Pécsi Tudományegyetem
Állam- és Jogtudományi Kar
Doktori Iskola

Eszteri Dániel

A World of Warcraft-tól a Bitcoin-ig: Az egyén, a gazdaság és a tulajdon helyzetének magán- és büntetőjogi elemzése a virtuális közösségekben

Doktori értekezés tézisei

Témavezető:
Polyák Gábor PhD
habilitált egyetemi docens

Pécs
2015

University of Pécs
Faculty of Law
Doctoral School

Dániel Eszteri

From World of Warcraft to Bitcoin: Analysis of the Status of Individuals, Economy and Property in Virtual Societies from the Point of Civil and Criminal Law

Theses of the Ph.D. dissertation

Consultant:
Gábor Polyák PhD, dr. habil.
Associate Professor

Pécs
2015

Tartalomjegyzék

A kutatás eredményeinek összefoglalása

A kutatásaim eredményeit az alábbiakban kívánom röviden összefoglalni, az egyes részek és fejezetek mentén feltárva a főbb megállapításokat, kritikákat és javaslatokat.

1. Bevezető gondolatok: a dolgozat témájának elméleti-történeti háttere és fő kérdései

Az értekezés első részében ismertettem a virtuális valóság fogalmát és annak értelmezési dimenzióit. A virtuális valóság ezek alapján úgy írható körül, mint egy csúcstechnológiába integrált interaktív médium, amely feltételezi a személyiségnek az általa teremtett alternatív valóságba történő oly mértékű belemerülését, hogy az egyén akár hajlamossá válhat a fizikai valójától való teljes elszakadásra és ez által újfajta énképeket építhet ki.

Ebben az értelemben a virtuális online közösségek első szintje a valós idejű online csatornákon (chat, fórum, videotelefon) keresztüli kommunikáció, melyek aktív használata során a személyiség elkezd kilépni a fizikai korlátok mögül. A közösségek második szintjeként a valóságszimulátorokat és online játékokat jelöltem meg, mivel a felhasználó személyisége ekkor már egy interaktív, általa irányított avatárban ölt testet, amellyel részese lehet egy olyan szimulációnak, mely akkor is tovább él, ha esetleg abból az egyes résztvevők kijelentkeznek. A közösségek harmadik szintje az egyes virtuális világok közötti átjárhatóság lehetősége, mely irányba a különböző szimulációk egységes elszámolási rendszerei (pl. Facebook-gamecard rendszer), vagy az online játékosok interaktív arénái és piacai mutatnak.

Az online virtuális közösségek fejlődéstörténetének rövid bemutatása kapcsán kitértem az egyes altípusok rövid jellemzőire, amely a téma átláthatóságát könnyítette. A sok-szereplős online szerepjátékok fogalmát, rendszerfelépítésüket, valamint az általuk megteremtett virtuális gazdaság alapvető jellemzőit is vázoltam a részben, ami a későbbi, konkrétabb problémák elemzése kapcsán szintén elengedhetetlen a megértéshez. Megállapítottam, hogy a virtuális gazdaságokban létrejövő tranzakciók olyan értékeket képviselnek, amelyek valós pénzben kifejezhető értékkel bírnak, a virtuális tárgyakkal való kereskedés pedig ma már teljesen hétköznapi jelenségnek számít a felhasználók körében.

Ezek a megállapítások előrevetítettek a disszertáció központi kérdéseit: A kereskedelmi viszonyokban a virtuális tárgyakra milyen szabályozás vonatkozik? Függetleníthető-e a szerzői jogi normáktól a virtuális gazdaság ezen része? Fennállhat-e tulajdonjog olyan tisztán virtuálisan létező árucikkeken, melyek nem felelnek meg a polgári jog dolog fogalmának, de viselkedésüket tekintve többek puszta pénzben kifejezhető értékkel bíró adatoknál? A szoftver

működése milyen kihatással lehet a virtuális világok és gazdaságok mindennapjaira? Milyen felépítésű virtuális piacok és árucikkek léteznek? Képezhetik-e bűncselekmény elkövetési tárgyát a virtuális eszközök?

Az első rész végül egy a központi témához lazán kapcsolódó okfejtéssel zárul a számítógépes (játék)szoftverek és a művészet viszonyáról, amely inkább művészeti, mint jogi okfejtés, szerepe viszont az, hogy egy különleges szempontból alapozza meg a dolgozat második nagyobb részének a szerzői jogokat vizsgáló felütését, és egyben indokolja, hogy a virtuális tulajdon problematikáját legelőször e jogág oldaláról közelítsük meg.

A dolgozat elején a magyar jogot és joghatóságot jelöltem ki irányadónak a téma vizsgálata kapcsán felvetődő problémák alapjául, mint elsődleges keretrendszert.

2. A virtuális valóságokat megalkotók jogi helyzetét érintő főbb megállapítások

A dolgozat egyik fő problémáját érintő második rész az egyén jogi helyzetét elemzi a virtuális világokban.

Az első fejezet „a teremtők jogai" címet kapta, mivel az a virtuális valóságot megalkotók helyzetét mutatja be, első sorban az ilyenkor leginkább irányadó szerzői jogi normák oldaláról.

A jelenleg hatályos szerzői jogi szabályozás alapján megállapítottam, hogy a virtuális valóságokat szimuláló szoftverek olyan jellemzően több szerző által létrehozott alkotások, melyek kapcsán az azt fejlesztő cég gyakorolja a szerzőt megillető jogokat. A szerzők jellemzően a szoftverhez mellékelt általános szerződési feltételekben írják le részletesen, hogy a felhasználók milyen feltételrendszer betartása mellett használhatják azt. A szoftver használatára kizárólag ezeknek a végfelhasználói szerződéseknek az elfogadása után nyílik lehetőség, amennyiben pedig a felhasználó az abban kikötött szabályokat megsérti, az részéről szerződésszegésnek minősül.

A virtuális valóság szabályait és a felhasználók viselkedését szabályozó normák közül ismertettem továbbá a magatartási szabályokat tartalmazó kódexeket, amelyek megsértése további szankciókkal járhat a játékosok szemszögéből (pl. figyelmeztetés, kitiltás a játékból). Az általános szabályozó normák mellett ismertettem a klánszabályok általános jellemzőit is, amelyek jellemzője, hogy egy szűkebb értelemben vett játékoscsoport, a klán működésének belső szabályait jelentik. Ezek megszegése nem von maga után a szoftverhasználat szempontjából általános retorziót, azt „csupán" az a szűkebb játékosközösség szankcionálja, amelynek a felhasználó maga is tagja. Az absztrakt magatartási szabályokat tartalmazó

előírások után végül a felhasználói lehetőségeket alapvetően determináló technikai közeg jelentőségét emeltem ki.

A végfelhasználói szerződések szerepét a virtuális közösségek mindennapjaiban egy jogeseten keresztül szemléltettem, melyben a World of Warcraft-ban a játékos karakterét automatikusan irányító és ezzel a virtuális világ erőforrásait kiaknázó robotprogrammal kapcsolatban állapította meg egy amerikai bíróság, hogy annak használata sérti a szerződési feltételeket.

A fentiek után rátértem a játékfejlesztő cégek szerzői jogait leginkább érintő problémára, a virtuális világok és gazdaságok lemásolására, avagy a magánszerverek létrehozására. A magánszervereket speciális emulátorprogramokat használva lehet üzemeltetni, melyek az eredeti szoftver forráskódjának visszafejtésére épülnek, és használják fel a programot, ami a szerzői jog szerint engedélyköteles tevékenységnek számít. Ennek értelmében a szerzői jogosultak részéről megalapozottak azon igények, amelyek egy adott virtuális közösség szoftver nem hivatalos szerverének leállítását célozzák, mivel azok engedély nélküli üzemeltetése sérti a szerzői jogot.

A magánszerver létrehozásának főbb motiváció között említettem az otthoni, független programozási célokat, a kísérletezgetési kedvet és az önálló, módosított világok fejlesztését. Kisebb részt megállapítottam, hogy a magánszerver olyan üzleti vállalkozássá is válhat, amelyből akár jelentős hasznot is húzhatnak annak üzemeltetői. Sok esetben nemcsak a szoftver felhasználása, hanem az interneten keresztül elérhető más szolgáltatások (pl. honlap) utánzása is megtörténik a hivatalos verziók alternatívájára.

Elemeztem továbbá a büntetőjogi felelősség problémáját is, amely szintén felmerülhet egy nem hivatalos szerver üzemeltetése révén. Ennek kapcsán megállapításra került az is, hogy a vagyoni hátrány okozása szempontjából – amely a Btk.-ban nevesített szerzői jogok megsértése bűncselekmény szükséges tényállása eleme – nem mindegy, hogy a szoftver eredetileg milyen módon hozzáférhető és kell-e használata után havi-, vagy regisztrációs díjat fizetni. Fontos kiemelni továbbá, hogy a bűncselekményt nem a játékosok, hanem csupán a magánszerver tulajdonosa követheti el, mivel az ő magatartása (dekompiláció és felhasználás) kapcsán következik be a szerzői jogok sérelme és ezzel okozati összefüggésben a vagyoni hátrány. Az egyes felhasználók egy magánszerver használatáért így büntetőjogi felelősséggel nem tartoznak.

Megállapítottam továbbá, hogy a virtuális valóság szoftvert futtató magánszerver létrehozását elősegítő emulátorprogram készítése, átadása, terjesztése tehát abban az esetben alapozhat meg önálló, a Btk. 386. §-ába ütköző büntetőjogi felelősséget, ha az alapszoftver

forráskódjának használatához az valamilyen, annak védelmét biztosító hatásos műszaki intézkedést játszik ki. Ha a szoftver nem tartalmaz ilyen védelmet, akkor önmagában az emulátor létrehozása még nem alapoz meg büntetőjogi felelősséget.

3. A virtuális valóság résztvevőire vonatkozó főbb megállapítások: a munkabizonyítékokon alapuló virtuális tárgy és azok feletti használati jogosultság fogalma

Az egyén jogi helyzetét elemző második rész második fejezete „az emberek jogai" címet kapta, amely a felhasználókat érintő különféle problémákra keresi a választ és rátér a virtuális tulajdonjog problémájára, amely a dolgozat által az egyik fő elemzés alá vont terület és annak magvát, valamint fő kérdésfelvetését adja.

Különböző virtuális gazdaságok működése kapcsán hozott egyszerű példákon keresztül próbáltam szemléltetni és végigvezetni azt, hogy a virtuális közösségekben a használatba vett tárgyak milyen utakon kerülhetnek az egyes felhasználókhoz (barkácsolás, vadászat, nyeremény stb.). Azt is sikerült megállapítani, hogy minden egyes virtuális közösségben, ahol léteznek virtuális tárgyak, azok a világ fizetőeszközében kifejezett, leginkább a felhasználói kereslet és kínálat viszonya által meghatározott értéket képviselnek.

Az a probléma, hogy adott tárgyon ki gyakorolhatja a használati jogot, akkor kerül felszínre, ha adott virtuális világba, valahogyan való-világbeli elem kerül. Ez az elem legtöbbször a valós pénz (valamelyik ország hivatalos pénzneme), amelyért adott tárgyat adják-veszik. A játékszoftvert fejlesztő cégnek ugyanis legtöbbször nem érdeke beavatkozni, az általa teremtett virtuális piacba, amíg az virtuális keretek között marad. Szinte minden egyes játékban léteznek olyan nagyobb presztízsértékű tárgyak, melyekért akár tetemes összeget is hajlandóak egyes felhasználók áldozni, méghozzá valódi pénzben. Azonban nem csak ritka, hanem hétköznapibb tárgyakat, vagy akár kész karaktereket is lehetséges venni az ilyen kereskedelemre szakosodott honlapokon keresztül, sőt a felhasználók is sokszor eladásra kínálják saját virtuális vagyontárgyaikat olyan népszerű aukciós portálokon, mint például az eBay.

