autentifikačných systémov.[35] S veľmi podrobnými informáciami, ktoré by sa mohli získať od používateľov metaverse, by bolo ťažšie bojovať proti takýmto exploitom. Tie by sa dali dokonca použiť na generovanie syntetických identít s celou hĺbkou človeka pridaním behaviorálnej vrstvy k deepfakes čo by vytvorilo dokonalé príležitosti na zneužitie cudzej identity, pričom by z hľadiska trestného práva mohlo ísť o trestný čin podvodu podľa § 221 slovenského zákona č. 300/2005 Z.z. Trestný zákon (ďalej len „Trestný zákon“)[36] alebo podľa § 209 českého zákona č. 40/2009 Sb. Trestní zákoník (ďalej len „Trestní zákoník“)[37] vzhľadom na uvedenie iného do omylu za účelom obohatenia sa. Už teraz sú známe medializované prípady podvodu, keď sa páchateľ vydával za niekoho iného za účelom vylákania finančných prostriedkov od obete.[38] Popísané konania môžu napĺňať aj ďalšiu skutkovú podstatu trestného činu a to poškodzovania cudzích práv podľa § 181 Trestního zákoníka,[39] ktorého objektom sú nemajetkové práva

[35] Genesis marketplace, a digital fingerprint darknet store insights: Into genesis marketplace, a black market trading in digital identity. [online]. [cit. 29. 03. 2023]. Dostupné z: https://www.f5.com/labs/articles/threat-intelligence/genesis-marketplace--a-digital-fingerprint-darknet-store

[36] Podľa § 221 ods. 1 Trestného zákona kto na škodu cudzieho majetku seba alebo iného obohatí tým, že uvedie niekoho do omylu alebo využije niečí omyl, a spôsobí tak na cudzom majetku malú škodu, potrestá sa odňatím slobody až na dva roky.

[37] Podľa § 209 ods. 1 Trestního zákoníka kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.

[38] Predstavil sa ako jej vnuk: Seniorku v Bratislave obrali o 14.000 eur. [online]. [cit. 31.03.2023]. Dostupné z: https://www.teraz.sk/regiony/predstavil-sa-ako-jej-vnuk-seniorku-v-b/704934-clanok.html

[39] Podľa § 181 ods. 1 Trestního zákoníka kdo jinému způsobí vážnou újmu na právech tím, že a) uvede někoho v omyl, nebo b) využije něčího omylu, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.

fyzickej a právnickej osoby,[40] najmä tie, ktoré vyplývajú z čl. 7 ods. 1 a čl. 10 Listiny základných práv a slobôd.[41]

Okrem toho, ak by podrobné osobné údaje boli presvedčivo použité na napodobňovanie osoby, pre orgány činné v trestnom konaní by bolo náročné identifikovať reálneho používateľa služby a prípadného páchateľa trestného činu. V tejto súvislosti je veľmi dôležitý postup identifikácie známy ako „poznaj svojho klienta“ (KYC - Know Your Customer), ktorý je už v súčasnosti využívaný najmä finančnými inštitúciami. Tento postup je rovnako dôležitý aj pre technológiu metaverse, pretože pomáha predchádzať zneužitiu osobných údajov a podporuje vyšetrovanie trestných činov spáchaných v tejto forme.

3.2 LEGALIZÁCIA VÝNOSU Z TRESTNEJ ČINNOSTI A PODVODY

Finančné prostriedky a ich hodnota môžu mať v metaverse rôzne formy. Zatiaľ čo NFT môžu umožňovať preukázanie vlastníctva digitálneho tovaru, transakcie v metaverse môžu byť uľahčené množstvom rôznych virtuálnych mien (kryptomien) v závislosti od príslušných platforiem, pričom fiat meny[42] pravdepodobne zostanú ako prostriedok vstupu z bežnej ekonomiky do ekonomiky metaverse. Legalizácia príjmov z trestnej činností, môže byť v metaverse pomerne jednoduchá vzhľadom na virtuálne meny a už viackrát spomínanú decentralizáciu systému.

Z ekonomického hľadiska bude v metaverse nevyhnutné, aby používatelia mohli vykonávať platby jednoducho a rýchlo. To znamená, že okrem tradičných fiat mien a známych kryptomien, ktoré poznáme, pravdepodobne uvidíme aj ďalšie implementácie platforiem špecifických pre virtuálne meny a iné decentralizované kryptomeny, ktoré budú vyžadovať nové právne riešenia. Tento nový digitálny priestor pravdepodobne zvýši nároky

[40] ŠÁMAL, Pavel, GŘIVNA, Tomáš, BOHUSLAV, Lukáš a kol. *Trestní právo hmotné.* 9. vydanie. Wolters Kluwer ČR, 2021, s. 698.

[41] Nedotknuteľnosť osoby a súkromia, právo na zachovanie svojej ľudskej dôstojnosti, osobnej cti, dobrej povesti a na ochranu mena, právo na ochranu pred neoprávneným zasahovaním do súkromného a rodinného života, právo na ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe.