A következő pontokban sikerült megállapítani azt, hogy kevésbé tűnik ésszerűnek az álláspont, amely szerint a virtuális tárgyak felett a játékosok a játéktéren kívüli tranzakciók során nem rendelkezhetnek, mivel az egyes tárgy nem függetleníthető a szoftver forráskódjától, ami a fejlesztő szellemi tulajdonának szerves része.

A legfontosabb szempont a virtuális tárgyakon fennálló „tulajdonjogot” illetően, hogy azok nem adat, hanem használati eszköz („dolog”) módjára viselkednek a virtuális térben. Az elsősorban tengerentúli szerzők által képviselt virtual property elmélet rámutat arra, hogy a virtuális tárgyakat nem lehet lemásolni, sokszorosítani, csak a virtuális téren belül fizikailag átadni, amelynek eredményeképpen az egyik felhasználó rendelkezése alól átkerül az a másikéba. Ebben az értelemben adott tárgy megjelenését és a megjelenítéséért felelős szoftverkomponenst függetleníteni kell magától az adott virtuális tárgytól. A tárgy megjelenéséért felelős forráskód a szoftverfejlesztő szellemi tulajdonát képezi, azonban – a virtual property elmélet szerint – maga a virtuális tárgy, amiket az egyes felhasználók használnak, viszont nem. A virtuális tárgy a szoftver része, azonban mivel annak fizikai léte függetleníthető az egyes felhasználók részére nyújtott szolgáltatástól, önálló értéket képvisel.

A szoftverfejlesztő szellemi tulajdonát képezi a virtuális tárgy dizájnja és belső tulajdonságai, tehát annak forráskódja, viszont a virtuális gazdaságban forgalomba kerülő tárgy adott példánya nem tekinthető a szellemi tulajdona részének. A digitális térben létezhetnek olyan adatok, amelyek a szó klasszikus értelmében vett adat fogalmának nem feleltethetőek meg. A jelenlegi jogszabályi környezet az adatot úgy kezeli, mint egy másolható, könnyen sokszorosítható létezőt, amely elsősorban e tulajdonságai miatt élvez fokozott védelmet. Ez igaz mind a digitális úton létrejött és kezelt adatokkal kiemelten foglalkozó szerzői jogi, mind az adatvédelmi és információbiztonsági jogi szabályozásokra.

A fejezetben sikerült bizonyítani, hogy az adat olyan formában is megjelenhet a digitális térben, ami viselkedését tekintve jobban hasonlít a fizikai kiterjedéssel bíró, testi tárgyakra. A virtuális valóságban a tulajdon átruházója, tehát a játékos képessé válik a virtuális tárgy átruházására, amennyiben a szoftver technikai beállításai ezt számára lehetővé teszik.

A virtuális árucikkek jogi helyzetének elemzésével kapcsolatban megállapítottam, hogy azok nem feleltethetőek meg a dolog jogi fogalmának, így dolgokként nem képezhetik tulajdonjog tárgyát, mivel a Ptk. az alatt a fizikai léttel bíró, birtokba vehető testi tárgyat érti. A jogdogmatikai elemzés kapcsán látható, hogy a hatályos jog dolgokra és tulajdonra megalkotott szabályai jelenleg nem alkalmasak arra, hogy a virtuális világokon belül forgalmazott árucikkek feletti rendelkezést ezek mentén rendezzük. A virtuális tárgy a testi tárgy fogalmának nem feleltethető meg, mivel fizikai léttel nem bír. A pénzre és értékpapírra vonatkozó szabályok pedig azért nem alkalmazhatóak, mivel a virtuális tárgyak fizikai léte adott szolgáltatástól nem függetleníthető. Ez a tulajdonságuk pedig azt eredményezi, hogy a velük való rendelkezést a szolgáltatás nyújtója a szolgáltatással (jelen esetben egy szoftver használatával) kapcsolatos végfelhasználói szerződésben korlátozhatja. Mivel azonban a

virtuális tárgyak adásvétel tárgyát képezhetik tulajdonságaik miatt, ezért kitértem az adásvétel általános szabályozására és megvizsgáltam, hogy az mennyire alkalmazható a virtuális árucikkekre. Megállapítottam, hogy ha az adásvételi szerződés a jogok átruházására vonatkozó szabályai alapján próbáljuk meg minősíteni a virtuális tárgyakkal történő tranzakciókat, akkor először is azt kell szem előtt tartanunk, hogy a tranzakciók lehetőségét elsősorban a szoftver technikai beállításai teszik lehetővé a felhasználóknak. Ezt a technikai lehetőséget szabályozza absztrakt szinten a szoftverhez mellékelt végfelhasználói szerződés, amely adott esetben megtilthatja, illetve legitimálhatja a virtuális tárgyak adásvételét valós pénzért cserébe. A végfelhasználó és a fejlesztő között létrejött szerződés tehát rendelkezhet arról, hogy a játékos a használatában lévő virtuális tárgynak a szoftveren belüli használati jogát átruházhatja ellenértékért cserébe egy másik félre. Ez a jogosultság a játékost azonban csak az azt létrehozó szerződés keretei között illeti meg, mivel ez határozza meg, hogy a virtuális tárgy forgalomképessé tehető-e valós pénzben, vagy sem. Ha a virtuális tárgy feletti játékon belüli rendelkezési jogot a végfelhasználó és a fejlesztő közötti szerződés forgalomképessé teszi, akkor a jogok adásvételére vonatkozó szabályok alkalmazásával feloldható a virtuális tárgyakat övező tranzakciós dilemma és a virtuális tulajdon elmélete által feltett kérdések. Ha azonban a szerződés kifejezetten megtiltja a virtuális tárgyak feletti szabad rendelkezés jogát, akkor az ezekkel valós pénzben történő kereskedelemnek nincs jogalapja.

A fejezetben bemutattam továbbá néhány, a gyakorlat szülte megoldást is, így a Diablo III valódi-pénzes aukciós házát, valamint a Second Life-ban kezelt felhasználói tartalmak viselkedését.

Konklúzióként egy hármas csoportosítást állítottam fel a felhasználói tartalom kezelésének szabályaira a virtuális közösségben. A virtuális vagyont így a következő elemek alkotják.

A felhasználók által kezelt tartalmak közül az első csoportba a virtuális környezettől függetleníthető szellemi terméket tettem. Ezek lényeges tulajdonsága, hogy az ilyen egyéni, eredeti alkotások (pl. versek, dalok, színdarabok) azon tulajdonsággal bírnak, hogy függetleníthetőek a szoftver forráskódjától, amellyel, és a környezettől, amiben létrehozták őket. Kapcsolatuk ezért szorosabb azok megalkotójával, mint a közvetítő közeggel.

A második csoportba a virtuális környezettől nem függetleníthető szellemi terméket tettem. A fejezetben sikerült megállapítani, hogy a virtuális közösségeket fenntartó szoftverek olyan funkciókkal is bírhatnak, amiket a játékosok arra használhatnak fel, hogy bizonyos eszközkészletből válogatva létrehozzák saját virtuális tárgyaikat, amelyek adott esetben forgalomképes árucikként jelenhetnek meg a virtuális tárgyak piacán. Erre a jelenségre a

Second Life tervezőkészlete az egyik legjobb példa, amely működését részletesen is bemutattam. Ezeknek a tárgyaknak a megjelenése a felhasználó által létrehozott tartalommá, ún. „user-generated content”-é válik, így egyéni eredeti jellegükre tekintettel később a felhasználók szellemi tulajdonát képezhetik, amelyre a Second Life lehetőséget is ad.

A harmadik csoport a már sokat emlegetett virtuális tárgyak köre, azaz maga az árucikkeké, amelyek legtöbbször képezik tranzakció tárgyát az egyes felhasználók között, akár virtuális, akár valódi pénzben. A virtuális tárgyak sajátossága, hogy dolog módjára viselkednek a virtuális térben, így a felettük létrejövő használat joga adható és vehető a felhasználók között. Fontos következtetés, hogy a virtuális vagyontárgyakhoz tapadó használati jog egyoldalú elvonása, adott esetben akár kártérítési igényt is megalapozhat a virtuális vagyon felett korábban rendelkező felhasználó részéről a szoftverfejlesztő felé.

A virtuális „tárgyak” azon tulajdonságuk alapján képviselnek értéket, hogy legtöbbször munkabizonyítékon alapul a létük. Azokat végső soron virtuális fogyasztási cikknek neveztem el, amelyek a szoftverhez mellékelt végfelhasználói szerződés keretei között vagyoni értékű jogokként kezelhetőek.

4. A mesterséges intelligencia funkciók szerepe a virtuális közösségekben és szoftver működése által okozott károkért való felelősség

Az egyén jogi helyzetét elemző második rész harmadik és egyben utolsó fejezete a mesterséges intelligencia viselkedését elemzi a virtuális világokon belül is, ezért „a kiborgok jogai” alcímet kapta.

A téma kapcsán először is szükség volt arra, hogy meghatározzuk a mesterséges intelligencia fogalmát, mivel azt kifejezett módon a hatályos jogszabályi környezet nem ismeri. Ehhez a filozófia eddigi próbálkozásait hívtam segítségül, amelyek mentén a gyenge és erős MI közötti különbségre sikerült rávilágítani. Megállapítottam, hogy a jelenleg mesterséges intelligenciának nevezett szoftverek a gyenge MI szintjén állnak, azok nem rendelkeznek önálló tudattal és általában egy bizonyos, intelligenciát is igénylő probléma megoldására hozzák létre őket.

A mesterséges intelligencia és a jogi szabályozás gondolatát Isaac Asimov törvényei mentén vázoltam fel, mivel ezek kapcsán merült fel először konkrétan, hogy a „csinált értelem” működését nem csak a technika, hanem egy magasabb szinten, a jog és törvényesség mércéjével is szabályozni kell. Asimov elméletén túl ismertetésre került több kortárs

jogirodalmi álláspont is az MI jogi besorolását illetően, amelyek elsősorban az ilyen funkcionalitással rendelkező szoftverek viselkedéséért való felelősség kérdéseit taglalják.

A mesterséges intelligenciának, mint jogi entitásnak az értékelésére eddig több eltérő álláspont alakult ki a szakirodalomban. Az első szerint a mesterséges intelligencia nem más, mint szoftver, így arra elsősorban a szoftverek jogi helyzetét szabályozó előírások irányadóak. Az MI szoftver fogalmának meghatározására eddig kevés kísérlet született törvényi szinten, erre hoztam példaként az USA New Jersey tagállamában a vezető nélküli autókra vonatkozó szabályokat tartalmazó törvényt, amely ebben a kontextusban egzakt módon meghatározza az MI fogalmát, azonban általános meghatározásnak nem lenne elégséges.

A második elmélet szerint a mesterséges intelligencia nem más, mint egyfajta jogalany, jogi személyiséggel való felruházására azonban nincsen lehetőség a polgári jog rendelkezései alapján, mivel azok sem elkülönült vagyonnal, sem vagyoni érdekekkel nem rendelkeznek. Az intelligens elektronikus ágenseket példaként hozva, azonban annyi mindenképpen megállapítható, hogy azok megbízóik nevében fejtenek ki joghatást kiváltó tevékenységeket közvetlen emberi irányítástól teljesen mentesen (pl. tőzsdei kereskedő szoftverek, áruszortírozó programok stb.). Az MI így önálló döntései révén maga köthet szerződést, vagy tehet más jognyilatkozatot, ami azonban az általa képviselt személyt kötelezi. Ebben az esetben úgy kell tekinteni, hogy az ilyen, az UNCITRAL Modelltörvény által is ismert „automatikus szerződési nyilatkozat” attól a jogi entitástól származik, aki az ágenst üzemelteti. Mivel a magyar jogban az automatikus szerződési nyilatkozatokkal és az ágensi „képviselettel” kapcsolatos pontos felelősségi szabályozás eddig nem került kialakításra, ezért javaslatot tettem a Modelltörvény által meghatározott szabályozás implementálásának lehetőségére.

A következőkben a hatályos jogszabályi környezet elemzése alapján elemeztem, hogy a mesterséges intelligenciával működő szoftverek, amennyiben üzemeltetésük során hibás működések kapcsán kárt okoznak, akkor ki tehető azért felelőssé. A téma kapcsán a szerződéses viszonyokra és szerződésen kívül kárfelelősség lehetőségeire is kitértem.

A szerződéses viszonyok keretei között okozott károkkal kapcsolatban megállapítható, hogy a felhasználó által önmagának, vagy harmadik személynek a szoftver használatával összefüggésben okozott károkért nem a szoftver szerzője (vagy forgalmazója), hanem a felhasználó felel, amelyet általában a szoftverhez mellékelt felhasználói szerződésekben foglaltakkal is igyekeznek megerősíteni a fejlesztők. Ettől meg kell különböztetni azt az esetkört, ha a szoftver hibásan került a piacra és e hibájából eredően álltak be károk a felhasználói oldalon. A Ptk. a hibás teljesítés jogintézményén keresztül enged lehetőséget

arra, hogy a szolgáltatás nyújtóját felelősségre lehessen vonni a szerződés hibás teljesítése, jelen esetben egy hibásan megírt számítógépes program szolgáltatása miatt. Ha a Ptk. fenti rendelkezéseit alkalmazzuk a szoftver forgalmazója és a felhasználó között létrejött jogviszonyra, megállapíthatjuk, hogy a felhasználó a hibásan megírt szoftver használatából bekövetkező károk (tapadó és következménykárok is) megterítését követelheti a hibás szoftver forgalmazójától. Ezen felül fontos kiemelni, hogy a kellékszavatosság előírásai alapján, ha a szerződés nem zárja ki, a hiba kijavítását a szoftver jogszerű felhasználója is elvégezheti, illetve kérheti azt annak fejlesztőjétől (forgalmazójától).

A szerződésen kívül okozott károk tekintetében a veszélyes üzemi felelősség modelljét találtam alkalmazhatónak az MI által okozott károkkal kapcsolatban. Az MI szoftver üzembentartójának fő szabály szerint mindig viselnie kell a felelősséget, azt nem háríthatja át másra. Ez abból ered, hogy a szoftver viselkedése előre nem tervezhető, így üzemeltetése fokozott veszéllyel járó tevékenységnek minősül. Kivétel lehet viszont, ha sikerül bizonyítani, hogy a szoftver működési körén kívüli külső tényezővel van okozati összefüggésben a káresemény bekövetkezése.

Büntetőjogi szempontból kitértem az MI szoftver elkövetői minőségének vizsgálatára, amely kapcsán megállapítottam, hogy arra nincs lehetőség, mivel a Btk. személyi hatálya kizárólag a természetes személyekre terjed ki, és a bűnös tudattartamon keresztüli elkövető szándék vizsgálata is lehetetlen. Továbbá – a korábban kifejtettek értelmében – az MI jogi személyiséggel sem rendelkezik, így a jogi személyekkel kapcsolatos bűnügyi intézkedések sem terjednek ki rá. Ezzel szemben az MI szolgálhat bűncselekmény elkövetési eszközéül, amelyre a virtuális valóságból is hoztam példát.

Végül a mesterséges intelligencia típusú komponensek a virtuális közösségekben történő szerepét vázoltam. Ezek jellemzően a szoftver kisebb részeként, automatikusan futó szkriptekként jelennek meg, amelyek például az ellenfelek mozgásáért, vagy a világ fenntartásának egyéb problémáiért felelősek. A virtuális létformákat két csoportba soroltam, az elsőbe a nem intelligens, a másikba a mesterséges intelligenciával ellátottak tartoznak.

A „fertőzött vér” incidensen keresztül próbáltam meg modellezni azt a tipikus esetet, amikor egy virtuális közösségben az egyes szoftverkomponens szkriptek hibás működése tönkreteszi a játékot és kellemetlenségeket okoz a felhasználóknak. A vázolt ügyben egy virtuális járvány tizedelte a World of Warcraft világában játszó felhasználók karaktereit, amely az egyik ellenfelet irányító MI hibás működéséből eredt. Megállapítottam, hogy a virtuális valóságokban található szkriptelt létformák a viselkedésükre vonatkozó információkat a programot (világot) fenntartó szerverekről nyerik. A központi szervert a

fejlesztőcég tartja fent a játékosok számára. Ebben az esetben tehát a mesterséges intelligencia üzembentartója nem a felhasználó lesz, hanem a szoftverfejlesztő. A probléma összegzéseként elmondható, hogy a virtuális valóság szoftver felhasználója által felhalmozott virtuális vagyon, amely leginkább karakterének és virtuális tárgyainak értékében testesül meg, a kiszolgáló szerverek üzemeltetőinek felróható mulasztás miatt végérvényesen megsemmisülhet. A fejlesztő a hibás teljesítés és a kellékszavatosság korábban ismertetett szabályai alapján kötelezhető arra, hogy kártérítést fizessen a felhasználónak, illetve állítsa helyre az eredeti állapotot (pl. az elveszett virtuális vagyon visszaállításával), amennyiben ez lehetséges.

A megoldási javaslataim a fenti anomáliákra a fejezet záró részében négy pontban foglaltam össze. A konklúzió szerint szükséges lenne az UNCITRAL modelltörvényben olvasható szabályozáshoz hasonló megoldás, amely alapján fő szabály szerint a mesterséges intelligencia viselkedéséért és azzal okozati összefüggésben keletkezett károkért annak üzembentartója felelne.

5. Bűnözés a virtuális közösségekben: az önszabályozás elsődlegessége

A dolgozat harmadik része a „bűnözés a virtuális közösségekben” címet kapta és arra próbál rávilágítani, hogy a virtuális környezetben is elkövethetőek olyan visszaélések, amelyeknek a fizikai világban is megvannak a párjaik. A dolgozat későbbi és megelőző részeiben is szerepelnek az egyes témák kapcsán felmerülő különös büntetőjogi problémákkal foglalkozó elemzések, azonban fontosnak tartottam egy általánosabb megközelítést tartalmazó külön fejezet megírását is a téma kapcsán, mivel ezen keresztül könnyebben mutathatóak be a jelenség által felvetett alapvető problémák is.

A számítógépes bűncselekményeket az elkövetési jellemzőik alapján három főbb csoportba osztottam. Az első a „klasszikus” informatikai bűncselekmények csoportja, amelyek jellemzője, hogy védett jogi tárgya maga a számítástechnikai rendszer és az abban tárolt adatok integritásához, biztonságos működéséhez fűződő általános érdek. Az ilyen számítógépes bűncselekményeket csak számítógéppel lehet elkövetni, ezért új törvényi tényállásokat kellett a jogalkotónak alkotnia azokra nézve. A második a „modern” informatikai bűncselekmények csoportja, melyek elkövetéséhez nem elengedhetetlenül szükséges az informatikai infrastruktúra, mégis – mivel legtöbbször digitalizálható adatokkal történnek a visszaélések –, a digitális technológia fejlődése akarva-akaratlanul is katalizátorként hat a bűnözés eme területeire (pl. gyermekpornográfia, szerzői jogok

megsértése, személyes adattal visszaélés). A harmadik csoportba az értekezés témája szempontjából is elemzendő visszaéléseket, azaz a „virtual crime” jelenségét soroltam, ami a számítógépes szoftverek által szimulált virtuális valóságban történő bűnözést jelenti. A virtuális bűnözés olyan csak számítógéppel elkövethető cselekményeket ölel fel, amelyekre azonban nem kell új tényállásokat alkotni, hiszen egyedül az különbözteti meg a fizikai világban elkövetett bűncselekményektől (pl. egy dolog ellopásától), hogy egy másik, alternatív univerzumban követik el, amitől viszont a megtörténtek nem függetleníthetőek. A virtual crime körébe sorolható számítógépes bűnözés a visszaélések sajátos, egyedi csoportja, és eltérő tendenciákat mutat, mint az első két csoportba tartozó elkövetési magatartások. A virtuális bűnözésen belül is differenciálhatunk személy elleni, vagyon elleni és gazdasági bűncselekmények között.

A személy elleni bűncselekmények jellemzőit egy klasszikus példán, Mr. Bungle esetén keresztül mutattam be. A virtuális nemi erőszak elkövetője egy Mr. Bungle néven játszó játékos volt, aki offenzív, erőszakos üzenetein, tehát játékbeli cselekedetein keresztül „erőszakolta meg” több másik játékos avatarját a játékkörnyezetben. A cselekményt egy virtuális tárgy, egy ún. voodoo baba segítségével követte el, ami alkalmas volt arra, hogy irányítsa vele mások játékbeli viselkedését. Sikerült megállapítani, hogy nem minősülhet a büntetőjog alapján szexuális erőszaknak az ominózus eset, hiszen ez a törvényi tényállás nem valósulhat meg a fizikai világon kívül. Alkalmas volt viszont arra, hogy lelki, pszichés szempontból felzaklassa az „erőszak” elszenvedőit. A példa alapján megállapítható, hogy a virtuális környezetben is elkövethetőek személy elleni bűncselekmények, még ha az közvetlenül csak adott felhasználó avatarja ellen irányul.

A virtuális vagyon elleni bűncselekmények sajátossága, hogy az online közösségekben is előfordulhatnak olyan esetek, amikor a közösség valamelyik tagjának sérülnek a vagyoni érdekei oly módon, hogy azzal kapcsolatban felmerülhet akár a bűncselekmény elkövetésének gyanúja is. A virtuális vagyont károsító bűncselekményeket olyan tárgyak ellen követik el, amik értékkel bírhatnak egy játékos-közösség szemében. Ezek nem mások, mint a virtuális vagyon alkotórészei, amelyet a virtuális „házlopási” példa alapján szemléltettem. Sikerült megállapítani, hogy a virtuális tárgyakért felelős adatok jogosulatlan kezelésével elkövethető a virtuális tárgyak „ellopása”, amely anyagi kárt is okozhat a jogosultnak. Arra a következtetésre jutottam, hogy az ilyen cselekmények a jelenleg hatályos büntetőjogi normák alapján is besorolhatóak, azokra azonban szükségszerűen a Büntető Törvénykönyv által nevesített információs rendszerek útján, illetve ezek ellen elkövetett bűncselekmények törvényi tényállásait lehet alkalmazni.

Egy harmadik sajátos csoportot alkot a virtuális vandalizmus, amely a háromdimenziós kibervilágban a másik fél által használt virtuális tárgyak, emléktárgyak, lakóházak elpusztításában ölthet például testet. A magam részéről a tárgyak jogtalan elpusztítását inkább soroltam a virtuális vagyon elleni visszaélések körébe természetükből adódóan.

Megemlítettem továbbá az úgy nevezett griefinget, amely olyan szándékos cselekedet, amely másokat zavar, az elkövetőjének célja a többi felhasználó idegesítése és a játékélmény csökkentése. A griefer (a griefinget elkövető személy) a játékban rejlő, elvileg szabályos lehetőségeket használja ki mások szórakozásának megzavarására. Ezen felül röviden kitértem a játékosközösségek által felállított belső szabályrendszer (ún. „klánszabályok") megsértésének büntetőjogi relevanciájára, továbbá ismertettem a hatalommal visszaélés lehetőségeit a virtuális valóságon belül. Ezekkel kapcsolatban azt találtam, hogy azok kivételes esetben kelthetik bűncselekmény elkövetésének gyanúját, azonban legtöbbször inkább csak a végfelhasználói szerződés, illetve a játékszabályok megszegésének minősülnek.