[42] Fiat mena predstavuje bežné peňažné prostriedky, akými sú euro, americký dolár a pod.

na monitorovanie a reguláciu. To znamená, že budú potrebné nové právne a regulačné mechanizmy, ktoré budú musieť riešiť otázky týkajúce sa vlastníctva virtuálnych aktív, zodpovednosti za škody spôsobené virtuálnymi transakciami a iné problémy, ktoré sa môžu objaviť v digitálnej ekonomike. Rovnako to môže otvoriť príležitosti pre cezhraničný prevod peňazí spôsobom, ktorý bude ťažšie monitorovateľný.

Už v súčasnosti sa kryptomeny využívajú na účely legalizácie výnosu z trestnej činnosti a uľahčovania kriminálnych prevodov peňazí. Medzi jednotlivé techniky legalizácie výnosu z trestnej činnosti patrí tzv. peeling a jeho opak tzv. layering. Pri peelingu dochádza k opakovanému posielaní malých čiastok nepresahujúcich istú sumu (napr. 1.000 eur) z celkového množstva kryptomien na rôzne adresy (najčastejšie burzy alebo zmenárne, kde môžu byť kryptomeny zmenené na fiat meny), pričom takýmto konaním dochádza k eliminovaniu jedného z najrizikovejších faktorov pri kontrole transakcií a to vysokých objemov súm. Layering predstavuje pridávanie dodatočných vrstiev (transakcií z rôznych adries kryptomien) k originálnej transakcii, čo v konečnom dôsledku sťažuje identifikáciu majiteľov adries a vykonávateľov transakcií v rámci celého procesu.[43]

Pri uvedenom konaní pri splnení ďalších predpokladov môže dojsť k naplneniu skutkovej podstaty trestného činu legalizácie výnosu z trestnej činnosti v zmysle ust. § 233[44] a § 233a[45] Trestného zákona.[46] Obe uvedené skutkové podstaty trestného činu legalizácie výnosu z trestnej činnosti vo svojej objektívnej stránke postihujú konanie páchateľa, ktorý taxatívne vy-

[43] ŠANTA, Ján, ŠANTA, Ivo, ŠIROKÝ, Tomáš. K niektorej aktuálnej trestnej činnosti spojenej s virtuálnymi menami. *Justičná revue*, 74, 2022, č. 4, s. 480.

[44] Podľa § 233 ods. 1 Trestného zákona kto nadobudne, prechováva alebo užíva vec, ktorá je výnosom z trestnej činnosti spáchanej inou osobou na území Slovenskej republiky alebo v cudzine, potrestá sa odňatím slobody na dva roky až päť rokov.

[45] Podľa § 233a ods. 1 Trestného zákona kto z nedbanlivosti ukryje, na seba alebo iného prevedie, prechováva alebo užíva vec väčšej hodnoty, ktorá je výnosom z trestnej činnosti spáchanej inou osobou na území Slovenskej republiky alebo v cudzine, potrestá sa odňatím slobody až na dva roky.

[46] V Trestním zákoníku sú predmetné trestné činy upravené v § 216 a § 217.

medzenými spôsobmi disponuje s výnosom pochádzajúcim z trestnej činnosti.[47]

Očakáva sa, že tento trend legalizácie výnosu z trestnej činnosti pomocou virtuálnych mien bude rásť s ich ďalším rozvojom. Možnosti anonymného používania kryptomien sťažia orgánom činným v trestnom konaní odhalenie trestných činov spojených s legalizáciou výnosu z trestnej činnosti a podvodmi.[48] Vzhľadom k tomu, že v metaverse budú existovať vlastné digitálne meny a hospodárske systémy, môže dôjsť k výskytu podvodov, kde sa používateľom sľubujú falošné investičné príležitosti, alebo k podvodom pri nákupe falošných digitálnych produktov napĺňajúci skutkovú podstatu už spomínaného trestného činu podvodu.[49]

3.3 OBŤAŽOVANIE A SEXUÁLNE ZNEUŽÍVANIE

Nebezpečné elektronické obťažovanie predstavuje v súčasnosti závažný problém, pričom až 58 % žien v medzinárodnom prieskume v roku 2020 realizovaného neziskovou organizáciou Plan International sa už s takýmto obťažovaním stretlo.[50] Preto je dôvodné očakávať, že takéto správanie bude existovať aj v metaverse, pričom bude mať rastúci potenciál.

Už v roku 2007 došlo k situácii, keď jeden avatar v online videohre Second Life údajne znásilnil druhého. Viacerí kritici odmietli simulovaný útok ako digitálnu fikciu, ale polícia v Belgicku proti páchateľovi reálne začala trestné stíhanie pre trestný čin znásilnenia.[51] Rovnako sme sa mohli stretnúť

---

[47] ŠANTA, Ján, ŠANTA, Ivo, ŠIROKÝ, Tomáš. K niektorej aktuálnej trestnej činnosti spojenej s virtuálnymi menami. *Justičná revue*, 74, 2022, č. 4, s. 490, 484 – 499.

[48] EUROPOL: Cryptocurrencies: tracing the evolution of criminal finances. [online]. 2022. [cit. 01.04.2023]. Dostupné z: https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances

[49] Over 80 percent of NFTs minted for free on OpenSea are fake, plagiarized or spam. [online]. [cit. 01. 04. 2023]. Dostupné z: https://www.engadget.com/opensea-freeminting-tool-220008042.html

[50] Online harassment is silencing girls: the EU and its Member States can do more and better. [online]. 2020. [cit. 02. 04. 2023]. Dostupné z: https://plan-international.org/eu/ blog/ 2020/11/25/online-harassment/

[51] Virtual rape is traumatic, but is it a crime? [online]. 2007. [cit. 02. 04. 2023]. Dostupné z: https://www.wired.com/2007/05/sexdrive-0504/

aj s incidentom, ktorý obeť opísala ako „online znásilnenie“ v rámci platformy Horizon Venues.[52]

Tieto druhy virtuálnych konaní vyvolávajú vážne otázky o uplatniteľnosti súčasnej legislatívy. Znásilnenie v zmysle § 185 Trestního zákoníka[53], resp. § 199 Trestného zákona[54] alebo sexuálny nátlak, resp. sexuálne násilie podľa § 186 Trestního zákoníka[55], resp. § 200 Trestného zákona[56] vyžaduje fyzický kontakt, zatiaľ čo kontakt s avatarom v metaverse je podľa definície virtuálny. Avšak z dôvodu napredovania technológii môže byť vymedzenie medzi fyzickým a virtuálnym svetom čoraz problematickejšie. Aj vzhľadom na prvé pokusy s implantovanými čipmi v mozgu opíc sa takéto konania môžu stať realistickejšími, aj keď k priamemu fyzickému kontaktu nemusí dôjsť.[57] Preto bude potrebné z legislatívneho hľadiska takýto technologický pokrok zohľadniť nie len v trestnoprávnych normách v zmysle citovaných ustanovení Trestního zákoníka, ako aj slovenského Trestného zákona, ale aj na úrovni medzinárodných dohovoroch.

V metaverse môžu vzniknúť nové formy znásilnenia a sexuálneho násilia, ktoré pre súčasné trestné právo ešte nie sú známe, pretože všetky interakcie v tomto virtuálnom svete môžu byť zaznamenané na blockchaine pod jednou identitou. Táto skutočnosť môže pomôcť pri vyšetrovaní a od-

---

[52] Reality or Fiction? [online]. 2021. [cit. 02. 04. 2023]. Dostupné z: https://medium.com/kabuni/fiction-vs-non-fiction-98aa0098f3b0

[53] Podľa § 185 ods. 1 Trestního zákoníka kdo jiného násilím nebo pohrůžkou násilí nebo pohrůžkou jiné těžké újmy donutí k pohlavnímu styku, nebo kdo k takovému činu zneužije jeho bezbrannosti, bude potrestán odnětím svobody na šest měsíců až pět let.

[54] Podľa § 199 ods. 1 Trestného zákona kto násilím alebo hrozbou bezprostredného násilia donúti ženu k súloži alebo kto na taký čin zneužije jej bezbrannosť, potrestá sa odňatím slobody na päť rokov až desať rokov.

[55] Podľa § 186 ods. 1 Trestního zákoníka kdo jiného násilím, pohrůžkou násilí nebo pohrůžkou jiné těžké újmy donutí k pohlavnímu sebeukájení, k obnažování nebo jinému srovnatelnému chování, nebo kdo k takovému chování přiměje jiného zneužívaje jeho bezbrannosti, bude potrestán odnětím svobody na šest měsíců až čtyři léta nebo zákazem činnosti.

[56] Podľa § 200 ods. 1 Trestného zákona kto násilím alebo hrozbou bezprostredného násilia donúti iného k orálnemu styku, análnemu styku alebo k iným sexuálnym praktikám alebo kto na taký čin zneužije jeho bezbrannosť, potrestá sa odňatím slobody na päť rokov až desať rokov.

[57] What should be considered a crime in the metaverse. [online]. 2022. [cit. 02. 04. 2023]. Dostupné z: https://www.wired.com/story/crime-metaverse-virtual-reality/

haľovaní páchateľov týchto trestných činov. Informácie zaznamenané v blockchaine môžu byť cenným dôkazom a následne môžu pomôcť pri identifikácii páchateľov. Avšak toto riešenie prináša aj potenciálne nebezpečenstvo pre obete, pretože zaznamenané informácie môžu byť opakovane vyhľadávané a viesť k sekundárnej viktimizácii, ktorá môže spôsobiť, že obete budú vystavené ďalším psychickým a emocionálnym ťažkostiam tak ako je tomu vo fyzickom svete, vzhľadom na podobnosť avatara fyzickej schránky obete a emocionálnemu prepojeniu so zážitkom, čím sa zvyšuje závažnosť tohto problému.