Végül az egyes visszaélések elemzése kapcsán részletesen foglalkoztam a virtuális valóság terrorista használatával. Egyes szerzők szerint az olyan lehetőségek, mint az anonimitás, a globális hozzáférés lehetősége és a hagyományos tranzakciós felületek kiterjesztése vonzóvá tehetik az ilyen szoftverek használatát a felhasználók számára, a másik oldalról nézve viszont nemzetközi fenyegetések támogatását is kiszolgálhatják. Az USA Nemzetbiztonsági Ügynökségének (NSA) elemzését felhasználva, az általuk illusztrált példákon keresztül igyekeztem bemutatni, hogy milyen módokon lehet a virtuális valóságot terrorizmus céljaira felhasználni. Konklúzióként azt vontam le, hogy az online játékok terroristák általi használatától az NSA elemzésében foglaltakhoz képest nem feltétlenül kell tartani, és ezt nem csak az a tény támasztja alá, hogy eddig egyetlen egy ilyen esetre sem derült fény, hanem, hogy ezen szervezetek céljaival sokkal jobban összeegyeztethető az anonim, titkosított csatornákon keresztüli kommunikáció.

A virtuális bűnözéssel kapcsolatban összegzésképpen megállapítható, hogy a virtuális közösségek önszabályozási mechanizmusai, illetve belső moderálása az esetek döntő többségében elégségesnek bizonyulnak, és csak legvégső esetben van szükség külső, hatósági beavatkozásra, így ezen a területen is maradéktalanul érvényesülni látszik a büntetőjog ultima ratio jellege. A visszaélések elkerülése és a hatékony fellépés érdekében pedig a hatóságok nemzeti és nemzetközi együttműködése, továbbá képzése kell, hogy a jövőben megvalósuljon.

6. A centralizált virtuális fizetési rendszerek és azokkal kapcsolatos főbb megállapítások

A dolgozatom negyedik és egyben utolsó különálló logikai része „a virtuális gazdaság fizetési rendszerei” címet kapta. Ebben a fejezetben a pénzpiaci és ehhez kötődő gazdasági működés jogi szempontjaiból elemeztem a különböző virtuális kereskedelmi platformok működését.

Az első fejezet a centralizált virtuális gazdasági rendszerrel foglalkozik, amelynek különös ismérve, hogy létezik benne egyfajta központi kontroll, amely végső soron irányítja és kontrollálja annak működését. A fejezet a pénz és a virtuális pénz kialakulásának rövid történetével kezdődik, amely megalapozza fogalmilag, hogy mit tekinthetünk virtuális fizetőeszköznek. Ezek alapján megállapítottam, hogy a virtuális fizetőeszközök csereeszközként és elszámolási egységként viselkednek meghatározott virtuális közösségben. Az Európai Központi Bank hivatkozott tanulmánya szerint a virtuális fizetőeszköz egy jogi értelemben nem szabályozott, digitális pénznem, amit alapvetően annak fejlesztői bocsátanak ki, irányítanak és egy meghatározott virtuális közösség tagjai fogadják el és használják, használatának jogi kereteit az azt kezelő szoftverhez mellékelt végfelhasználói szerződés tartalmazza.

A virtuális pénzügyi rendszereket három kategóriába soroltam, a szerint, hogy más valutákra átválthatóak és valódi tárgyak vásárlásának lehetősége adott-e. A zárt virtuális pénzügyi rendszerben maga a szoftver és ahhoz kapcsolódó hivatalos szolgáltatások nem teszik lehetővé a virtuális pénz valódi valutára történő átváltást és az abban való kereskedést. A félig nyitott virtuális pénzügyi rendszerben a virtuális valutát valódi pénzért lehet meghatározott árfolyamon vásárolni a fejlesztő által támogatott platformon keresztül, azonban a visszaváltási lehetőséget az már hivatalosan nem támogatja. A teljesen nyitott rendszerben az átváltási lehetőség már oda-vissza működik a szoftver részeként.

Az elektronikus pénz és a virtuális pénz viszonyát abból a szempontból elemeztem a továbbiakban, hogy az általános jogi szabályozottság hiányát emeltem ki. Amíg elektronikus pénzzel kapcsolatban mind nemzeti, mind Európai Uniós szinten létezik szabályozás, addig ez a virtuális fizetőeszközökről nem mondható el. A vonatkozó EU irányelv és a Hpt. meghatározása szerint az elektronikus pénzt annak kibocsátója pénzeszköz átvétele ellenében bocsátja ki. Ez a virtuális pénzre csak részben igaz, hiszen arra nem csak valódi pénz átváltása (átvétele), hanem virtuális tevékenység (pl. küldetések teljesítése utáni jutalom, bányászat stb.) kifejtése kapcsán is szert lehet tenni. Szintén szembetűnő különbség, hogy az

elektronikus pénzt annak kibocsátóján kívül harmadik félnek is el kell fogadnia fizetési műveletek teljesítése céljából. Ez a virtuális pénzre egyáltalán nem igaz, mivel azzal kizárólag az azt használó virtuális világon belül lehet fizetni. A virtuális pénzek továbbá teljesen más elszámolási egységeket használnak, így azok úgy viselkednek, mint egy teljesen különálló valutanem és nem úgy, mint egy már létezőnek a puszta elektronikus megfelelője.

A fentiek alapján a Second Life centralizált gazdaságát mutattam be példaként. A Second Life önellátó gazdasággal rendelkezik, ami annyit jelent, hogy az teljesen zártan működik, aminek nincs kapcsolata közvetlenül a külvilággal. A gazdaság kizárólag virtuális tárgyakra és szolgáltatásokra koncentrál, továbbá teljes mértékben a Linden Lab által fejlesztett infrastruktúrát használja, ennek keretei között működik. A fenti alapvető különbségeken kívül a virtuális világ gazdasága hasonló elvek mentén működik, mint a fizikai világbeli párja. A fenti tulajdonságok miatt a Second Life-beli gazdaság teljesítőképessége mérhető.

A centralizált virtuális gazdaságok egyik fő problémája abban ragadható meg, hogy azokban az egyetlen szabályozó autoritás a szoftverfejlesztő. A felhasználókat érintő jogok szempontjából megállapítható, hogy azok egyoldalúan a fejlesztőcég felelőtlenségére és a felhasználó felelősségére vannak általában kialakítva, amelyet az általános szerződési feltételek egyoldalú megállapítása tesz lehetővé számukra.

Fontos azonban azt is kiemelni, hogy a felhasználók részéről a visszásságok orvoslása érdekében a fejlesztők mindig biztosítják a panaszjogot és a felhasználók által elkövetett visszaélések esetén, így például a játékszabályok megsértésekor igyekeznek visszaállítani az eredeti állapotot.

7. A decentralizált virtuális fizetési rendszereket érintő főbb megállapítások és a virtuális tulajdon fogalmának kiterjesztése

A negyedik rész második fejezete – amely egyben a dolgozat utolsó különálló nagyobb egysége – a decentralizált virtuális fizetési rendszerek sajátosságait hivatott elemezni, azok közül is kiemelkedően foglalkozik a Bitcoinnal és kisebb mértékben az annak alternatívájára létrehozott más kriptovalutákkal.

A decentralizált modellben semmilyen felsőbb szintű kontroll nem létezik, az előre lefektetett technikai szabályrendszeren túl a felhasználók és a virtuális pénz (árucikk) maga a meghatározó tényezők.

A továbbiakban a decentralizált rendszert a Bitcoin protokollon keresztül mutattam be, amely egy újfajta független fizetőeszköz, amely a Satoshi Nakamoto álnevű teremtőjének

2008 őszén megjelent tanulmányában lefektetett szabályrendszeren alapul. A fizetőeszköz csak digitális formában létezik, fizikai megtestesülésével, érmeként vagy bankjegyként sehol sem találkozhatunk vele.

A Bitcoin elődeiről szóló rövid összefoglalóban ismertettem, hogy milyen logikai megoldások mentén lett végül létrehozva a gyakorlatban a Bitcoint kezelő rendszer. A Bitcoin érméket kezelő szoftver egyfajta virtuális pénztárcaként funkcionál az egyes felhasználók számítógépein. A pénztárca egy fájl a számítógépen, amit „*wallet.dat*” néven találhatunk meg. A Bitcoin küldésére és fogadására alkalmas címeket a program felhasználói kérésre automatikusan generálja. Mindegyik Bitcoin-cím két részből áll. Az egyik része az úgy nevezett „*nyilvános kulcs*”, a másik pedig a „*privát kulcs*”. A nyilvános kulcs látható, és ezt kell megadniuk a felhasználóknak egymásnak az utalások kivitelezéséhez. A privát kulccsal pedig – amely viszont rejtve marad a másik fél előtt – a szoftver aláírja a kérdéses tranzakciót. A nyilvános kulcsokat és hozzájuk tartozó privát kulcspárokat a már említett wallet.dat nevű fájlban tárolja a program a számítógép merevlemezén.

A Bitcoin hálózat a rajta keresztül létrejövő tranzakciókat az egész hálózaton szétküldi, így azok teljesen nyilvánosak. Szemben a hagyományos pénzügyi intézetekkel, amelyek az ügyfelek személyes adatait és magánszféráját a tranzakciókra vonatkozó információk visszatartásával védik, ezt a Bitcoin rendszerében az biztosítja, hogy a címek és az azokon keresztülfolyó tranzakciók tulajdonosaira vonatkozó személyi azonosításra alkalmas információk egyáltalán nem ismertek. A tranzakciók technikai működését egy egyszerű példán keresztül is igyekeztem szemléltetni a könnyebb átláthatóság érdekében.

A Bitcoin rendszer decentralizált szisztémájának sajátossága, hogy nincs benne olyan központi adatbázis, szerver vagy bármilyen egyéb hatóság, ami a tranzakciók független ellenőrzését végzi. Technikailag a rendszer a tranzakciók biztonságát és a csalás lehetőségét ezért úgy iktatja ki, hogy a világon forgalomban lévő összes Bitcoinnal végzett valamennyi utalás naplózódik a virtuális érméket tartalmazó, úgy nevezett blokkokban. A szokásos banki modellektől eltérően nem a tranzakciók titkosak és a számlatulajdonosok ismertek, hanem éppen fordítva. A Bitcoin-kliens a beüzemelése után minden egyes felhasználónak letölti az összes blokkot a számítógépe merevlemezére, később pedig hozzá mindig a legújabbakat. Az összes tranzakció teljes adatbázisa megtalálható minden egyes ember számítógépén, aki Bitcoint használ és az a nyílt hálózaton keresztül folyamatosan frissül. Ahhoz, hogy egy utalás teljesülhessen legalább hat másik hálózatra kapcsolódott számítógépnek kell igazolnia a tranzakciót. A virtuális pénztárcában lévő kulcspárokat a szoftver összeveti a blokkokban

tárolt tranzakciós információkkal és ez alapján számolja ki, hogy mennyi Bitcoin felett rendelkezhet az adott felhasználó.

Az érméket tároló egyes blokkok a Bitcoin-hálózat csomópontjain generálódnak, amikor a rendszer megoldást talál egy kriptográfiai algoritmusra. A Bitcoinok ilyen úton történő előállításához le kell tölteni egy szoftvert, amely az után a felhasználó számítógépe számítókapacitását használja az ilyen matematikai problémák megoldásához eszközül. Ezeket a programokat „*bányász-szoftvernek*" („mining-software") nevezzük. Ha sikerült megoldatni a számítógéppel a Bitcoin-hálózaton egy algoritmust, létrejön egy úgy nevezett blokk, amelyekben a virtuális érmék tárolódnak és ezen kívül tartalmazza a velük végzett tranzakciós adatokat is. Ez az úgy nevezett munkabizonyítékokra támaszkodó rendszer lényege, amit a Bitcoinnal kapcsolatban „proof-of-work" koncepciónak nevezünk. A Bitcoinok azonban nem hozhatók létre végtelen mennyiségben, hanem számuk az idő előrehaladásával exponenciálisan csökken, amíg az eléri a közel 21 millió érmét. Ezek után számuk statikus marad és nem hozható létre belőlük több darab.