Aj napriek tomu, že používanie takýchto služieb môže požadovať overenie veku užívateľa, takéto overenie sa dá ľahko obísť a neexistuje tak vekový konsenzus pre vyššie popísané možnosti konania. Na platforme sociálnej siete VRChat sa používatelia stretávali so striptízovými klubmi.[58] Medzitým v platforme Roblox ľudia vytvárali sexuálne „byty“, kde dochádzalo medzi avatarmi k vzájomnej súloži.[59] Napriek tomu, že takéto konania nemusia byť v súlade s podmienkami používania jednotlivých platforiem, nie len maloletí užívatelia sú aj napriek tomu s takýmito konaniami konfrontovaní.

Metaverse môže byť ideálnym miestom pre páchateľov mravnostnej kriminality na získanie prístupu k maloletým, nakoľko môže páchateľom umožniť zapojiť sa do interakcie s maloletými a postupne prehĺbiť ich zneužívanie za pomoci vzájomnej komunikácie bez toho, aby sa s nimi stretli vo fyzickom svete. Navyše, pre maloletých môže byť náročné rozlíšiť dospelých od iných maloletých v metaverse, čo vytvára nebezpečné prostredie pre grooming a iné formy sexuálneho zneužívania detí.

Vývoj v oblasti haptiky a podobných technológií prináša nový zmyslový prvok pre interakcie používateľov. Páchatelia môžu využiť tieto technológie na sexuálne zneužívanie maloletých bez fyzického kontaktu. Vzhľadom na realistické vizuálne prezentácie avatarov a možnosti pocitov by mohli

[58] Metaverse app allows kids into virtual strip clubs. [online]. 2022. [cit. 03. 04. 2023]. Dostupné z: https://www.bbc.com/news/technology-60415317

[59] The children’s game with a sex problem. [online]. 2022. [cit. 03. 04. 2023]. Dostupné z: https://www.bbc.com/news/technology-60314572

páchateľom poskytnúť nový fyzický rozmer pri sexuálnom zneužívaní v metaverse.

3.4 TRESTNÉ ČINY TERORIZMU A EXTRÉMIZMU

V minulosti sme videli, ako teroristi využívali internet na komunikáciu a organizáciu svojich aktivít, pričom vhodné prostredie môžu nájsť aj v metaverse, ktorý môžu použiť predovšetkým na propagandu, nábor a výcvik nových členov.[60]

Metaverse môže byť skutočne užitočným prostredím na školenie a vzdelávanie, nielen v oblastiach ako hry a zábava, ale aj v závažnejších oblastiach, akými je aj terorizmus. Využitie metaverse na školenie umožňuje používateľom získať praktické skúsenosti bez potreby fyzickej prítomnosti a bez rizika skutočných nebezpečenstiev. Avšak virtuálna simulácia miesta môže byť zneužitá pre plánovanie a trénovanie teroristických aktivít, kde môžu byť používané virtuálne nástroje na plánovanie a koordináciu útokov vo fyzickom svete. To znamená, že metaverse môže byť využívaný aj ako tréningový nástroj pre teroristické skupiny a umožniť vojenským jednotkám vykonávanie prieskumu a plánovanie cieľov v rámci virtuálneho prostredia. Takéto virtuálne prostredie môže byť veľmi užitočné pre plánovanie misií, ktoré môžu byť použité na testovanie rôznych scenárov a stratégií v rámci teroristických útokov. Z trestnoprávneho hľadiska hovoríme pri takomto konaní o skutkovej podstate trestného činu teroristického útoku podľa § 311 ods. 1 písm. a) Trestního zákoníka[61] v štádiu prípravy podľa § 20 Trestního zákoníka.[62]

Na druhej strane metaverse môže používateľom umožniť vytvoriť taký virtuálny svet, ktorý by si chceli docieliť svojimi aktivitami vo fyzickom svete, napr. vytvoriť virtuálny kalifát alebo virtuálne miesto nadradenosti jednej rasy. Členovia takýchto miest by mohli žiť svoj virtuálny život podľa svojich pravidiel, ktoré môžu byť v rozpore so zákonmi štátov a hodnotami spoločnosti, v ktorej žijú vo fyzickom svete. Pre kontext možno uviesť sku-

[60] Violent extremists could find the metaverse a useful recruiting and organizing tool – and a target-rich environment. [online]. 2022. [cit. 04. 04. 2023]. Dostupné z: https://www.nextgov.com/ideas/2022/01/metaverse-offers-future-full-potential-terrorists-and-extremiststoo/360494/

točnosť, že na platforme Roblox užívatelia vytvárali nacistické plynové komory a vyhladzovacie tábory.[63] Uvedené konania tak môžu napĺňať skutkovú podstatu trestného činu založenia, podpory a propagácie hnutia smerujúceho k potlačeniu základných práv a slobôd podľa § 421 Trestného zákona[64], nakoľko podporou je akékoľvek konanie, ktorým sa poskytuje ideológii alebo jej šíriteľom možnosť šírenia, ako aj možnosť získavania prívržencov. Prostriedky podpory môžu byť materiálne, napr. poskytovaním financií, technických prostriedkov, vytváraním podmienok na založenie hnutia alebo nemateriálne, napr. získavaním priaznivcov, možnosťou publikovať názory, umožnením vydávať letáky a tlačoviny a pod.[65]

Virtuálne svety môžu byť využité aj na vytvorenie paralelného sveta, kde by boli uvalené extrémistické pravidlá na každého, kto by do tohto sveta vstúpil. Títo používatelia by potom mohli žiť a konať podľa scenárov, ktoré by podkopávali akceptovanie právneho štátu. To by mohlo vytvoriť

[61] Podľa § 311 ods. 1 písm. a) Trestního zákoníka kdo v úmyslu poškodit ústavní zřízení nebo obranyschopnost České republiky, narušit nebo zničit základní politickou, hospodářskou nebo sociální strukturu České republiky nebo mezinárodní organizace, závažným způsobem zastrašit obyvatelstvo nebo protiprávně přinutit vládu nebo jiný orgán veřejné moci nebo mezinárodní organizaci, aby něco konala, opominula nebo trpěla, zničí nebo poškodí ve větší míře veřejné prostranství, majetek nebo veřejné zařízení, dopravní nebo telekomunikační systém, pevnou plošinu na pevninské mělčině, energetické, vodárenské, zdravotnické nebo jiné důležité zařízení, včetně počítačového systému, na jehož fungování takové zařízení, systém nebo plošina závisejí, s cílem vydat majetek v nebezpečí škody velkého rozsahu, bude potrestán odnětím svobody na tři až dvanáct let, popřípadě vedle tohoto trestu též propadnutím majetku.

[62] Podľa § 20 Trestního zákoníka jednání, které záleží v úmyslném vytváření podmínek pro spáchání zvlášť závažného zločinu, zejména v jeho organizování, opatřování nebo přizpůsobování prostředků nebo nástrojů k jeho spáchání, ve spolčení, srocení, v návodu nebo pomoci k takovému zločinu, je přípravou jen tehdy, jestliže to trestní zákon u příslušného trestného činu výslovně stanoví a pokud nedošlo k pokusu ani dokonání zvlášť závažného zločinu.

[63] Children's gaming platform removes 'disturbing' nazi concentration camp 'experience' with gas chambers. [online]. 2022. [cit. 04. 04. 2023]. Dostupné z: https://www.algemeiner.com/2022/02/21/childrens-gaming-platform-removes-disturbing-naziconcentration-camp-experience-with-gas-chambers/

[64] Podľa § 421 ods. 1 Trestného zákona kto založí, podporuje alebo propaguje skupinu, hnutie alebo ideológiu, ktorá smeruje k potlačeniu základných práv a slobôd osôb, alebo ktoré hlása rasovú, etnickú, národnostnú alebo náboženskú nenávisť alebo kto propaguje skupinu, hnutie alebo ideológiu, ktorá v minulosti smerovala k potlačeniu základných práv a slobôd osôb, potrestá sa odňatím slobody na jeden rok až päť rokov.

[65] ČENTÉŠ, Jozef a kol. *Trestný zákon - Veľký komentár*. Eurokódex, 2020. s. 941.

nové prostredie pre extrémistov, aby šírili svoju ideológiu a vykonávali nábor nových členov do svojich organizácií.

3.5 ŠÍRENIE POPLAŠNEJ SPRÁVY A DEZINFORMÁCIE

Súčasný Web2.0 viedol k vzniku bezprecedentnej presnosti v schopnostiach zamerať sa na špecifické demografické skupiny s cieľom ovplyvniť ich správanie na účely komerčného alebo politického zisku.[66] Nesmierne zvýšené množstvo údajov, ktoré môžu nové zariadenia získať od používateľov platforiem budú mať väčší vplyv na správanie ľudí, pričom takéto správanie môže destabilizovať jednotlivé komunity, ktoré majú orgány činné v trestnom konaní chrániť, a páchatelia môžu tento vplyv využiť aj na to, aby sa zamerali na svoje obete.

Súčasné technológie už umožňujú personalizované zameranie reklám na základe vyhľadávania a zhromažďovanie informácií o preferenciách a aktivitách používateľov na sociálnych sieťach. Metaverse však poskytuje ešte väčšie možnosti na sledovanie a zameriavanie informácií na konkrétnych používateľov, vzhľadom na ich správanie vo virtuálnom svete.