A Bitcoin mindenkori árfolyamát – a központi szabályozó szerv hiánya miatt – tisztán a kereslet és kínálat viszonya határozza meg, így jellemző a gyors és drasztikus árfolyamingadozás, amelyre több példa is volt a virtuális elszámolási egység eddigi rövid történetében, amelyeket bemutattam.

A következőkben összehasonlítottam a Bitcoin viselkedését a fizetési lehetőségek hagyományos módozataival, így az online fizetéssel, a virtuális valutákkal és az államok hivatalos (offline) fizetőeszközeivel. Megállapítottam, hogy a rendszer előnyei egyben a hátrányaiként is felfoghatóak, így az anonimitás és decentralizáltság veszélyei taszító hatással vannak a decentralizált pénz nagyobb arányú elterjedésére. Azt is kiemeltem viszont az iraki svájci dinár példáján keresztül, hogy akár hosszabb távon is fent tud maradni egy olyan fizetőeszköz, amely mögött nem állnak garanciák, ha a piac, mint fizetőeszközt elfogadja azt és megbízik benne.

A Bitcoin jogi státuszának besorolásával kapcsolatban többoldalú megközelítést és kizárásos módszert alkalmaztam. Elemeztem a hatályos jogszabályi környezet alapján, hogy a decentralizált fizetőeszközök minek feleltethetőek meg, és azt találtam, hogy az sajátos tulajdonságai alapján sem pénznek, vagy értékpapírnak, sem vagyoni értékű jognak, vagy szellemi terméknek nem tekinthető. Tulajdonságai miatt leginkább egyfajta sajátos digitális árucikkhez hasonlatos, amely a nemesfémekhez hasonlóan csak szűkös számban és előre meghatározott mennyiségben áll rendelkezésre és emiatt értéke is valószínűleg nőni fog. Ezt alátámasztja az is, hogy a legújabb piaci tapasztalatok alapján a Bitcoinra a felhasználók

egyfajta kincsképző és befektetési eszközként tekintenek. A fentieken túl azt is megállapítottam, hogy adott Bitcoin mennyiség feletti rendelkezési jogosultsága a felhasználónak vagyoni értékű jognak tekinthető a konkrét szerződéses viszonyokban (ha például Bitcoinnal fizetnek egy termékért, vagy szolgáltatásért).

A továbbiakban áttekintettem az egyes államok eddigi jogi reakcióit a Bitcoin jelenséggel kapcsolatban és összesen három kategóriába osztottam azokat. Az elsőbe az olyan országok tartoznak, amelyek elfogadják a használatát. Közös bennük azonban, hogy szinte egytől egyig felhívják a piac figyelmét a kockázati tényezőkre és valamilyen szabályozás létrehozását sürgetik. A legtöbb ilyen országban a Bitcoinból származó nyereségét adóköteles jövedelemnek tekintik. A kriptovaluta jogi besorolása kétes és elmondható, hogy vonakodnak állást foglalni azzal kapcsolatban az egyes államok, habár abban általában egyet értenek, hogy klasszikus értelemben vett pénzként nem kezelhető a Bitcoin. A piaci viszonyokat és realitásokat figyelembe véve a digitális árucikként történő meghatározás áll talán a legközelebb a valósághoz, amely a felhasználók vagyonának része.

A második csoportba olyan országokat soroltam, amelyek korlátozzák a Bitcoin használatát. A szabályozás általában azon a szinten áll meg, hogy a Bitcoinnal történő üzletelésre apelláló pénzügyi szervezetek működését korlátozza, vagy tiltja adott állam, azonban a magánhasználatot engedélyezi.

A harmadik csoportba azon kevés országok tartoznak, amelyek teljesen betiltották a kriptovaluták használatát. A szabályozásokról elmondható, hogy azok mögött általában a nemzeti pénzpiac rendkívül szigorúan értelmezett védelme, vagy a bűnmegelőzési célzat húzódik meg.

A fejezet következő pontjában a Bitcoint a bűnözésben betöltött szerepe alapján vizsgáltam büntetőjogi és kriminológiai szempontból, a megállapítások azonban kiterjeszthetőek valamennyi decentralizált elszámolási rendszerre azok hasonló működési elvei miatt.

A központi kontroll hiányának tagadhatatlan előnyei (gyorsaság, anonimitás, egységes elszámolás stb.) mellett bőven olyan tulajdonságokkal is bír a virtuális tranzakciós rendszer, amely inkább a feketepiaci használatnak kedvez. Habár a decentralizált fizetőeszközöket használó bűnözők utáni nyomozás elsőre lehetetlennek tűnhet, a rendszer kiindulásképpen ad némi kapaszkodót is. Ilyen például a Bitcoinnal végzett tranzakciók nyilvánossága, amely alapján a blokkláncban visszakövethető a gyanús utalások útja. Az egyes címek valódi tulajdonosai utáni kutatás céljából pedig kiemeltem a Bitcoin váltó honlapok adatkezelését és azok megkeresésének lehetőségét, hiszen ezek az egyes címekkel kapcsolatban már kellő

személyes adattal rendelkeznek (pl. regisztrációs név, e-mail cím, belépési IP címek, bankszámlaszám) egy bizonyos személy beazonosításához.

A Bitcoint két jellemző bűncselekmény, a pénzmosás és a lopás szempontjából részletesen is elemeztem a jobb megértés érdekében. A pénzek Bitcoinra történő átváltásával, majd annak különböző Bitcoin-címekre való továbbutalgatásával elvileg könnyen megvalósítható a bűncselekmények elkövetéséből származó pénzösszegek tisztására mosása. Kiemeltem azt is, hogy az interneten találhatóak továbbá olyan speciális honlapok, amelyek nem titkoltan Bitcoin-mosásra szakosodnak, az egyes felhasználók anonimitásának megőrzése érdekében. Ezzel kapcsolatban javaslatot tettem arra, hogy a nyomozáshoz szükséges adatok könnyebb beszerzése érdekében célszerű lenne az egyes Bitcoin-tőzsdék részéről egy online megkereső felület biztosítása az egyes bűnüldöző szervek részére, mint ahogy arra a közösségi oldalak és aukciós portálok (pl. a Facebook, eBay) részéről léteznek már jó példák.

A pénzmosás mellett Bitcoinok ellopásáról már jó néhány esetet dokumentáltak is. Az ilyen visszaélések szempontjából a legfontosabb tényező a számítógépen található pénztárca fájl (wallet.dat), ami tartalmazza, hogy épp mennyi virtuális érme felett rendelkezhet adott felhasználó. Kiemeltem, hogy a Bitcoin kétes, vagy inkább nem létező jogi besorolása miatt sok esetben nem egyértelmű, hogy a virtuális vagyontárggyal történő különböző visszaélésekre a Büntető Törvénykönyv melyik különös törvényi tényállását kellene alkalmazni a helyes minősítés érdekében. A kifejtett véleményem szerint, mivel a számítógépes környezet elengedhetetlenül szükséges a Bitcoinnal való bűncselekmények elkövetésére, így – noha az tulajdonságait tekintve inkább árucikként viselkedik, mint adatként – indokolt a virtuális pénzlopásokat számítógépes bűncselekményként (tehát a Btk. 375. §, 423. § vagy a Btk. 424. §-aiba ütköző magatartásokként) értékelni, nem pedig lopásként. A fenti érvelés több, a gyakorlatban is megvalósult példával támasztottam alá.

A továbbiakban kitértem arra, hogy a Bitcoint olyan tevékenységek kivitelezéséhez is előszeretettel használhatják, mint az illegális termékek (pl. fegyver, kábítószer) adásvétele. Végül elemeztem és megcáfoltam azt a közkeletű teóriát, amely szerint a Bitcoin-rendszer nem más, mint egy világméretű piramisjáték, hiszen a profitálás azoktól eltérően nem abból ered, hogy a korai belépők a rendszer népszerűsítése útján történő kiszélesítésével és új tagok beléptetésével minél több pénzt szedjenek be a későbbi tagoktól. A korai Bitcoin tulajdonosok a virtuális valuta árfolyamának növekedéséből tettek szert nyereségre.

A fejezet utolsó pontjában ismertettem több más kriptovalutát is, amelyek a Bitcoin megjelenése óta törtek fel a piacon és logikailag sokban hasonlítanak az úttörő találmányra.

Kiemeltem a decentralizált domain név rendszerként működő Namecoint, a második legnagyobb piaci részesedéssel bíró Litecoint, a rendszerbe beépített inflációt adó Peercoint, a decentralizált árupiacként is működő Ripplet és az egyes kriptovaluták közötti átválthatóság kérdésével kísérletező Mastercoint.

Összefoglalásképpen elmondható, hogy fel kell ismerni azt, hogy léteznek olyan adathalmazok, amelyek nem a klasszikus értelemben vett adatként, hanem „dolog" módjára viselkednek a virtuális térben és a fizikailag létező testi tárgyakhoz hasonló tulajdonságokkal bírnak, azzal a különbséggel, hogy csak digitálisan léteznek. Ebből a szempontból a konkrét szabályozás hiánya sok bizonytalanságot szül, így a szakmai vita elkezdése az ügyben már nem várathat sokat magára.

Véleményem szerint, figyelemmel annak tulajdonságaira, és a piac működésére a Bitcoin egy újfajta digitális terméknek, árucikknek tekinthető, ami hasonlatossá teszi azt az olyan virtuális tárgyakhoz, amelyek felett használati jog szerezhető.

A virtuális tárgy és a kriptovaluta között azonban az a különbség, hogy az nem egy szerződéses, vagy más törvény által szabályozott jogviszony alapján jön létre, hanem azon kívül termelhető, állítható elő. Egy adott érmemennyiség feletti rendelkezés jogát az a felhasználó szerzi meg, aki azt kibányászta, illetve akinek azt továbbutalták. Egy konkrét Bitcoinnal kapcsolatos későbbi szerződéses viszonyban így az érmemennyiség feletti rendelkezés joga már vagyoni értékű jogként jelenik meg. A rendelkezési jogosultság értékét pedig elsősorban a kriptovaluta árfolyama és a felek által kialkudott ár határozza meg.

Az ideális megoldás az új technológiával kapcsolatban véleményem szerint mindenképpen egy önálló, európai szintű szabályozás megalkotása lenne, amely önálló jogi léttel ruházná fel a kriptovalutákat és azokat virtuális vagyontárgyként kezelné, valamint pontosan meghatározná, hogy milyen kritériumoknak kell megfelelni egy Bitcoin alapú, illetve ezt is használó vállalkozás létrehozásához.

Summary of the doctoral research

I would like to summarize the results of my thesis briefly by presenting the main statements, criticism and suggestions of the particular parts and chapters as follows.

1. Opening thoughts: Theoretical and historical background of the thesis and main questions to answer

In the first part of the doctoral thesis the concept of virtual reality and the possibilities of its interpretation were presented. Virtual reality can be described as an interactive medium interpreted into emerging technology that makes possible for human personality to get engaged in an alternative reality. This engagement is so intense that after a certain point the concerned persons tend to tear themselves apart from their physical selves and build up new self-concepts.

The first level of virtual communities is real time communication on online channels such as chat-rooms, forums or videoconference software. By actively using this online services personality starts to exit of its physical boundaries. I marked as second level of virtual communities life simulators and online games because the personality of the user takes shape in an interactive avatar controlled by him or her. Users can be part of a simulation that goes onward even when the participants log out. The third level of virtual communities is the possible passage between virtual worlds. Such developments indicate the reason for existence of this level as joint settlement systems of different interactive simulations (e.g.: Facebook-gamecard) or common arenas and markets of players.