Na platformách metaverse sa môžu tiež šíriť hoaxy a poplašné správy, podobne ako na sociálnych sieťach, čo môže napĺňať skutkovú podstatu trestného činu šírenia poplašnej správy podľa § 361 ods. 1 Trestného zákona[67], resp. § 357 ods. 1 Trestního zákoníka[68], ktorých objektom je verejný kľud a záujem na ochrane obyvateľstva pred vyvolávaním vážneho znepokojenia na základe rozširovania nepravdivých poplašných správ. Poplašnou správou je taká objektívne nepravdivá správa, ktorá je spôsobila podľa svojho obsahu vyvolať obavy z určitej udalosti u aspoň časti obyva-

[66] BASTICK, Zach Would you notice if fake news changed your behavior? An experiment on the unconscious effects of disinformation, In: *Computers in human behavior*, 2021, Volume 116, s. 33.

[67] Podľa § 361 ods. 1 Trestného zákona kto úmyselne spôsobí nebezpečenstvo vážneho znepokojenia aspoň časti obyvateľstva nejakého miesta tým, že rozširuje poplašnú správu, ktorá je nepravdivá, alebo sa dopustí iného obdobného konania spôsobilého vyvolať také nebezpečenstvo, potrestá sa odňatím slobody až na dva roky.

[68] Podľa § 357 ods. 1 Trestního zákoníka kdo úmyslně způsobí nebezpečí vážného znepokojení alespoň části obyvatelstva nějakého místa tím, že rozšiřuje poplašnou zprávu, která je nepravdivá, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.

teľstva.[69] Avšak v tomto prípade by mohlo byť oveľa ťažšie ich overiť, pretože šírenie informácií by bolo ešte viac decentralizované a mohli by ich šíriť aj fiktívne osoby alebo umelá inteligencia.

V kombinácii s algoritmami a technológiami, ktoré sledujú správanie používateľov, môžu poplašné správy v metaverse mať ešte väčší dopad a vďaka kombinácii technológií, ktoré sledujú správanie používateľov by mohlo dôjsť k ešte väčšiemu šíreniu poplašných správ. Tento dopad môže byť ešte silnejší vďaka možnosti ponoreného zážitku, ktorý sa môže javiť ako reálnejší. Ďalej, decentralizácia šírenia poplašných správ by mohla viesť k situácii, kedy bude nemožné odstrániť nepravdivé informácie, pretože sa budú šíriť cez rôzne platformy a siete, vrátane Web3 technológie.

4. ZÁVER

V tomto príspevku sme si predstavili základne druhy trestnej činnosti, ktoré môžu byť spáchané v metaverse. Aj keď predmetný príspevok môže vyznievať ako sci-fi, netreba zabúdať, že takýmto sci-fi bol na počiatku tohto milénia aj samotný internet. Napriek tomu má metaverse stále ďaleko od vízií inovátorov a technologických spoločnosti. Nie je možné predpokladať, ako sa daný koncept bude vyvíjať, ale technológie napredujú každým dňom, pričom legislatíva na ne nedokáže v dostatočnej miere reagovať, čo sa preukázalo aj pri počítačovej kriminalite.

Vďaka výraznému vývoju vo virtuálnej realite budeme navštevovať obchodné centrá, cestovať, stretávať sa so známymi v kaviarňach a vymieňať si zážitky spôsobom, ktorý bude pôsobiť až prekvapivo autenticky. Metaverse už existuje v štruktúre internetových hier pre viacerých hráčov. Čoskoro však môžeme dosiahnuť éru pohlcujúcich zážitkov na nerozoznanie od nášho skutočného sveta, čo prinesie nové druhy angažovanosti pre hráčov, ale aj bežných používateľov internetu. Decentraland a Somnium Space, dva prototypy produkčných metaverse, už demonštrujú virtuálne začiatky civilizácie s ľuďmi, ktorí osídľujú pôdu, spoločensky sa stýkajú, obchodujú s vecami a presadzujú vlastníctvo občianskych slobôd.

[69] ŠÁMAL, Pavel, GŘIVNA, Tomáš, BOHUSLAV, Lukáš a kol. *Trestní právo hmotné.* 9. vydanie. Wolters Kluwer ČR, 2021. s. 1027.

Dohliadanie na metaverse predstavuje značnú výzvu. Významnú rolu v tomto procese budú mať organizácie, ktoré poskytujú platformy pre monitorovanie a moderovanie obsahu, ktorý sa na nich nachádza. Súčasne budú zodpovedné aj za poskytnutie nástrojov a mechanizmov, ktoré umožnia efektívne presadzovanie práva a ochranu záujmov v rámci týchto platform. Podobne ako v prípade súčasných online aktivít, aj tu sa predpokladajú zložité výzvy, ktoré budú umocnené novými, doposiaľ nepoznanými problémami. Riešenie týchto problémov si vyžaduje zodpovedný prístup a aktívnu spoluprácu medzi všetkými zainteresovanými stranami.