I briefly presented the development history of online virtual communities in particular by describing the features of subgenres. Furthermore I introduced the concept, technical background and interactive virtual economies of online role-playing games because it is crucial to understand the concrete problems being drawn up later. Transactions in virtual economies represent a value which can be expressed in real-world money and trading virtual items can be considered as an everyday phenomenon among users.

These statements raised the main questions of the thesis: what regulation can be applied to virtual items in commercial relations? Should be the virtual economy separated from copyright norms concerned? Can ownership consist on purely virtually existing goods that cannot be interpreted as asset according to civil law but are more than valuable data due to

their behavior in virtual space? What effects can the operation of the software have on virtual worlds and simulated economy? What type of virtual markets and goods exist? Can virtual items be the object of crime committed in virtual realities?

Finally the first part closes with a loosely connecting reasoning to the central topic about the relationship of art and computer games which is rather artistic than legal train of thought. Its role is to ground from a special point of view the second part of the thesis examining copyright issues and justifies that the problem of virtual property should be examined from this side of law at first.

In the beginning of the thesis I appointed Hungarian law and jurisdiction as the primal legal ground and framework for the problems presented in later parts of the dissertation.

2. About the legal status of virtual world creators

The second part of the thesis analyzes one of the presented main problems: the legal status of individuals in virtual worlds.

The first chapter is titled “the rights of creators” because it presents the status of virtual world creators in particular describing copyright issues as the main source of problematic legal situations.

According to copyrights norms in force I ascertained that virtual world simulation software are typically artworks created by more authors, and the developer (usually a company) practices the author’s rights in connection with them. Authors usually specify in contracts attached to the software and called general terms and conditions or license agreements that what rules shall users comply with when running the software. The software could be used only after accepting these contractual terms. When the user breaks the rules laid down in the agreements it is considered as a breach of contract.

Further I described the norms which are regulating the behavior of users in virtual worlds especially the so called codes of conduct. Violation of these codes can infer special sanctions on players (e.g.: warning, periodic or permanent ban from the game). Beside general regulations I described the features of clan rules. Clan rules are the inner, closed behavioral norms of a certain group of players who are playing together to advance in the game content. The breaching of clan rules do not imply general retaliation regarding software use but only sanctioned by the closed group of users in which the player is a member too. After presenting the abstract norms regarding the status of users in virtual societies I pointed out that the

technical environment – the programming of the software itself – has huge impact on the possibilities of the user's behavior too.

I introduced the role of license agreements in the everyday life of virtual societies through a legal case in which one of the federal courts of the USA stated that using an automated robot software to control the avatar and consume this way faster virtual resources than normal in World of Warcraft breaches the general terms of the contract attached to the software.

After introducing the abovementioned phenomenon I proceeded to one of the most crucial problems in connection with copyright issues of developing companies: the illicit imitation of virtual worlds and economies via private servers. Private servers are being created by using special emulator software which are built upon the decryption of the original source code that is subject to authorization according the Hungarian copyright law. Such claims of the copyright holders that want to shut down virtual world private servers seem to be well established. According to copyright law, operating such service without authorization breaches copyright of the authors.

Among the motivations for maintaining private servers I mentioned the purpose for independent home programming and software development, experimentation and developing modified virtual environments based on the taste of the user. I also determined that a private server could become such a business that can make serious illegal profit for their developers. In many cases not only the imitation of the virtual world server but the imitation of other internet based services happen too (e.g.: the website) as an alternative option to the official versions.

I analyzed the problem of criminal liability in connection with private server operation too. According to this problem it was appointed that calibrating the amount of financial loss is based on how the software is legally accessible and should the users pay monthly fee or one time registration fee. It is also important to mention that not the players but only the operators of the private server may commit criminal offense because their actions (illegal decryption and use of the source code) harm copyright and in connection with these actions occurs financial loss at the side of the original copyright holder.

It was also ascertained that programming, handing over or disseminating the emulator software usable to create a private server can make a suspicion of committing crime only when the decryption of the source code was done by compromising or defrauding the integrity of technical measures for the protection of copyright. If the original virtual world software does not contain such protection mechanism than only the act of creating an emulator does not make ground for criminal liability.

3. The legal status of participants in virtual worlds: the concept of work-proof based virtual commodity and right of disposal on them

The second chapter of the second part of my thesis is titled “rights of people” because it seeks the answers for issues regarding users of virtual worlds and expounds the theory of virtual property which is one of the main areas examined by the dissertation and gives its core and most crucial question.

I tried to illustrate using simple examples from the everyday life of virtual economies that how users can acquire virtual items (crafting, raiding, winning etc.). It has been also described that the value of virtual items can be expressed also in real world money in every virtual society where such items exist. Virtual items generally represent a value which is specified by supply and demand of users.

The problem of who should have the right of disposal on virtual items comes to surface when somehow ‘real world element’ gets involved in the virtual world. This element is most often real world money (the official currency of a country) on which virtual items are bought and sold. The software developer company in most cases is not interested to intervene into the created virtual economy until commerce stays inside virtual frames. In almost every virtual world such virtual items exist that are representing bigger prestige value and players tend to give out huge amounts of money in real world currencies to obtain these items. It is also important to mention that not just rare but more frequent items or even avatars can be purchased on websites specialized for these kind of transactions and even users tend to offer their own virtual items on popular online auction webpages like eBay.

In the following points of the chapter it has been proven successfully that the standpoint is not rational which says that users cannot practice their right of disposal on their virtual items in outer transactions because such an item cannot be made independent from the source code of the software.

The most important viewpoint regarding ‘ownership’ on virtual items is that they behave not as data but as physical items (‘things’) in virtual space. A theory shared primarily by American authors called virtual property concept points out that in most cases virtual goods cannot be copied, multiplied or shared but only handed over in a physical sense. By handing over the virtual item it is being transferred from one user’s disposal to an other’s. In this sense we should separate from each other the legal fate of the software-component responsible for the appearance of the virtual item and the copy of the concerned virtual item itself which participates in the market processes. The source code responsible for the appearance of the

virtual item is part of the intellectual property of the virtual world software developer but – according to the virtual property theory – the item itself used by users in in-game transactions is not. The virtual item is part of software but having regard to the fact the its 'physical' existence cannot be separated from the service offered to end-users, it represents an independent value.

The software's source code responsible for the appearance and the attributions of the virtual item should be handled as the integral part of the developer's intellectual property but one of the item's independent virtual copy should not be treated as part of it. In virtual space such data could exist that cannot correlate the classic legal concepts about the management of digitalized data. This statement can be also true to copyright, data protection and information security norms which are dealing exclusively with the problem of managing digitalized data.

In this chapter it was successfully proven that data can be present in such form in virtual space which behavior is more akin to physically existing items than multipliable data. In virtual reality the user of the virtual item is capable to assign the right of usage of the virtual asset to another user if the technical background of the software allows it.

Furthermore I came to the conclusion by analyzing the legal status of virtual items that they cannot be treated as physical things (assets) according to the doctrines of Hungarian civil law so their usage does not originate from the legal regulation about ownership on physically existing assets. According to my legal analysis it can be seen that regulations about ownership on assets cannot be applied to virtual items so we cannot arrange the problem of virtual property using these doctrines in force. Virtual item cannot be treated as physical asset according to civil law because it does not exist in physical reality only in virtual reality. Rules for money, securities and forces of nature (e.g.: electricity) cannot be applied to virtual items as well because the existence of the item cannot be made independent from the provided online service. This attribution of them gives the result that the service provider (in these case the developer of the software) can restrict the right to provision on the virtual items in the EULAs. Regarding the fact that virtual items can form the object of trade due to their inner virtue and special attributions I introduced the general rules of purchasing contract and examined the possibility to apply these rules to virtual items. I concluded that if we would like to apply the regulation for purchasing intangible assets (according Hungarian civil law: 'rights') than we should bear in mind at first that the possibility of virtual transactions is based on the technical settings of the software primarily. This technical possibility is regulated on abstract level by the provision of the EULA that can prohibit or allow the purchasing of virtual items on real world currencies. The contract between the end-user and the developer of

the software can assess that right of usage on a player's virtual items can be assigned to other users for consideration (quid pro quo). The users enjoy this right only in the frame of the EULA contract that creates the legal possibility that virtual items can be negotiable or not. If the contract between the end-user and the developer creates the possibility to have negotiable rights on goods in the virtual world than the dilemma surrounding virtual property and virtual transactions can be solved according to the rules of civil law regarding the purchase of intangible assets. If the EULA expressly prohibits the free disposal of virtual items for users than their commercial transactions in real world currencies does not have legal ground anymore.

I introduced in the chapter some practical solutions for virtual property in particular the real money auction house of Diablo III and the issues about user generated content in Second Life.

As conclusion I presented a triple classification for management rules of user-related contents in virtual communities. According to this, virtual property consists of the following elements:

The first group of user related content consists of intellectual products which can be separated from the virtual environment. Their essential attribution is that some individual original creative works (e.g. poems, songs, plays) can be separated from the environment in which they were created. Therefore their relationship is stronger with their creator than the transferring medium.

I put to the second group intellectual products which cannot be separated from virtual environments. In the chapter it was described earlier that virtual world simulators can have such functions that players can use to create their own virtual items which can appear on virtual market as negotiable assets. The best example for this is the designer kit of Second Life. These items' appearance becomes user generated content, so having respect to their original creative nature they can become the intellectual property of the users. This possibility is already the part of Second Life and its EULA.

The third group consists of virtual items. These assets form in most cases the object of transaction in virtual- or real world money. The specialty of virtual items is that they behave as physically existing assets in virtual space, so they can be bought and sold as assets between users. An important conclusion is that arbitrary deprivation of the right of disposal on virtual items in certain situations can result in compensation claim from the user against the software developer.

Virtual items can represent value due to their nature and because their existence is mostly based on proof-of-work. I named them finally virtual commodities (consumer goods) and the

right of usage on them can be treated as intangible asset having regard to the terms and conditions of the software's EULA.

4. Role of artificial intelligence functions in virtual communities and liability for damages caused by the software

The third and last chapter of the second part examining the rights of individuals is intended to present the behavior of artificial intelligence entities in virtual worlds so it was titled "rights of cyborgs".

First of all it was necessary to define the concept of artificial intelligence because it is not exactly defined in the current legal environment. I invoked the attempts of philosophy and distinguished between the concept of week and strong AI. It can be also concluded that today's artificial intelligence driven software are on the level of week AI: they cannot bear own consciousness and are created to solve problems require some level of intelligence.

I draw up the concept of legal regulation of artificial intelligence using the three fundamental laws of robotics by Isaac Asimov because this was the fist attempt to raise the question that 'created intellect' should be regulated not just on technical but on a higher level: by law and legal norms. Beside Asimov's theory I also introduced several contemporary standpoints about the problem from legal science which analyze the legal liability for the behavior of software with artificial intelligence functionalities.

There are some standpoints about the concept of artificial intelligence as legal entity in the scientific literature. According to the first concept, artificial intelligence entities should be treated legally as software, so already existing rules for computer programs must be applied to them. There are very few attempts to define artificial intelligence on statutory level as far. The State of New Jersey legislature for autonomous driven cars is a good example for this. This act exactly writes down the legal definition of artificial intelligence, though in my opinion it is not general enough to be used as a unified general definition.

According to the second concept, artificial intelligence should be treated as some kind of legal entity. I came to the conclusion that it is impossible to treat artificial intelligence as legal person in the context of civil law because AI entities do not have separated property or property interests. If we look at the example of intelligent electronic agents at least it can be concluded that these kind of digital entities can make legally binding actions in the name of their principals without human control or guidance (e.g. stock exchange dealer agent software, product assorting programs). AI can make contracts or other legally binding agreements

guided by their own ‘decisions’ but it obliges the legal entity operating the software. In this case it should be deemed that the ‘automatic contracting declaration’ stems from that legal entity which operates the AI agent. This theory is the concept of UNCITRAL Model Law for Electronic Commerce too. I made a suggestion for the implementation of the Model Law’s definition into Hungarian law because no exact liability system has been developed so far for representation by electronic agents.