Povaha metaverse predstavuje značnú výzvu z hľadiska kontroly a monitorovania, čiže sledovania a regulácie toho, čo sa na týchto platformách deje. Táto výzva vyplýva z faktu, že očakávaný nárast počtu platforiem zvýši nároky na kontrolu a reguláciu obsahu. Monitorovanie online aktivít v metaverse predstavuje náročnú úlohu, ktorá sa týka nielen moderovania značného množstva obsahu, ale aj sledovania správania používateľov, ktoré je oveľa viac závislé od kontextu než samotný obsah. Interakcie v metaverse môžu byť takmer také efemérne ako v reálnom svete, čo znamená, že po týchto interakciách nemusia zostať žiadne stopy použiteľné na účely trestného konania.

História internetu a ďalších technológií nás naučila, že trestnú činnosť s nimi spojenú nie je možné podceňovať. Pochopenie vývoja technológii predstavuje hlavnú výzvu pre orgány činné v trestnom konaní, aby dokázali na trestnú činnosť reagovať adekvátnym spôsobom. Je preto potrebné získavať skúsenosti s novými technológiami a osvojovať si potrebné informácie, ktoré môžu dopomôcť k úspešnému trestnému stíhaniu páchateľov. Vybudovanie medzinárodnej siete odborníkov a následná medzinárodná spolupráca sa tak javí ako najlepšia možnosti budovania poznatkov nie len v oblasti metaverse.

5. ZOZNAM POUŽITÝCH ZDROJOV

5.1 KNIHY

[1] ČENTÉŠ, Jozef a kol. *Trestný zákon - Veľký komentár*. Eurokódex, 2020. 1024 s. ISBN 978-808-1550-96-6.

[2] MA Winston, HUANG Ken. *Blockchain and Web3: Building the Cryptocurrency, Privacy, and Security Foundations of the Metaverse.* 1st Edition, Wiley, 2022, 400 s. ISBN 978-111-9891-08-6.

[3] ŠÁMAL, Pavel, GŘIVNA, Tomáš, BOHUSLAV, Lukáš a kol. *Trestní právo hmotné.* 9. vydanie. Wolters Kluwer ČR, 2021, s. 698. ISBN 978-807-5987-64-8.

5.2 PRÍSPEVOK V ODBORNOM PERIODIKU

[4] BASTICK, Zach. Would you notice if fake news changed your behavior? An experiment on the unconscious effects of disinformation, *Computers in human behavior*, 2021, Volume 116, s. 25 – 48. ISSN 0747-5632.

[5] KUMAR, Randhir, TRIPATHI, Rakesh. Implementation of distributed file storage and access framework using IPFS and blockchain, *Fifth international conference on image information processing.* Institute of Electrical and Electronics Engineers (IEEE). 2019. s. 241 - 259. ISBN 978-172-8109-00-8.

[6] ŠANTA, Ján, ŠANTA, Ivo, ŠIROKÝ, Tomáš. K niektorej aktuálnej trestnej činnosti spojenej s virtuálnymi menami. *Justičná revue*, 74, 2022, č. 4, s. 484 – 499. ISSN 1335-6461

5.3 ONLINE ZDROJE

[7] ALI Mansoor, NACEM Faisal, KADDOUM, Georges, HOSSAIN, Ekram. Metaverse Communications, Networking, Security, and Applications: Research Issues, State-of-the-Art, and Future Directions. [online]. 2022. [cit. 18.08.2023]. Dostupné z: https://arxiv.org/pdf/2212.13993.pdf

[8] BANAEIAN FAR Saeed, RAD IMANI Azadeh. Applying Digital Twins in Metaverse: User Interface, Security and Privacy Challenges. [online]. 2022. [cit. 08.08.2023]. Dostupné z: https://arxiv.org/pdf/2204.11343.pdf

[9] CURTIS, Joanna, OXBURGH, Gavin. Understanding cybercrime in 'real world' policing and law enforcement. [online]. 2022. [cit. 07.11.2023]. Dostupné z: https://journals.sagepub.com/doi/10.1177/0032258X221107584

[10] Elon Musk má veľké plány: Čochvíľa začne testovať Neuralink aj na ľuďoch! [online]. 2022. [cit. 19.03.2023]. Dostupné z: https://www.techbyte.sk/2022/12/elon-musk-zacne-testovat-neuralink-ludoch/

[11] EUROPOL: Cryptocurrencies: tracing the evolution of criminal finances. [online]. 2022. [cit. 01.04.2023]. Dostupné z: https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances

[12] Genesis marketplace, a digital fingerprint darknet store insights: Into genesis marketplace, a black market trading in digital identity. [online]. [cit. 29.03.2023]. Dostupné z: https://www.f5.com/labs/articles/threat-intelligence/genesis-marketplace--a-digital-fingerprint-darknet-store

[13] HUYNH, Thien, REDDY GADEKALLU, Thippa, WANG Weizheng et al. Blockchain for the metaverse: A Review. [online]. 2022. [cit. 18.08.2023]. Dostupné z: https://www.sciencedirect.com/science/article/pii/S0167739X23000493