It can be concluded about damages caused in the frame of contractual relations that damage caused by users to themselves or third party is not the liability of the AI software developer but the operator (the user) itself. These circumstances are written down in most contractual terms attached to the software product too. That is not the case when the AI appears on the market as a faulty software product containing programming mistakes and it causes damage due to these mistakes of the developer. The Hungarian Civil Code allows through the legal instrument of defective performance to challenge the service provider regarding the defective performance of the contract, in our case for the supplement of a defectively operating computer software. If we apply the aforementioned instruments of the Civil Code for the relationship between the user and the developer of the software than it can be seen that users can have a valid claim against the developer to refund their damages caused by malfunctioning AI software. It is also important to highlight that according to the rules of warranty (if the contract does not exclude it) the user could also perform the necessary corrections of the software or could ask for it by the developer.

I found applicable to AI-caused damages in non-contractual relations the concept of liability for damages originating from hazardous operations. The operator of the AI software shall be liable for any damage caused thereby and cannot devolve it to others, because the behavior of AI cannot be planned as by ‘normal’ software therefore its operation carries considerable hazards. It can be an exception if the operator can prove that the damage occurred due to an unavoidable cause that falls beyond the realm of activities involving considerable hazards, in this case: beyond the operation of the software.

I also examined the criminal liability for the operation of AI software. I came to the conclusion that AI entities cannot the treated as perpetrators of criminal offenses because the personal scope of the Hungarian Criminal Code only includes natural persons (human beings) and it is also impossible to examine the criminal state of mind of an AI entity regarding lack of consciousness. Furthermore they cannot be treated as legal persons regarding the previously explained situations so criminal measures for legal entities cannot be applied to

them too. Nonetheless AI can serve as tool for committing crimes so I also brought an example for such a case from the virtual worlds.

Finally I drew up the role of artificial intelligence driven components in virtual societies. These components are typically presented in the virtual world simulation software as smaller parts; automatically running scripts which are responsible for movement and control of opponents or other automated aspects of the world. I classified virtual entities into two categories: the first are virtual entities without AI, the second are with AI components.

I modelled using the circumstances of the so called "corrupted blood" incident as typical event when malfunctioning of AI components in a virtual world causes serious inconvenience to users. In this case a virtual disease decimated the characters of World of Warcraft players which stemmed from the malfunctioning AI script of one of the opponents. I also described that scripted entities of virtual worlds gain the information necessary for their working mechanisms from the servers responsible for permanent operation. The central servers are maintained by the developer for the connecting users. In this case the operator of the AI entity is not the user but the developer itself.

As a conclusion it can be said that due to insufficient operation of the servers, the user's virtual property can be in danger and can be destroyed in connection with the omission of the developers. The developer can be obliged according to the rules of warranty to pay compensation for damages to the concerned user or to restore the original condition (e.g. restore the lost virtual property) if it is possible.

I summarized my suggestions for the abovementioned anomalies in the closing point of the chapter in a four-point enumeration. I suggested a solution similar to UNCITRAL Model Law based on which the operator of the software should be held liable for the behavior of and damages caused by artificial intelligence.

5. Crimes committed in virtual societies: priority of self-regulation

The third part of the dissertation is titled "crime in virtual societies" and wants to highlight that such abuses can be committed in virtual environments that have their pairs in the physical world too. In the later and earlier parts of the dissertation there are criminal law related examinations too but I considered important to write a more general part about criminal law problems of the topic because the more fundamental issues are easier to present this way.

I divided crimes committed in computer environments into three groups regarding perpetration methods. The first is the group of 'classic cybercrimes' which common feature is

that the protected general social interest is the integrity and safety of information technology systems and data stored in them. Such cybercrimes can be committed only by computer so the legislator had to create new legal definitions for these new phenomenons. The second is the group of 'modern cybercrimes' which cannot be committed only by using computer infrastructure but the abuses often affect such data that can be digitalized. The evolvement of technology catalyzes these areas of crime (e.g. child pornography, infringement of copyright, misuse of personal data). The third and last is the group of virtual crimes which are crimes committed in computer simulated virtual environments. Virtual crime encompasses such crimes that can be committed only by computers but the legislator did not have to create new definitions. Virtual crime differs from crimes committed in the physical world (e.g. stealing the property of somebody) in a sense that they are committed in an alternative universe from which they cannot be separated. Abuses belonging to the group of virtual crime are forming a unique, specific group among cybercrimes and shows different tendencies than acts defined in the first two groups. Among virtual crimes we can also differ between crimes against person, property and economy.

I presented the specifics of virtual crimes against personal rights and interests through the case of Mr. Bungle. The perpetrator of a virtual rape was a player whose avatar was called Mr. Bungle. The player in the Lambda MOO game by his offensive, violent actions and messages 'raped' other players' avatars in the game environment. He committed this act using a virtual item: a voodoo doll which was capable to control other player's behavior in the game. The legal conclusion about the incident is that it cannot be treated as sexual assault because such a crime cannot be committed outside the physical world. However it was suitable to harass the victims of the violent act from a psychical viewpoint. According to this case crimes offending persons can be committed in virtual environments too, even if these are targeting only the avatar of a certain player.

The specificity of crimes against virtual property is that in virtual communities such events can also happen when a member's property interest is offended so that the suspicion of crime comes to surface. Crimes offending virtual property are committed against items that have value in the virtual community. These are the components of virtual property and their role was demonstrated in connection with the virtual 'house-stealing' incident. I came to the conclusion that by misappropriation of data responsible for virtual items one can commit 'theft' on virtual goods which can cause material damage to their original owner, the victim. The legal definitions of the criminal code can be applied to such criminal acts by classifying them as crimes via or against information technology system or data.

A third specific group of virtual abuses is virtual vandalism which means the destruction of items, keepsakes or real estates belonging to other players of the three dimensional cyberworld. I classified the destruction of virtual goods as offense against virtual property due to their nature.

I also mentioned the phenomenon of 'griefing' which can be described as an intentional act that embarrasses others and the perpetrator's goal is to bother the players and reduce positive gaming experience. In principle the griefer abuses regular possibilities of the game to harass the entertainment of other users. I also described the harming of inner rules of gamer communities (the so called clan-rules) and their criminal relevance and also presented the possibility of power abuse in online communities. I found about them that in an exceptional case such acts can also cause the suspicion of crime but in most cases they are harming only the end user license agreement or the code of conduct of the game.

Finally I examined in detail the possibility of using the virtual world for terrorist purposes. According to particular authors such possibilities as anonymity, global access and extending transactional surfaces can easily make the software likeable for users but on the other hand they can serve as tool for international threats too. I used the analysis of the National Security Agency (NSA USA) and presented their examples to show how virtual reality can be used for terrorist purposes. I came to the conclusion that we do not have to be afraid about the terrorist use of online games as it was described in the analysis of the NSA. This is confirmed by the fact that no such event has came to surface so far. Furthermore I also mentioned that with the goals of terrorist organizations it is more compatible to communicate using anonymous, encrypted channels.

About virtual crime it can be said as a conclusion that self-regulating mechanisms of virtual communities and their inner moderation is enough to handle the situations in most cases so the intervention of the authorities should remain a final solution. Criminal law should remain as 'ultima ratio' in this area too. The national and international cooperation of the competent authorities and their training should be realized in the future in order to avoid abuses and make effective actions.

6. Centralized virtual payment systems and main conclusions about them

The dissertation's fourth and last individual part is titled "payment systems of the virtual economies". In this part I examined from a legal perspective the operation of commercial platforms in virtual communities regarding economical and financial market issues.

The first chapter deals with the payment systems of centralized virtual economies. These economies have some kind of central control that supervises their operation. The chapter starts with the evolution-story of money and virtual currencies and draws up what can be considered as virtual paying instrument. The conclusion is that virtual instruments of payment are behaving as medium of exchange and unit of account in the virtual economies. According to the cited study of the European Central Bank: virtual currency is a legally not regulated, digital type of currency that is issued and controlled by its developers, accepted and used by members of certain virtual communities and the legal background for its use is included in the end user contract agreement attached to the software product.

I classified centralized virtual financial systems into three categories regarding that is it possible to change it to other currencies or buy real world items on it. In a closed virtual financial system the software and the official related services do not allow users to change or trade their virtual currency to real world money. In a half-opened virtual financial system the service provider allows users to buy virtual currency using the official platform of the virtual world on previously specified exchange rates, but switching back is not officially supported. In a fully opened virtual financial system the exchanging option is officially supported back and forth as the feature of the software.

Further I examined the possible similarity of electronic money and virtual money. From a legal perspective I highlighted the lack of general regulation. Electronic money is regulated properly on national and European level but we cannot say this about virtual money at all. According to the respecting EU directive and the Hungarian Act about Credit Institutions and Financial Ventures, electronic money is being issued by its issuer for the reception of cash. This is only partly true to virtual money because it can be achieved not only by changing cash but by making certain virtual activities (e.g. reward for completing quests, mining). It is also a conspicuous difference that electronic money must be accepted not only by its issuer but by third party too for the purpose of completing payment operations. This is not true to virtual money at all because it can be used only inside that virtual world which uses it as medium of exchange. Furthermore virtual money types use totally different exchange units therefore they behave more as truly independent currencies and not as the electronic form of an already existing one.

I presented as an example the centralized economy of Second Life which has a self-supporting inner market operating totally closed and has no direct relation with physical world. The economy concentrates exclusively to virtual items, services and uses completely a virtual infrastructure developed by Linden Lab and operates inside this framework. Beside of

this essential difference the economy of this virtual world operates similarly to its pairs in the physical world. Due to this nature the economic performance of Second Life can be measured and compared to economies of the world's real countries.

One of the main problems of centralized virtual economies can be expressed so that the only regulating authority of them is their developer. In the terms of user rights it can be concluded that due to the one-sided nature of software end-user contractual agreements the responsibility of users is usually higher than the developer's and services provider's responsibility.

It is also important to mention that on the other hand developers always grant users the right to complain about misuses and incidents regarding the use of the virtual world software and they tend to restore the original condition in case of violation of the game rules.

7. Decentralized virtual payment systems and expanding the concept of virtual property

The second chapter of the fourth part – which is the dissertation's last main separate part – is intended to analyze the specialties of the decentralized virtual payment systems and deals exclusively with Bitcoin and in a lesser extent with other alternative cryptocurrencies.

Central control does not exist in the decentralized virtual currency model so beside the predetermined technical regulating system only the virtual medium of exchange and the users are the determinative factors.

Hereinafter I presented the specifics of the decentralized system based on the Bitcoin protocol. It is a new independent medium of exchange which is based on the rules defined in the study published by Satoshi Nakamoto in the autumn of 2008. Satoshi Nakamoto is a pseudonym and the identity of the original creator has not been surfaced yet. The currency exist solely in digital form and we cannot see its physical manifestation as coin or banknote on the market.

I introduced in the brief summary about the predecessors of Bitcoin and what kind of logical solutions led finally to the creation of the system which is operating the Bitcoin protocol. The Bitcoin handling software is functioning as a digital wallet on our computer after installation and it also stores our virtual money. Our wallet is nothing but a file on our hard drive named 'wallet.dat'. Our Bitcoin address is generated automatically by the software and it is appropriate to send and receive virtual currency. Every single Bitcoin-address consists of two parts. One is the so-called 'public key'; the other is the 'private key'. Our public key can be seen in the application on the 'Your Bitcoin Address' line, but the private key stays hidden.