[14] HUYNH Thien, PHAM Quoc-Viet, PHAM Xuan-Qui et. Artificial Intelligence for the Metaverse: A Survey. [online]. 2022. [cit. 11.08.2023]. Dostupné z: https://arxiv.org/pdf/2202.10336.pdf

[15] Children's gaming platform removes 'disturbing' nazi concentration camp 'experience' with gas chambers. [online]. 2022. [cit. 04.04.2023]. Dostupné z: https://www.algemeiner.com/2022/02/21/childrens-gaming-platform-removes-disturbing-naziconcentration-camp-experience-with-gas-chambers/

[16] Introducing Meta: A social technology company. [online]. 2021. [18.03.2023]. Dostupné z: https://about.fb.com/news/2021/10/facebook-company-is-now-meta/

[17] Metaverse app allows kids into virtual strip clubs. [online]. 2022. [cit. 03.04.2023]. Dostupné z: https://www.bbc.com/news/technology-60415317

[18] Online harassment is silencing girls: the EU and its Member States can do more and better. [online]. 2020. [cit. 02.04.2023]. Dostupné z: https://plan-international.org/eu/ blog/2020/11/25/online-harassment/

[19] Over 80 percent of NFTs minted for free on OpenSea are fake, plagiarized or spam. [online]. [cit. 01.04.2023]. Dostupné z: https://www.engadget.com/opensea-freeminting-tool-220008042.html

[20] Policing in the metaverse: what law enforcement needs to know. [online]. 2022. [18.03.2023]. Dostupné z: https://www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know

[21] HUYNH-THE Thien, PHAM Quoc-Viet, PHAM Xuan-Qui et. Artificial Intelligence for the Metaverse: A Survey. [online]. 2022. [cit. 11.08.2023]. Dostupné z: https://arxiv.org/pdf/2202.10336.pdf

[22] Predstavil sa ako jej vnuk: Seniorku v Bratislave obrali o 14.000 eur. [online]. [cit. 31.03.2023]. Dostupné z: https://www.teraz.sk/regiony/predstavil-sa-ako-jej-vnuk-seniorku-v-b/704934-clanok.html

[23] Rada Európskej únie: Metaverse – virtual world, real challenges. [online]. 2022. [cit. 19.03.2023]. Dostupné z: https://www.consilium.europa.eu/media/54987/metaverse-paper-9-march-2022.pdf

[24] RASHID, Mamunur, CHOI, Piljoo, KWON, Ki-Ryong. Emergence of the Metaverse: How Blockchain, AI, AR/VR, and Digital Transformation Technologies will change the Future World. [online]. 2022. [cit. 09.08.2023]. Dostupné z: https://www.researchgate.net/publication/362302545_Emergence_of_the_Metaverse_How_Blockchain_AI_ARVR_and_Digital_Transformation_Technologies_will_change_the_Future_World

[25] Reality or Fiction? [online]. 2021. [cit. 02.04.2023]. Dostupné z: https://medium.com/kabuni/fiction-vs-non-fiction-98aa0098f3b0

[26] Rozhodnutie Rady, ktorým sa členské štáty poverujú podpísať v záujme Európskej únie Druhý dodatkový protokol k Dohovoru o počítačovej kriminalite o posilnenej spolupráci a sprístupňovaní elektronických dôkazov. [online]. 2022. [cit. 27.03.2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:52021PC0718

[27] The children's game with a sex problem. [online]. 2022. [cit. 03.04.2023]. Dostupné z: https://www.bbc.com/news/technology-60314572

[28] Violent extremists could find the metaverse a useful recruiting and organizing tool – and a target-rich environment. [online]. 2022. [cit. 04.04.2023]. Dostupné z: https://www.nextgov.com/ideas/2022/01/metaverse-offers-future-full-potential-terrorists-and-extremiststoo/360494/

[29] Virtual rape is traumatic, but is it a crime? [online]. 2007. [cit. 02.04.2023]. Dostupné z: https://www.wired.com/2007/05/sexdrive-0504/

[30] WANG Yuntao, SU Zhou, ZHANG Ning et. A Survey on Metaverse: Fundamentals, Security, and Privacy. [online]. 2022. [cit. 09.08.2023]. Dostupné z: https://arxiv.org/pdf/2203.02662.pdf

[31] What is the metaverse and how will it work? [online]. [18.03.2023]. Dostupné z: https://blog.servermania.com/what-is-metaverse/

[32] What should be considered a crime in the metaverse. [online]. 2022. [cit. 02.04.2023]. Dostupné z: https://www.wired.com/story/crime-metaverse-virtual-reality/

[33] Which companies are investing in the metaverse? 7 stocks to watch. [online]. [18.03.2023]. Dostupné z: https://finance.yahoo.com/news/companies-investing-metaverse-7-stocks

5.4 ONLINE PRÍSPEVOK V ODBORNOM PERIODIKU

[34] FENWICK, Mark, JURCYS, Paulius: The contested meaning of Web3 and why it matters for (IP) Lawyers. In: Product and services. [online]. 2022. [cit. 19.03.2023]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4017790