The software uses the private key to authenticate transactions. This key also belongs to the randomly generated Bitcoin-addresses but remains invisible to other users; it functions as a specific digital signature. The software uses private keys as digital signatures to authenticate every single transaction with the virtual coins. The public and private key pairs are stored in the 'wallet.dat' file on the hard drive of the user's computer.

Every single transaction made through the Bitcoin-network is published on the internet. The traditional financial institutions such as banks protect their customers' privacy as they hide the transactions from unauthorized persons. In the Bitcoin system privacy protection is solved so, that users' personal data is totally unknown, but the money transactions are made public. I also introduced the working mechanisms of the transactions using a simple example for easier understanding.

One of the most important specifics of the decentralized system of Bitcoin is that no such central database, server or any other authority exists which is entitled to verify the transactions independently. Technically the system solves this in a way that there is a register of transactions, addresses and the digital signatures on the Bitcoin-network in the so-called blocks. These blocks are small databases, and every single Bitcoin transaction's information can be found in them. Unlike in the traditional banking system, in the Bitcoin network it is not the accountholder's data which are public, but those of the transactions. The Bitcoin client downloads every single block from the network to the user's computer, and later the new ones also. The database consists of every single successful Bitcoin-transaction and it is stored on every single Bitcoin-user's computer, and it updates permanently through the network. At least six other computers have to legitimize a transaction on the network to be successful. The information stored in the virtual wallet is compared with that in the blocks, and this is how the software counts how many Bitcoins a certain user have.

The virtual coins are generated on the nodes of the Bitcoin network, when the computers find the solution to a cryptographic algorithm. To produce Bitcoins this way one has to download software which uses the computing power of our computer's processor or video-card to solve such algorithmic problems on the network. These applications are called 'mining-software' and work completely independent of the 'wallet' software. When we manage to solve an algorithm, a block is created which stores virtual coins and contains every single transaction carried out with them. This is the essential core of the proof-of-work concept meaning that virtual items should have work performance behind their creation. Bitcoin, however, cannot be created in unlimited quantities. The maximum quantity of Bitcoin

which can be created is predetermined to 21 million coins. After creating this amount of Bitcoin the number in circulation will be constant.

The current exchange rate of Bitcoin is purely determined by supply and demand due to lack of central control so rapid and drastic exchange rate fluctuation is typical. I described this phenomenon with some examples from the history of the virtual coin.

In the following points I compared the behavior of Bitcoin with more traditional payment methods like online paying options, virtual currencies of online games and official (offline) currencies of states. I came to the conclusion that the advantages of the system can be considered as disadvantages too. Dangers in anonymity and decentralization are repulsive to the bigger expanse of the decentralized virtual currency. I also pointed out regarding the example of the 'Iraqi Swiss Dinar' that a currency without central guaranties can remain on the market for longer time if the market accepts it as medium of exchange and trusts in it.

About the legal classification of Bitcoin I used multilateral approach and method of elimination. I analyzed according the legal regulation in force that how can be decentralized currencies classified and I found that they can be treated nor as money, nor security, nor intangible asset or intellectual creation. Due to its nature it can be treated as special digital asset or commodity that behaves similar to precious metals because it is available in a scarce and predetermined amount therefore its value will probably rise in the future. This theory is confirmed by the fact that Bitcoin users treat the digital asset more likely as treasure forming and investment tool.

In the following point of the chapter I reviewed the legal reactions of existing country legislations so far about the Bitcoin phenomenon and divided them into three categories. To the first group such countries belong that accept the use of the virtual commodity on the market. It is common in these legislatures that the central bank or the financial supervisory authority raises the attention of the market about the risk factors and urges the creation of legislation related to the topic. Most of these countries treat the profit from Bitcoin transactions as taxable income. The legal classification of the cryptocurrency is doubtful and the competent authorities of the concerned countries are reluctant to take a stable standpoint. However there is a consensus among them that Bitcoin cannot be treated as money in a classical view. Having regard to the market relations and behavior, the classification as digital commodity that is part of the user's (virtual) property is most close to reality.

I listed in the second group such countries that are restricting the use of Bitcoin on the market. The regulation usually stops at the level that it limits or forbids the operation of ventures doing business in Bitcoin but allows private use.

Finally a few countries were listed in the third group that banned totally the use of cryptocurrencies. It can be said about their regulations in general that the very strict protection of the national financial market or crime prevention purposes are behind their interpretations.

In the next point of the chapter I examined the role of Bitcoin in criminal activities from the perspective of criminal law and criminology. The statements can be applied comprehensively to almost all other cryptocurrencies due to similar working mechanisms.

Beside the unquestionable benefits of lacking central control (fastness, anonymity, unified settlement etc.) the virtual transactional system has plenty of attribution that are rather in favor of black market usage. At first sight it seems impossible to track back and investigate criminals who are using decentralized currencies, though the system gives some help to start. For example every transaction is public in the blockchain so suspicious transfers can be tracked back to the source. I also pointed out from the perspective of searching for the original owner of an address that it is possible to request information from operators of Bitcoin exchange websites because these could have enough personal data of users (e.g. registered user name, e-mail address, IP address used for logging in, bank account number) to identify the perpetrator or other persons involved.

For better understanding I also examined the possible role of Bitcoin in two specific crimes: theft and money laundering. By exchanging money to Bitcoin and transferring the amounts to specific Bitcoin-addresses it is not difficult to launder money clean originating from criminal activities. I introduced also such webpages that are openly specialized for Bitcoin laundering in order to protect the anonymity of users. Having regard to this phenomenon I made a suggestion that Bitcoin exchange sites should operate special requesting services for investigating authorities in order to provide information easier. There are already similar good examples on the side of social networks and auction sites (e.g. Facebook, eBay).

Compared to money laundering, about the theft of Bitcoins we already met some well documented cases. The most important factor about these abuses is the virtual wallet file on the hard drive of the computer (wallet.dat) containing how much coin certain user have. I pointed out that due to its doubtful or even non-existing legal classification in most cases it is not clear that which specific legal definition of the Criminal Code should be applied to state of affairs for right classification. In my opinion the computer environment is indispensably necessary for committing crimes with or using Bitcoin so it is more reasonable to treat them legally as computer crimes (therefore, as crimes defined in sections 375., 423. or 424. of the Criminal Code) than theft even though the virtual currency behaves more akin to commodities

than data. I confirmed my aforementioned argumentation with more practical cases from Bitcoin's history.

Furthermore I mentioned that Bitcoin is preferred to use for activities such as purchasing illegal goods (e.g. firearms, drugs) on the internet. Finally I examined and disproved the popular theory that Bitcoin-system is none other than a world-wide 'pyramid game'. The earliest users of Bitcoin made profit from the increase of the virtual commodity's exchange rate and not from popularizing the system to get more and more members paying fees to earlier members in order to widen the Ponzi-scheme and get disbursement.

In the last point of the chapter I introduced other alternative cryptocurrencies that are bursting forward on the market since the appearance of Bitcoin but are logically similar to the pioneering invention.

I highlighted the decentralized domain name system of Namecoin. Litecoin which have the second biggest market share after Bitcoin. Peercoin with built-in inflation ratio. Ripple that operates as a decentralized commodity market and finally Mastercoin that experiments with interoperability between cryptocurrencies.

As a final conclusion it can said that such data sets exist in virtual space which behave more akin to commodities than the classical meaning of data and bear similar nature as physically existing assets except the fact that they exist only in digital form. From this point of view the lack of proper regulation bears much uncertainty so the professional debate should not be awaited much longer now.

In my opinion regarding the nature of Bitcoin and the known market mechanisms it should be treated as new kind of digital commodity. In this concept it is a bit similar to such virtual items on right of disposal can be obtained.

Although there is one essential difference between items of virtual worlds and cryptocurrencies. Cryptocurrencies are created not from a contractual or from other statutory governed relation but can be obtained (mined) outside of them. The right of disposal on a certain amount of Bitcoin is obtained by the user who mined the coins or got it from other users. The right of disposal on Bitcoin appears in a concrete contractual relationship – for example in a Bitcoin purchasing contract – as intangible asset. The value of the right of disposal is determined primarily by the exchange rate and the negotiated price.

The ideal solution about the new technology would be an independent regulation on national and European level that would confer legal existence to cryptocurrencies and treat them as negotiable objects and virtual commodities, furthermore this new general regulation should define the criteria for creating ventures using or accepting Bitcoin.

A témában megjelent tanulmányok:

1. *Fantázia vagy valóság? Virtuális világok szerzői jogi problémái*. In: Infokommunikáció és jog 44. Budapest, 2011.
2. *Virtual Crime: Bűnözés egy alternatív valóságban*. In: Infokommunikáció és jog 47. Budapest, 2011.
3. *Fantázia vagy valóság? Virtuális világok szerzői jogi problémái.* In: Studia Iuvenum Iurisperitorum 6. Pécs, 2012.
4. *Bitcoin: Az anarchisták pénze vagy a jövő fizetőeszköze*. In: Infokommunikáció és jog 49. Budapest, 2012.
5. *Bitcoin: Az anarchisták pénze vagy a jövő fizetőeszköze – átdolgozott, bűnügyi résszel bővített változat.* In: Jura 2012/2. szám. Pécs, 2012.
6. *Bitcoin: Anarchist Money or Currency of Future*. In: Studia Juridica 2013. évi szám. Pécs, 2013.
7. *A számítógépes bűnözés legújabb tendenciái, különös tekintettel az online közösségi tereken elkövetett visszaélésekre*. In: Magyar Rendészet 2013/1. Budapest, 2013.
8. *Bitcoin: The Decentralised Virtual Currency as Criminal Tool*. In: European Police Science and Research Bulletin 9. Luxembourg (Luxemburg), 2013.
9. *BitCoin: General and Criminal Analysis of the Decentralized Virtual Currency*. In: Proceedings of the Estonian Academy of Security Sciences 12., Tallinn (Észtország), 2014.
10. *Felelősség a mesterséges intelligencia által okozott károkért*. In: PTE ÁJK PhD Tanulmányok 2014. Pécs, 2014.
11. *A mesterséges intelligencia fejlesztésének és üzemeltetésének egyes felelősségi kérdései*. In: Infokommunikáció és jog 62., Budapest, 2015. (megjelenés alatt)

A témában elhangzott önálló előadások:

1. *Investigating Cybercrimes*. 8th Summer School of IP and ICT Law (szervező: European Academy of Law and ICT), 2013. augusztus 4-10., Reichenau an Rax, Ausztria
2. *Legal Background of Cybercrime*. 10. Jubileumi Hacktivity, Informatikai Biztonsági Konferencia, 2013. október 11-12., Budapest

3. *Bitcoin – Advantages and Dangers of a Decentralized Digital Currency*. Cyberspace 13, Informatikai Jogi Nemzetközi Konferencia, 2013. november 22-23., Masaryk University Brno, Csehország

4. *A számítógépes bűnözés kriminológiai és jogi háttere*. Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, 2014. március 12., tantermi előadás a kriminológia tantárgy keretében

5. *Liability for Damages Caused by Artificial Intelligence in Online Games*. Cyberspace 14, Informatikai Jogi Nemzetközi Konferencia, 2014. november 28-29., Masaryk University Brno, Csehország

6. *A számítógépes bűnözés kriminológiai és jogi háttere*. Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, 2015. február 26., tantermi előadás a kriminológia tantárgy keretében

7. *Felelősség a mesterséges intelligencia által okozott károkért*. Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 2015. május 13., előadás az Infokommunikációs és Polgári jogi Tudományos Diákkör keretein belül.

8. *Investigation and Legal Background of Cybercrime. Crimes, Techniques and Cases*. The Reality of Cyber Security – On the Edge of Digital War, Nemzetközi Konferencia (szervező: Pécs Debate Academy), 2015. augusztus 18-19., Pécs, PTE Műszaki és Informatikai Kar.

A szerző elektronikus elérhetősége / author's e-mail address: eszteri@outlook.com